AEPA Solicitation Audit Checklist

Proposal: 025-F Cybersecurity Solutions & Training

Awarded Vendor(s): CDWG;

Award Date: 2/20/25 **Contract Number:** 025-F

- ☑ 1 Legal Affidavit(s)
- ☑ 2 Copy of Solicitation Documents
- ☑ 3 Copy of Questions & Answers
- NA ~~4 Copy of Addenda~~
- ☑ 5 Access Report
- ☑ 6 Opening Record
- ☑ 7 Copy of Qualified Vendor Responses
- ☑ 8 Recommendation for New Contracts
- ☑ 9 Copy of Signed Contract(s)

Forum Communications Company

MN Affidavit No. g7pIRh9COnjxOhmg2UaU

See Proof on Next Page

AFFIDAVIT OF PUBLICATION

State of Texas, County of Bexar, ss:

Hayden Lipsky, being first duly sworn, deposes and says: That (s)he is a duly authorized signatory of Column Software, PBC and duly authorized agent of the The Forum of Fargo-Moorhead (MN), a newspaper printed and published in the City of Moorhead, County of Clay, State of Minnesota.

1. I have personal knowledge of the facts stated in this Affidavit, which is made pursuant to Minnesota Statutes §331A.07.
2. The newspaper has complied with all of the requirements to constitute a quailified newspaper under Minnesota law, including those requirements found in Minnesota Statutes §331A.02.
3. The dates of the month and the year and the day of the week upon which the public notice attached/copied below was published in the newspaper are as follows: Wednesday, August 7, 2024, Wednesday, August 14, 2024
4. The publisher's lowest classified rate paid by commercial users for comparable space, as determined pursuant to §331.A06, is as follows: $25.00 per column inch.
5. Pursuant to Minnesota Statutes §580.033 relating to the publication of mortgage foreclosure notices: The newspaper's known office of issue is located in CASS County. The newspaper complies with conditions described in §580.033, subd. 1, clause (1) or (2). If the newspaper's known office of issue is located in a county adjoining the county where the mortgaged premises or some part of the mortgaged premises described in the notice are located, a substantial portion of the newspaper's circulation is in the latter county.

(Signed) Hayden Lipsky

NOTARY PUBLIC STATE OF TEXAS

Robert Hollie III

ID NUMBER
133582194
COMMISSION EXPIRES
February 10, 2026

VERIFICATION

State of Texas
County of Bexar

Subscribed in my presence and sworn to before me on this: 08/14/2024

Notary Public

Electronically signed and notarized online using the Proof platform.

AEPA #025 – LEGAL NOTICE

-

Notice to Vendors

Sealed solicitations will be received by the Association of Educational Purchasing Agencies (AEPA) on behalf of its 30 State Member Agencies until: 1:30 p.m. ET, September 17, 2024

Solicitations: 025-A Athletic Field Lighting, 025-B Hardwood & Synthetic Flooring, 025-C Copiers, Multi-Function Print Devices, Printers, & Managed Print Services, 025-D Roofing & Related Services, 025-E Security Solutions, 025-F Cybersecurity & Training, 025-G Portable & Modular Classrooms

All responses shall be submitted online via Bonfire by the due date and time listed above. Vendors are requested to visit AEPA's website at https://aepacoop.org/registration-solicitations/for instructions on how to register at no cost with Bonfire. AEPA documents will be released on August 1, 2024. Note that Vendors must be able to provide their proposed products and services in up to 30 states.

Solicitations will be publicly opened after 1:30 p.m. ET, September 17, 2024 at Lakes Country Service Cooperative, 1001 E Mt Faith, Fergus Falls, MN 56537. An opening record will be posted to AEPACOOP.org.

(Aug. 7 & 14, 2024)

Ad Number: 0000494591-01
Insertion Number: N/A
Size: 1 Col x 3.57 in
Color Type: 0
Advertiser: Cooperative Purchasing Network
Agency: N/A
Section-Page-Zone(s): D-3-All
Description: Notice to Vendors Sealed solicita...

Google ruling may slowly bring changes

By SHIRA OVIDE
Washington Post



JASON HENRY • New York Times
The U.S. government must now propose to Judge Amit Mehta ways to restrain Google's actions to fix its monopoly. It could take years to resolve.

A federal judge last week said Google broke the law to kneecap competition in web search in ways that entrenched the company's power.

It was the second time in the past year that a judge or jury had declared Google an illegal monopoly. The previous time was over how Google runs its Android app store.

The next steps, which involve proposing legal fixes to undo Google's behavior, are essentially about imagining an alternative future in which Google isn't Google as we know it.

What new ideas could flourish, which new companies might get off the ground or what products might be cheaper if Google were handcuffed from flexing its monopoly power over search?

Here are some changes that could result. In the end, though, not much may really change. That's what happened after Google was found to have broken the European Union's antimonopoly laws.

The U.S. government must now propose to Judge Amit Mehta ways to restrain Google's actions to fix its monopoly. It could take years to resolve. In the app store case, a judge will soon decide how Google must change its illegal status quo.

Google said it plans to appeal Monday's ruling and is "focused on making products that people find helpful and easy to use." A spokesman for Google declined to discuss speculation about what happens next.

But here are some possibilities.

A search engine without ads?

Imagine a Google-quality search engine but without ads — or one tailored to children, news junkies or Lego fans.

It's possible that Google could be forced to let other companies access its search technology or its essential data to create search engines with the technical chops of Google. What results could be more specialized choices.

You might imagine that a company takes Google's secret sauce and tweaks it to make a kid-friendly search engine, suggested Matt Stoller, director of research at the American Economic Liberties Project and a frequent critic of Big Tech power. Another company could prioritize websites that look out for your privacy. Another might show searches in a visual-first way.

"We're going to see the innovation of mankind come out," Stoller said.

Letting a thousand Google-type search engines bloom is probably the idea that Google critics have embraced the most. But even if the government asks for it and Mehta agrees, it might not work.

Could Google break up? It seems unlikely, but the government could ask the judge to split Google into parts to fix its illegal monopoly power. In this scenario, the Chrome browser might be its own company and so might Google search and Android, for example.

There have been, and are, other search engines, including Microsoft's Bing, the privacy-focused DuckDuckGo and Neeva, started by a former senior Google executive. DuckDuckGo and Bing are nowhere near as popular or as lucrative as Google. Neeva was little used and shut down this year.

Apple could create a search engine

Google pays Apple many billions of dollars a year — $20 billion in 2022 — to make Google the standard way to search the web on Apple's Safari browser.

That arrangement gives Google access to valuable searches from Apple device owners, and it guarantees Apple gobs of money.

Megan Gray, an antitrust law specialist with GrayMatters Law & Policy and a critic of Google's power, said the judge could significantly change or end Google's deals with Apple and companies that put Google search front-and-center on Android phones and web browsers.

The likeliest scenario is you'd need to pick whether to use Google on your iPhone or something else. But technologists and stock analysts have also speculated for years that Apple could make its own search engine. It would be like when Apple started Apple Maps as an alternative to Google Maps.

Apple didn't respond to a request for comment.

Could advertising become less expensive?

Mehta said Google has the power to charge artificially high prices for the text ads you might see when you search for terms like "auto insurance quotes Minneapolis."

In theory, if alternative search engines become popular, there would be more competition and lower prices for the insurance providers and other companies trying to grab your attention when you search.

And again, in theory, if they pay less for advertising, car insurance and other products you buy could be cheaper.

Could the company break up?

This one seems unlikely, but the government could ask the judge to split Google into parts to fix its illegal monopoly power. In this scenario, the Chrome browser might be its own company and so might Google search and Android, for example.

Stoller said that when corporations such as Standard Oil and AT&T have been forced to split up in past illegal-monopoly rulings, the component companies were liberated to come up with clever ideas that didn't have a chance inside the giant corporation.

Could privacy be strengthened?

Jason Kint, chief executive of online news lobbying group Digital Content Next, said Google's multiple products should no longer be allowed to co-mingle information about what you do. It would essentially be a divorce of Google's products without breaking the company up.

That could mean, for example, that whatever you did on your Android phone or the websites you visit using Chrome would not feed into one giant Google repository about your activities and interests.

If Google had less information, it could be better for your privacy, and it might help other companies that don't have Google's wealth of data.

Could Android app store change?

The judge in the other Google monopoly case has seemed receptive to loosening the company's absolute power over apps.

That might mean that you would be able to buy an Amazon Kindle e-book from its Android app, which you can't do now. Games such as "Fortnite" that have been absent from Android phones might be available, too.

In a recent court hearing, the judge also seemed open to cutting the fees that Google collects when you buy digital subscriptions. to things like Disney Plus, Match.com or X from Android apps. That could translate into lower prices for things you buy in apps.

Our data is not safe. Resist when you can.

◂ **SINGLETARY** from D1

As part of the sign-up process, I was required to provide birthday information. However, I mistakenly reversed the numbers for month and day. Spotting my error minutes after registering, I tried to correct my profile, but Qatar's system wouldn't allow it.

I couldn't get help on the airline's site, so I sent a message via X to @qatarsupport, which promised 24/7 customer support.

In a direct message, I was instructed that I would have to upload two identification documents, such as a passport, birth certificate or driver's license.

Wait, what?

I didn't have to provide documentation when setting up the account.

Immediately, I became concerned. How many people have access to the data? Where is it stored? How secure is Qatar's system?

After several attempts, I couldn't get direct answers from Qatar through an emailed media request, so I reviewed its privacy notice.

The airline writes it "has taken adequate safeguards to ensure the confidentiality and security of your personal data."

I know I cannot win in the race to protect my data. It has been repeatedly exposed. But every act of defiance, however small, is worth a victory lap.

Then, it promised that to prevent unauthorized access, it has "put in place physical, technical and administrative measures to safeguard" my data.

This assurance did not comfort me after reading the following caveat: "Although we use reasonable efforts to protect your personal data, we cannot guarantee the security of your personal data transmitted to our website or mobile apps via the internet or similar connection."

Our data is not safe.

In 2013, Target's computer system was breached, allowing criminals to access to steal credit and debit card information from as many as 40 million consumers. An additional 70 million customers had their names, phone numbers and email addresses compromised.

This incident affected my personal information.

Almost seven years ago, Equifax announced a massive breach had exposed the personal information of about 147 million people. At the time, the company said hackers exploited a "website application vulnerability."

People's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers, credit card numbers and other personal information were stolen, putting millions of folks at risk of identity theft and other fraudulent activity.

Equifax notified me that my data was compromised.

Every time there's a data breach, the companies involved tell their customers that they deeply regret the inconvenience it might cause. They pledge to enhance security procedures. However, gaps in data protection continue to lead to stolen data.

And, to be fair to the companies, con artists and hackers work full time, sometimes with the help of foreign governments, to outsmart corporate security systems.

So, I will not be uploading my driver's license, birth certificate or passport to Qatar's website for its travel rewards program. I found a workaround.

I deleted the one account with the wrong information and created a new one.

I know I cannot win in the race to protect my data. It has been repeatedly exposed.

But every act of defiance, however small, is worth a victory lap.

Resistance isn't always futile.

CLASSIFIEDS + PUBLIC NOTICES

STARTRIBUNE.COM/CLASSIFIEDS
• 612.673.7000 • 800.927.9233

Proposals for Bids

Sealed proposals will be received by the Cooperative Purchasing Connection (CPC) on behalf of its current and potential member agencies in Minnesota, North Dakota, and South Dakota until for RFP #25.2 – Instructional Materials and Classroom Supplies.

Specifications and forms may be obtained by registering for free with CPC on Public Purchase (www.publicpurchase.com).

Proposals must be uploaded to Public Purchase by 1:00 p.m. CT on Tuesday, September 17, 2024, and late proposals will not be considered.

Legal Notices

Public Notice
The Ordway Center for the Performing Arts in St. Paul, MN is securing RFP for the provision of Intelligent LED based Theatrical Lighting Fixtures and support materials. Please request a copy of the RFP by email to aluft@ordway.org or by clicking this link. Proposals must be submitted by August 16, 2024 for consideration.

Public Notice
The Ordway Center for the Performing Arts in St. Paul, MN is soliciting RFPs for an Electrical Contractor and an ETC Theatrical Lighting System Integrator for the renovation and upgrade of the Ordway Music Theater Lighting Infrastructure and Atrium Lighting Systems. Please request a copy of the RFP by email to aluft@ordway.org or by clicking the link below. Proposals must be submitted by October 7, 2024 for consideration.

Electrical Contractor - https://onedrive.live.com/?authkey=%21ADHvH1UN8bmMUzg&id=F07928DE1B5E66B7%2149411&cid=F07928DE1B5E66B7&parId=root&parQt=sharedby&o=OneUp

ETC Systems Integrator - https://onedrive.live.com/?authkey=%21AObbzcsLvXjoVY0&id=F07928DE1B5E66B7%2149413&cid=F07928DE1B5E66B7&parId=root&parQt=sharedby&o=OneUp

Proposals for Bids

Notice to Vendors
Sealed solicitations will be received by the Association of Educational Purchasing Agencies (AEPA) on behalf of its 30 State Member Agencies until:
1:30 p.m. ET, September 17, 2024
Solicitations: 025-A Athletic Field Lighting, 025-B Hardwood & Synthetic Flooring, 025-C Copiers, Multi-Function Print Devices, Printers, & Managed Print Services, 025-D Roofing & Related Services, 025-E Security Solutions, 025-F Cybersecurity & Training, 025-G Portable & Modular Classrooms, 025-H Playgrounds & Equipment
All responses shall be submitted online via Bonfire by the due date and time listed above. Vendors are requested to visit AEPA's website at https://aepacoop.org/registration-solicitations/ for instructions on how to register at no cost with Bonfire. AEPA documents will be released on August 1, 2024.
Note that Vendors must be able to provide their proposed products and services in up to 30 states.
Solicitations will be publicly opened after **1:30 p.m. ET, September 17, 2024** at Lakes Country Service Cooperative, 1001 E Mt Faith, Fergus Falls, MN 56537. An opening record will be posted to AEPACOOP.org.

Notice to Vendors
Sealed solicitations will be received by the Association of Educational Purchasing Agencies (AEPA) on behalf of its 30 State Member Agencies until:
1:30 p.m. ET, September 17, 2024
Solicitations: 025-A Athletic Field Lighting, 025-B Hardwood & Synthetic Flooring, 025-C Copiers, Multi-Function Print Devices, Printers, & Managed Print Services, 025-D Roofing & Related Services, 025-E Security Solutions, 025-F Cybersecurity & Training, 025-G Portable & Modular Classrooms
All responses shall be submitted online via Bonfire by the due date and time listed above. Vendors are requested to visit AEPA's website at https://aepacoop.org/registration-solicitations/ for instructions on how to register at no cost with Bonfire. AEPA documents willbe released on August 1, 2024. Note that Vendors must be able to provide their proposed products and services in up to 30 states.
Solicitations will be publicly opened after **1:30 p.m. ET, September 17, 2024** at Lakes Country Service Cooperative, 1001 E Mt Faith, Fergus Falls, MN 56537. An opening record will be posted to AEPACOOP.org.

StarTribune Business Monday, August 12, 2024

AFFIDAVIT OF PUBLICATION

STATE OF MINNESOTA)
COUNTY OF HENNEPIN)

650 3rd Ave. S, Suite 1300 | Mineapolis, MN | 55488

Terri Swanson, being first duly sworn, on oath states as follows:

1. (S)He is and during all times herein stated has been an employee of the Star Tribune Media Company LLC, a Delaware limited liability company with offices at 650 Third Ave. S., Suite 1300, Minneapolis, Minnesota 55488, or the publisher's designated agent. I have personal knowledge of the facts stated in this Affidavit, which is made pursuant to Minnesota Statutes §331A.07.

2. The newspaper has complied with all of the requirements to constitute a qualified newspaper under Minnesota law, including those requirements found in Minnesota Statutes §331A.02.

3. The dates of the month and the year and day of the week upon which the public notice attached/copied below was published in the newspaper are as follows:

Dates of Publication		Advertiser	Account #	Order #
StarTribune	08/05/2024	COOPERATIVE PURCHASING CONNECTION	1000337556	494591
StarTribune	08/12/2024	COOPERATIVE PURCHASING CONNECTION	1000337556	494591

4. The publisher's lowest classified rate paid by commercial users for comparable space, as determined pursuant to § 331A.06, is as follows: **$459.20**

5. Mortgage Foreclosure Notices. Pursuant to Minnesota Statutes §580.033 relating to the publication of mortgage foreclosure notices: The newspaper's known office of issue is located in Hennepin County. The newspaper complies with the conditions described in §580.033, subd. 1, clause (1) or (2). If the newspaper's known office of issue is located in a county adjoining the county where the mortgaged premises or some part of the mortgaged premises described in the notice are located, a substantial portion of the newspaper's circulation is in the latter county.

FURTHER YOUR AFFIANT SAITH NOT.

Terri Swanson

Subscribed and sworn to before me on: 08/12/2024

Diane E Rak Kleszyk

DIANE E RAK KLESZYK
Notary Public
Minnesota
My Commission Expires January 31, 2027

Notary Public

LocaliQ
South Dakota
GANNETT

PO Box 630567 Cincinnati, OH 45263-0567

AFFIDAVIT OF PUBLICATION

Cooperative Purchase, Lori Mittelstadt
Lakes Country Service Cooperative
1001 E Mount Faith AVE
Fergus Falls MN 56537-2375

STATE OF WISCONSIN, COUNTY OF BROWN

The Argus Leader, a daily newspaper published in the city of Sioux Falls, Minnehaha County, State of South Dakota, and personal knowledge of the facts herein state and that the notice hereto annexed was Published in said newspapers in the issue:

08/05/2024, 08/12/2024

and that the fees charged are legal.
Sworn to and subscribed before on 08/12/2024

D. Roberts
Legal Clerk

Nicole Jacobs
Notary, State of WI, County of Brown

8-21-26
My commission expires

Publication Cost:	$37.56	
Tax Amount:	$0.00	
Payment Cost:	$37.56	
Order No:	10429535	# of Copies:
Customer No:	1248830	0
PO #:	LABD0137287	

THIS IS NOT AN INVOICE!

Please do not use this form for payment remittance.

NICOLE JACOBS
Notary Public
State of Wisconsin

AEPA 025

Notice to Vendors

Sealed solicitations will be received by the Association of Educational Purchasing Agencies (AEPA) on behalf of its 30 State Member Agencies until:

1:30 p.m. ET, September 17, 2024

Solicitations: 025-A Athletic Field Lighting, 025-B Hardwood & Synthetic Flooring, 025-C Copiers, Multi-Function Print Devices, Printers, & Managed Print Services, 025-D Roofing & Related Services, 025-E Security Solutions, 025-F Cybersecurity & Training, 025-G Portable & Modular Classrooms

All responses shall be submitted online via Bonfire by the due date and time listed above. Vendors are requested to visit AEPA's website at https://aepacoop.org/registration-solicitations/ for instructions on how to register at no cost with Bonfire. AEPA documents will be released on August 1, 2024. Note that Vendors must be able to provide their proposed products and services in up to 30 states.

Solicitations will be publicly opened after 1:30 p.m. ET, September 17, 2024 at Lakes Country Service Cooperative, 1001 E Mt Faith, Fergus Falls, MN 56537. An opening record will be posted to AEPA-COOP.org.

Published August 5, 12 2024, at the total approximate cost of "37.56 and may be viewed free of charge at www.sdpublicnotices.com

LABD0137287

Forum Communications Company

ND Affidavit No. FRv93dDHvIPN7hfg3y6Z

AFFIDAVIT OF PUBLICATION

State of Pennsylvania, County of Lancaster, ss:

Yuade Moore, being first duly sworn, deposes and says: That (s)he is a duly authorized signatory of Column Software, PBC and duly authorized agent of the The Forum of Fargo-Moorhead (ND), a newspaper printed and published in the City of Fargo, County of Cass, State of North Dakota.

1. I am the designated agent of The The Forum of Fargo-Moorhead (ND), under the provisions and for the purposes of, Section 31-04-06, NDCC, for the newspaper listed on the attached exhibit.

2. The newspaper listed on the exhibit published the advertisement of: ***ND Bids/Proposals Notice;*** *(2) time: Wednesday, August 7, 2024, Wednesday, August 14, 2024*, as required by law or ordinance.

3. All of the listed newspapers are legal newspapers in the State of North Dakota and, under the provisions of Section 46-05-01, NDCC, are qualified to publish any public notice or any matter required by law or ordinance to be printed or published in a newspaper in North Dakota.

(Signed) Yuade Moore

Commonwealth of Pennsylvania - Notary Seal
Nicole Burkholder, Notary Public
Lancaster County
My commission expires March 30, 2027
Commission Number 1342120

VERIFICATION

State of Pennsylvania
County of Lancaster

Subscribed in my presence and sworn to before me on this: 08/14/2024

Nicole Burkholder

Notary Public
Notarized remotely online using communication technology via Proof.

AEPA #025 – LEGAL NOTICE

-

Notice to Vendors
Sealed solicitations will be received by the Association of Educational Purchasing Agencies (AEPA) on behalf of its 30 State Member Agencies until:
1:30 p.m. ET, September 17, 2024
Solicitations: 025-A Athletic Field Lighting, 025-B Hardwood & Synthetic Flooring, 025-C Copiers, Multi-Function Print Devices, Printers, & Managed Print Services, 025-D Roofing & Related Services, 025-E Security Solutions, 025-F Cybersecurity & Training, 025-G Portable & Modular Classrooms, 025-H Playgrounds & Equipment
All responses shall be submitted online via Bonfire by the due date and time listed above. Vendors are requested to visit AEPA's website at https://aepacoop.org/registration-solicitations/for instructions on how to register at no cost with Bonfire. AEPA documents will be released on August 1, 2024. Note that Vendors must be able to provide their proposed products and services in up to 30 states.
Solicitations will be publicly opened after 1:30 p.m. ET, September 17, 2024 at Lakes Country Service Cooperative, 1001 E Mt Faith, Fergus Falls, MN 56537. An opening record will be posted to AEPACOOP.org.
(Aug. 7 & 14, 2024)

The Bismarck Tribune

AFFIDAVIT OF PUBLICATION

See Proof on Next Page

State of Texas, County of Bexar, ss:

Hayden Lipsky, being first duly sworn, deposes and says: That (s)he is a duly authorized signatory of Column Software, PBC and duly authorized agent of The Bismarck Tribune, and that the publication(s) were made through The Bismarck Tribune on the following dates:

PUBLICATION DATES:
Aug. 5, 2024, Aug. 12, 2024

NOTICE ID: Vn8oB8wl6p2jnHApaP8M
PUBLISHER ID: COL-ND-0385
NOTICE NAME: AEPA 25 ND Bismarck Tribune
Publication Fee: $165.60

(Signed) Hayden Lipsky

VERIFICATION

State of Texas
County of Bexar

NOTARY PUBLIC STATE OF TEXAS
Robert Hollie III
ID NUMBER
133582194
COMMISSION EXPIRES
February 10, 2026

Subscribed in my presence and sworn to before me on this: 08/13/2024

Notary Public
Electronically signed and notarized online using the Proof platform.

AEPA 25

AEPA #025 – LEGAL NOTICE

-

Notice to Vendors

Sealed solicitations will be received by the Association of Educational Purchasing Agencies (AEPA) on behalf of its 30 State Member Agencies until:

1:30 p.m. ET, September 17, 2024

Solicitations: 025-A Athletic Field Lighting, 025-B Hardwood & Synthetic Flooring, 025-C Copiers, Multi-Function Print Devices, Printers, & Managed Print Services, 025-D Roofing & Related Services, 025-E Security Solutions, 025-F Cybersecurity & Training, 025-G Portable & Modular Classrooms, 025-H Playgrounds & Equipment

All responses shall be submitted online via Bonfire by the due date and time listed above. Vendors are requested to visit AEPA's website at https://aepacoop.org/registration-solicitations/for instructions on how to register at no cost with Bonfire. AEPA documents will be released on August 1, 2024. Note that Vendors must be able to provide their proposed products and services in up to 30 states.

Solicitations will be publicly opened after 1:30 p.m. ET, September 17, 2024 at Lakes Country Service Cooperative, 1001 E Mt Faith, Fergus Falls, MN 56537. An opening record will be posted to AEPACOOP.org.

8/5, 8/12 - COL-ND-0385

Ad Number: 0000494592-01
Insertion Number: N/A
Size: 1 Col x 3.39 in
Color Type: 0
Advertiser: Cooperative Purchasing Network
Agency: N/A
Section-Page-Zone(s): D-3-All
Description: Notice to Vendors Sealed solicita...

Google ruling may slowly bring changes

By SHIRA OVIDE
Washington Post



JASON HENRY • New York Times
The U.S. government must now propose to Judge Amit Mehta ways to restrain Google's actions to fix its monopoly. It could take years to resolve.

A federal judge last week said Google broke the law to kneecap competition in web search in ways that entrenched the company's power.

It was the second time in the past year that a judge or jury had declared Google an illegal monopoly. The previous time was over how Google runs its Android app store.

The next steps, which involve proposing legal fixes to undo Google's behavior, are essentially about imagining an alternative future in which Google isn't Google as we know it.

What new ideas could flourish, which new companies might get off the ground or what products might be cheaper if Google were handcuffed from flexing its monopoly power over search?

Here are some changes that could result. In the end, though, not much may really change. That's what happened after Google was found to have broken the European Union's antimonopoly laws.

The U.S. government must now propose to Judge Amit Mehta ways to restrain Google's actions to fix its monopoly. It could take years to resolve. In the app store case, a judge will soon decide how Google must change its illegal status quo.

Google said it plans to appeal Monday's ruling and is "focused on making products that people find helpful and easy to use." A spokesman for Google declined to discuss speculation about what happens next.

But here are some possibilities.

A search engine without ads?

Imagine a Google-quality search engine but without ads — or one tailored to children, news junkies or Lego fans.

It's possible that Google could be forced to let other companies access its search technology or its essential data to create search engines with the technical chops of Google. What results could be more specialized choices.

You might imagine that a company takes Google's secret sauce and tweaks it to make a kid-friendly search engine, suggested Matt Stoller, director of research at the American Economic Liberties Project and a frequent critic of Big Tech power. Another company could prioritize websites that look out for your privacy. Another might show searches in a visual-first way.

"We're going to see the innovation of mankind come out," Stoller said.

Letting a thousand Google-type search engines bloom is probably the idea that Google critics have embraced the most. But even if the government asks for it and Mehta agrees, it might not work.

Could Google break up? It seems unlikely, but the government could ask the judge to split Google into parts to fix its illegal monopoly power. In this scenario, the Chrome browser might be its own company and so might Google search and Android, for example.

There have been, and are, other search engines, including Microsoft's Bing, the privacy-focused DuckDuckGo and Neeva, started by a former senior Google executive. DuckDuckGo and Bing are nowhere near as popular or as lucrative as Google. Neeva was little used and shut down this year.

Apple could create a search engine

Google pays Apple many billions of dollars a year — $20 billion in 2022 — to make Google the standard way to search the web on Apple's Safari browser.

That arrangement gives Google access to valuable searches from Apple device owners, and it guarantees Apple gobs of money.

Megan Gray, an antitrust law specialist with GrayMatters Law & Policy and a critic of Google's power, said the judge could significantly change or end Google's deals with Apple and companies that put Google search front-and-center on Android phones and web browsers.

The likeliest scenario is you'd need to pick whether to use Google on your iPhone or something else. But technologists and stock analysts have also speculated for years that Apple could make its own search engine. It would be like when Apple started Apple Maps as an alternative to Google Maps.

Apple didn't respond to a request for comment.

Could advertising become less expensive?

Mehta said Google has the power to charge artificially high prices for the text ads you might see when you search for terms like "auto insurance quotes Minneapolis."

In theory, if alternative search engines become popular, there would be more competition and lower prices for the insurance providers and other companies trying to grab your attention when you search.

And again, in theory, if they pay less for advertising, car insurance and other products you buy could be cheaper.

Could the company break up?

This one seems unlikely, but the government could ask the judge to split Google into parts to fix its illegal monopoly power. In this scenario, the Chrome browser might be its own company and so might Google search and Android, for example.

Stoller said that when corporations such as Standard Oil and AT&T have been forced to split up in past illegal-monopoly rulings, the component companies were liberated to come up with clever ideas that didn't have a chance inside the giant corporation.

Could privacy be strengthened?

Jason Kint, chief executive of online news lobbying group Digital Content Next, said Google's multiple products should no longer be allowed to co-mingle information about what you do. It would essentially be a divorce of Google's products without breaking the company up.

That could mean, for example, that what you did on your phone or the websites you visit using Chrome would not feed into one giant Google repository about your activities and interests.

If Google had less information, it could be better for your privacy, and it might help other companies that don't have Google's wealth of data.

Could Android app store change?

The judge in the other Google monopoly case has seemed receptive to loosening the company's absolute power over apps.

That might mean that you would be able to buy an Amazon Kindle e-book from its Android app, which you can't do now. Games such as "Fortnite" that have been absent from Android phones might be available, too.

In a recent court hearing, the judge also seemed open to cutting the fees that Google collects when you buy digital subscriptions. to things like Disney Plus, Match.com or X from Android apps. That could translate into lower prices for things you buy in apps.

Our data is not safe. Resist when you can.

◂ **SINGLETARY** from D1

As part of the sign-up process, I was required to provide birthday information. However, I mistakenly reversed the numbers for month and day. Spotting my error minutes after registering, I tried to correct my profile, but Qatar's system wouldn't allow it.

I couldn't get help on the airline's site, so I sent a message via X to @qatarsupport, which promised 24/7 customer support.

In a direct message, I was instructed that I would have to upload two identification documents, such as a passport, birth certificate or driver's license.

Wait, what?

I didn't have to provide documentation when setting up the account.

Immediately, I became concerned. How many people have access to the data? Where is it stored? How secure is Qatar's system?

After several attempts, I couldn't get direct answers from Qatar through an emailed media request, so I reviewed its privacy notice.

The airline writes it "has taken adequate safeguards to ensure the confidentiality and security of your personal data."

I know I cannot win in the race to protect my data. It has been repeatedly exposed. But every act of defiance, however small, is worth a victory lap.

Then, it promised that to prevent unauthorized access, it has "put in place physical, technical and administrative measures to safeguard" my data.

This assurance did not comfort me after reading the following caveat: "Although we use reasonable efforts to protect your personal data, we cannot guarantee the security of your personal data transmitted to our website or mobile apps via the internet or similar connection."

Our data is not safe.

In 2013, Target's computer system was breached, allowing criminals to access to steal credit and debit card information from as many as 40 million consumers. An additional 70 million customers had their names, phone numbers and email addresses compromised.

This incident affected my personal information.

Almost seven years ago, Equifax announced a massive breach had exposed the personal information of about 147 million people. At the time, the company said hackers exploited a "website application vulnerability."

People's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers, credit card numbers and other personal information were stolen, putting millions of folks at risk of identity theft and other fraudulent activity.

Equifax notified me that my data was compromised.

Every time there's a data breach, the companies involved tell their customers that they deeply regret the inconvenience it might cause. They pledge to enhance security procedures. However, gaps in data protection continue to lead to stolen data.

And, to be fair to the companies, con artists and hackers work full time, sometimes with the help of foreign governments, to outsmart corporate security systems.

So, I will not be uploading my driver's license, birth certificate or passport to Qatar's website for its travel rewards program. I found a workaround.

I deleted the one account with the wrong information and created a new one.

I know I cannot win in the race to protect my data. It has been repeatedly exposed.

But every act of defiance, however small, is worth a victory lap.

Resistance isn't always futile.

CLASSIFIEDS + PUBLIC NOTICES
STARTRIBUNE.COM/CLASSIFIEDS
• 612.673.7000 • 800.927.9233

Proposals for Bids

Sealed proposals will be received by the Cooperative Purchasing Connection (CPC) on behalf of its current and potential member agencies in Minnesota, North Dakota, and South Dakota until for RFP #25.2 – Instructional Materials and Classroom Supplies.

Specifications and forms may be obtained by registering for free with CPC on Public Purchase (www.publicpurchase.com).

Proposals must be uploaded to Public Purchase before 1:00 p.m. CT on Tuesday, September 17, 2024, and late proposals will not be considered.

Legal Notices

Public Notice
The Ordway Center for the Performing Arts in St. Paul, MN is securing RFP for the provision of Intelligent LED based Theatrical Lighting Fixtures and support materials. Please request a copy of the RFP by email to aluft@ordway.org or by clicking this link. Proposals must be submitted by August 16, 2024 for consideration.

Public Notice
The Ordway Center for the Performing Arts in St. Paul, MN is soliciting RFPs for an Electrical Contractor and an ETC Theatrical Lighting System Integrator for the renovation and upgrade of the Ordway Music Theater Lighting Infrastructure and Atrium Lighting Systems. Please request a copy of the RFP by email to aluft@ordway.org or by clicking the link below. Proposals must be submitted by October 7, 2024 for consideration.

Electrical Contractor - https://onedrive.live.com/?authkey=%21ADHvH1UN8bmMUzg&id=F07928DE1B5E66B7%2149411&cid=F07928DE1B5E66B7&parId=root&parQt=sharedby&o=OneUp

ETC Systems Integrator - https://onedrive.live.com/?authkey=%21AObbzcsLvXjoVY0&id=F07928DE1B5E66B7%2149413&cid=F07928DE1B5E66B7&parId=root&parQt=sharedby&o=OneUp

Proposals for Bids

Notice to Vendors
Sealed solicitations will be received by the Association of Educational Purchasing Agencies (AEPA) on behalf of its 30 State Member Agencies until:
1:30 p.m. ET, September 17, 2024
Solicitations: 025-A Athletic Field Lighting, 025-B Hardwood & Synthetic Flooring, 025-C Copiers, Multi-Function Print Devices, Printers, & Managed Print Services, 025-D Roofing & Related Services, 025-E Security Solutions, 025-F Cybersecurity & Training, 025-G Portable & Modular Classrooms, 025-H Playgrounds & Equipment
All responses shall be submitted online via Bonfire by the due date and time listed above. Vendors are requested to visit AEPA's website at https://aepacoop.org/registration-solicitations/ for instructions on how to register at no cost with Bonfire. AEPA documents will be released on August 1, 2024.
Note that Vendors must be able to provide their proposed products and services in up to 30 states.
Solicitations will be publicly opened after **1:30 p.m. ET, September 17, 2024** at Lakes Country Service Cooperative, 1001 E Mt Faith, Fergus Falls, MN 56537. An opening record will be posted to AEPACOOP.org.

Notice to Vendors
Sealed solicitations will be received by the Association of Educational Purchasing Agencies (AEPA) on behalf of its 30 State Member Agencies until:
1:30 p.m. ET, September 17, 2024
Solicitations: 025-A Athletic Field Lighting, 025-B Hardwood & Synthetic Flooring, 025-C Copiers, Multi-Function Print Devices, Printers, & Managed Print Services, 025-D Roofing & Related Services, 025-E Security Solutions, 025-F Cybersecurity & Training, 025-G Portable & Modular Classrooms
All responses shall be submitted online via Bonfire by the due date and time listed above. Vendors are requested to visit AEPA's website at https://aepacoop.org/registration-solicitations/ for instructions on how to register at no cost with Bonfire. AEPA documents willbe released on August 1, 2024. Note that Vendors must be able to provide their proposed products and services in up to 30 states.
Solicitations will be publicly opened after **1:30 p.m. ET, September 17, 2024** at Lakes Country Service Cooperative, 1001 E Mt Faith, Fergus Falls, MN 56537. An opening record will be posted to AEPACOOP.org.

StarTribune Business Monday, August 12, 2024

AFFIDAVIT OF PUBLICATION

STATE OF MINNESOTA)
COUNTY OF HENNEPIN)

650 3rd Ave. S, Suite 1300 | Mineapolis, MN | 55488

Terri Swanson, being first duly sworn, on oath states as follows:

1. (S)He is and during all times herein stated has been an employee of the Star Tribune Media Company LLC, a Delaware limited liability company with offices at 650 Third Ave. S., Suite 1300, Minneapolis, Minnesota 55488, or the publisher's designated agent. I have personal knowledge of the facts stated in this Affidavit, which is made pursuant to Minnesota Statutes §331A.07.

2. The newspaper has complied with all of the requirements to constitute a qualified newspaper under Minnesota law, including those requirements found in Minnesota Statutes §331A.02.

3. The dates of the month and the year and day of the week upon which the public notice attached/copied below was published in the newspaper are as follows:

Dates of Publication		Advertiser	Account #	Order #
StarTribune	08/05/2024	COOPERATIVE PURCHASING CONNECTION	1000337556	494592
StarTribune	08/12/2024	COOPERATIVE PURCHASING CONNECTION	1000337556	494592

4. The publisher's lowest classified rate paid by commercial users for comparable space, as determined pursuant to § 331A.06, is as follows: **$436.80**

5. Mortgage Foreclosure Notices. Pursuant to Minnesota Statutes §580.033 relating to the publication of mortgage foreclosure notices: The newspaper's known office of issue is located in Hennepin County. The newspaper complies with the conditions described in §580.033, subd. 1, clause (1) or (2). If the newspaper's known office of issue is located in a county adjoining the county where the mortgaged premises or some part of the mortgaged premises described in the notice are located, a substantial portion of the newspaper's circulation is in the latter county.

FURTHER YOUR AFFIANT SAITH NOT.

Terri Swanson

Subscribed and sworn to before me on: 08/12/2024

Diane E Rak Kleszyk

DIANE E RAK KLESZYK
Notary Public
Minnesota
My Commission Expires January 31, 2027

Notary Public

Request for Proposal
AEPA RFP#025 - F
Cyber Security & Training

BID SECURITY REQUIRED: None

Part A – Instructions and Specifications

Notice to Respondents

Solicitation offers will be received by the Association of Educational Purchasing Agencies (AEPA) on behalf of its Member Agencies until:

September 17, 2024, at 1:30 p.m. ET

Each package consists of multiple parts:

Part A – Instructions and Specifications
Part B – AEPA General Terms and Conditions
Part C – Member Agency (State) Terms and Conditions
Part D – Questionnaire
Part E – Signature Forms
Part F – Discount & Pricing Workbook

All offers must be submitted online via the Bonfire eProcurement website by the due date and time listed above. AEPA solicitation documents can be downloaded after registering, at no cost, on Bonfire, https://aepacoop.bonfirehub.com/.

AEPA and/or the respective Member Agencies reserve the right to reject any or all offers in whole or in part; to waive any formalities or irregularities in any offers, and to accept the offers, which in its discretion, within state law, are for the best interest of any of the AEPA Member Agencies and/or their Participating Entities. Note that Respondents must be able to provide their proposed products and services in up to 30 states including California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, Texas, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. Note that not all states participate in each solicitation. The complete list of participating states is found below.

Solicitations will be opened online on **September 17, 2024, at 1:30 p.m. ET.**

Bid & Contract Timeline:

August 1, 2024	Release of IFBs/RFP via Bonfire
August 19, 2024	Voluntary Pre-Bid Conference Call
August 30, 2024	Deadline for questions from Respondents
September 17, 2024	Deadline for Submittals and Reading via Bonfire

September 19, 2024	Opening Record posted on the AEPA website, www.aepacoop.org
December 2-4, 2024	AEPA Approval of Offers
After December 4, 2024	Vendor Partners submit required documentation to AEPA Agencies
	Initial contract term–See Term of Contract and Extensions in General Terms & Conditions. Annual contract renewal dates subject to approval by AEPA

I. General Solicitation Procedures

A. Issuing Agency

The great benefit to the Vendor is that one response may be prepared for approval by AEPA and awarded by multiple AEPA Member Agencies and utilized by their Participating Entities located throughout many states. Solicitations may be issued as an IFB or an RFP depending on the category of goods/services being solicited. Respondents to a solicitation will submit their response in the required formats (PDF, Excel) of all files requested along with current pricing via Bonfire, a free online bidding platform, by the published due date and time. Respondents selected in response to this solicitation have the potential to provide products and services to local education agencies serving over 36,000,000 (excludes non-represented AEPA states) students, with additional local government agencies as permitted by state law.

Each AEPA Member Agency will individually publish notice of the solicitation. Respondents will submit responses online, electronically via Bonfire, https://aepacoop.bonfirehub.com/. Instructions on registering for AEPA solicitations on Bonfire can be found on the AEPA website, www.aepacoop.org. Responses deemed complete at opening will be evaluated by solicitation category committees comprised of AEPA Member Agencies representatives who have indicated they will participate in the category of products and services being solicited, and after AEPA approval, individual AEPA Member Agencies may award contracts to the AEPA Approved Vendor Partners or reject their offers.

The procurement activities of AEPA are limited to document preparation, distribution of the solicitation, initial evaluation, and recommendation for possible approval to AEPA Member Agencies. AEPA consists of agency officials who have agreed to assist one another in meeting the public purchasing needs of local school districts and other political subdivisions.

Contracts awarded through cooperative purchasing must meet the procurement laws of the states of each AEPA Member Agency. When these laws are satisfied, an individual entity using these contracts is deemed in compliance with competitive procurement regulations. As allowed by specific state statutes, they can issue purchase orders for any amount without the necessity to prepare their own solicitation, Request for Proposal (RFP), or Request for Quotations (RFQ). This saves the entity time and allows for economical and efficient purchasing.

AEPA requires that Respondents only respond if they can offer prices equal to or better than what they ordinarily offer to individual entities or cooperatives with equal or lesser volume. State laws that permit or encourage cooperative purchasing contracts do so in the belief that it saves the participants both time and money. Time is saved by having access to volume discounted contracts publicly solicited and being able to purchase what is needed without having to wade through the solicitation process (write solicitation, advertise the solicitation, open each response, evaluate, and select). Money is saved in procurement cost and lower prices will be the result of volume purchasing. Therefore, a contract issued by a cooperative can be used by hundreds of separate political units; but if it has the same or higher prices than what a single agency or state contract can get through its own solicitation, a cooperatively solicited contract may not be attractive to these members. **We request that**

Respondents respond with advantageous pricing and package so that together we can attract members to prefer the cooperatively awarded contract.

The AEPA policy for membership permits new agencies to become AEPA Member Agencies upon approval of existing members. If additional Agencies are added, they and their members may procure from existing contracts upon approval of the awarded Vendor Partners and in accordance with their state laws.

B. Questions

All questions from Respondents must be submitted online through Bonfire, AEPA will not accept questions in any other format during the solicitation process. All questions received during the solicitation process will be available via Bonfire. All Respondents will be automatically notified through email when AEPA responds to a question asked by a potential respondent. It is the Respondent's responsibility to check Bonfire for any questions and answers before the deadline. Questions received after the question deadline date will not be answered.

Should AEPA issue addenda during the solicitation process, all Respondents will be automatically notified through email of the released addenda. AEPA is not responsible for Respondents not acknowledging the issued addenda and not submitting a response according to those changes.

Questions regarding this solicitation after Opening, but before the approval of the contract, should be submitted to questions@aepacoop.org.

Questions regarding this solicitation after Notification of Approval should be submitted to bid-committee@aepacoop.org.

C. Respondent Qualifications

An essential part of the solicitation process is an evaluation to qualify the company being considered. All solicitations must contain answers, responses, and/or documentation to the information requested in the documents. Any Respondent failing to provide the required information/ documentation may be considered non-responsive, this includes submitting a response not in the proper format.

Respondents must demonstrate their ability, capacity, and available resources to provide the proposed products and services to participating AEPA member states and purchasing entities as defined in this solicitation. The Respondents are required to communicate and demonstrate within their response they have extensive knowledge, background, and at least five (5) years of experience with manufacturing, obtaining, delivering, installing, maintaining, and/or supporting the product lines of products, equipment, services, or software offered. AEPA and/or its Member Agencies reserve the right to accept or reject newly formed companies or companies failing to demonstrate their abilities or capacity solely based on information provided in the solicitation response and/or its own investigation of the company.

D. Bid/Proposal Security

If required as noted at the top of this Part, bids or proposals must be accompanied by a satisfactory security bond. Please note that not all AEPA Bid categories require a security bond.

If a security bond is required, a hard copy of the bid security must be in the possession of AEPA on or before, the exact due date and time. Original copies of the security must be submitted to AEPA c/o LCSC, ATTN: Purchasing Dept, 1001 E Mt Faith, Fergus Falls, MN 56537 in a sealed envelope with the Solicitation Number, Solicitation Category, and Respondent's name and address clearly indicated on the envelope or box. A copy of the bid security must be submitted via Bonfire. AEPA will not reject a response from a Vendor whose bid bond has not arrived by the due date and time as long as a scanned copy of the bid bond dated prior to the due date is uploaded with their response and the actual bond is in transit.

An acceptable bid/proposal security will have the principal being the Respondent and the Association of Educational Purchasing Agencies listed as the Agency of Record. The Security may be a one-time bond underwritten by a surety company licensed to issue bonds in the state of Nevada and said surety to be approved in federal circular 570 as published by the United States treasury department or the equivalent in cash or an irrevocable letter of credit from a FDIC financial institution. The security bond must remain in force for one hundred twenty (120) days of the solicitation opening.

E. Solicitation Submittal

1. Preparation of the Response

a. The solicitation is published in multiple parts.
   i. Part A contains the solicitation instructions, and the technical specifications.
   ii. Part B is the general terms and conditions for all AEPA agencies.
   iii. Part C includes specific state terms and conditions. This is where you will find information about each AEPA state member and any specific procurement rules of each state.
   iv. Part D is a required Questionnaire found and completed in Bonfire.
   v. Parts E and F are to be filled out in their entirety and submitted online via Bonfire in their required formats with the Respondent's offer. Some categories may request additional forms. All forms must be uploaded before the published solicitation due date and time of opening.

b. All responses must be on the forms provided by AEPA for each solicitation found in Bonfire unless otherwise noted. Respondents will submit all documents, in their required formats, online via Bonfire by the due date and time of the solicitation.

c. Forms requiring signatures must be submitted by the person authorized to sign the bid or proposal response. Failure to properly sign the solicitation documents may result in the offer being deemed non-responsive.

d. In case of an error in extension of prices in the solicitation, unit prices must govern.

e. Periods of time stated as a number of days must be in calendar days, not business days.

f. It is the responsibility of all Respondents to examine the entire solicitation package, to seek clarification of any item or requirement that may not be clear, and to check all responses for accuracy before submitting an offer. Negligence in preparing an offer confers no right of withdrawal after due time and date.

g. The Respondents' ability to follow the preparation instructions set forth in this solicitation will also be considered to be an indicator of the Respondents' ability to follow instructions should they receive an award as a result of this solicitation. Any contract between the AEPA Member Agency and a Respondent requires the delivery of information and data. The quality of organization and writing reflected in the offer will be considered to be an indication of the quality of organization and writing which would be prevalent if a contract was awarded. As a result, the offer will be evaluated as a sample of data submission.

2. **Document Development:** Forms for this solicitation are published in Bonfire, in Excel, and PDF formats. Some forms (questionnaire) may be completed directly in Bonfire. Respondents must scan and upload all documents to Bonfire following the Solicitation Checklist, along with any additional documents or files other than those listed below that may be requested and/or related to the solicitation.

   a. **Part C – Member Agency (State) Terms and Conditions:** Some states require additional documentation and signature forms. Review Part C and submit the required state documents with your offer. Submit all state-specific forms as one (1) form in PDF format.

   b. **Part D – Questionnaire:** Complete directly in Bonfire. The questionnaire seeks information about the Respondent's pricing structure, service areas, past

performance, and commerce processes. The Company Information form provides background information on the Respondent's company.

c. **Part E – Signature Forms**: Complete the forms provided. The signature form includes multiple areas where signatures are required. Submit the form as one (1) individual form in PDF format.

d. **Part F – Discount & Pricing Workbook:** Complete the Excel workbook provided. Title the Excel document as per the instructions in Document Development above. Be sure to complete the required tabs as outlined in Part F.

3. **Price Lists and/or Catalogs:** For catalog bids, Respondent's most recent catalog(s) or price lists must be included. If a hard copy is submitted, it should be in pdf format. Links to online pricing are acceptable as long as pricing is included, not just descriptions of product.

4. **Solicitation Transmittal**

a. It is the responsibility of the Respondent to be certain that its submittal has been uploaded in its entirety to Bonfire, on or prior to the exact published due date and time.

b. If a security bond is required (noted a the top of Part A), a hard copy of the security must be in the actual possession of, on or before, the exact due date and time and a copy must be submitted via Bonfire. Original copies of the security must be submitted in a sealed envelope properly addressed to the Association of Educational Purchasing Agencies, with the Solicitation Number, Solicitation Category, and Respondent's name and address clearly indicated on the envelope or box to AEPA c/o LCSC, ATTN: Purchasing Dept, 1001 E Mt Faith, Fergus Falls, MN 56537 in a sealed envelope. AEPA will not reject a response from a Vendor whose bid bond has not arrived by the due date and time as long as a scanned copy of the bid bond dated prior to the due date is uploaded with their response and the actual bond is in transit.

c. If the designated location for receiving the bid or proposal security is closed due to an unforeseen circumstance on the day the security is due (due date), the security will be due at the same time on the next day the building is open.

d. Responsive offers will be opened, and the name of each Respondent and other appropriate information will be posted on the AEPA website.

F. **Solicitation Evaluation, Approval, and Award:** Solicitation responses received will be evaluated in accordance with acceptable standards of cooperative procurement, set forth in and governed by the Procurement Codes of AEPA Member Agency's states; AEPA by-laws, policies, and procedures; AEPA Member Agencies' policies and procedures.

For IFB categories, approval of prospective Vendor Partners and recommendation of contracts will be made to the lowest responsive and responsible Respondent utilizing the criteria listed in this solicitation. As a reminder, AEPA recommends offers to Respondents. Final contract awards are subsequently made by individual AEPA Member Agencies.

1. **Responsive Offer:** A responsive offer reasonably and substantially conforms to all material requirements of the solicitation. Offers must be responsive and approved by AEPA to receive award consideration by AEPA Member Agencies. To be determined responsive, the response must meet all of the requirements below:

a. Submitted on time.

b. Materially satisfy all mandatory requirements identified throughout the solicitation.

c. Must substantially conform to all of the specified requirements in the solicitation in the judgment of AEPA and its AEPA Member Agency representatives.

d. Any deviation from requirements indicated herein must be stated, in writing, and included with the offer submitted. Otherwise, it will be considered that responses

are in strict compliance with all requirements, and any successful vendor will be held responsible, therefore.

e. Deviations or exceptions stipulated in response may result in the offer being classified as non- responsive. Language to the effect that the Respondent does not consider this solicitation to be part of a contractual obligation will result in that Respondent's offer being disqualified. Terms of the solicitation that any Respondent considers particularly unwarranted, and to which that would have to take significant exception in his/her offer, should be stated clearly and concisely as exceptions and/or deviations.
f. In preparing a proposal, the Respondent's inability to follow the proposal preparation instructions set forth in this solicitation and its inability to provide written responses, narratives, requested and support documentation relating to the Respondent's qualifications; abilities; capacity; products; specifications; delivery, installation, setup, maintenance; support services and pricing utilized by AEPA evaluators may result in the Respondent's offer to be deemed non-responsive.

2. **Non-responsive Offer:** Any offer that does not conform to all material requirements of the solicitation including, but not limited to: offers received after the deadline; offers that do not contain required items and/or provided in the format required, such as proper and/or signed forms, pricing, catalogs, electronic files; offers that do not contain the proper security bond where required; failure to meet the specified qualifications, product specifications, stipulated documentation or pricing equal to or better than individual entities or cooperatives with equal or lesser volume. AEPA reserves the right to request documents that do not affect pricing, waive minor irregularities, and/or seek clarification following its Board approved procedures. Offers deemed non-responsive will not be considered for approval and award.

3. **Responsible Respondent:** A responsible Respondent is a firm or person with the qualifications, capability, and capacity to perform the contract requirements with integrity and reliability, which will assure good faith performance. As a part of the process of determining responsible respondents during the evaluation period, the category committee may request reports that describe the financial soundness of your organization. You may be asked to include a third-party report or reports that demonstrate your firm's strength. Accepted financial reports may include balance sheets and Profit & Loss statements for the past three years, a Letter of Credit or Line of Credit from a bank or lending institution indicating the line of credit limit and the average outstanding balance, Dun & Bradstreet reports, a complete Annual Financial Report (for publicly traded companies).

   AEPA's approval of a response will make the Respondent available for consideration to the AEPA Member Agencies for contract award. Factors to be considered in determining whether the standard of responsibility has been met may include but is not limited to whether a Vendor Partner has:

   a. Submitted a responsive offer;
   b. The qualifications stipulated in this solicitation, such as adequate financial resources, production or service facilities, personnel, service reputation and experience to make satisfactory delivery of the products, services, or construction;
   c. A demonstrated and documented satisfactory track record of performance in the national marketplace;
   d. A satisfactory record of integrity and a reputation of responding to and meeting educational and local government institutions' needs, adherence of and compliance with federal, state, local and industry standards, rules, regulations, and codes;
   e. Quality and suitability of products and services offered to meet and perform to the specifications, expectations, and requirements identified in this solicitation;

f. Supplied all necessary information and data in connection with determining whether a Respondent meets the standard of responsibility.

4. Cost Evaluation:

a. Cost and price schedules conform to and provide the information required in this part of the bid or proposal;
b. Pricing offered that is equal to or better than what they ordinarily offer to individual entities or cooperatives with equal or lesser volume;
c. Methodology used by AEPA and its AEPA Member Agencies to approve prospective Vendor Partners and award contracts;
   i. Line-Item/Construction Bid: Lowest responsive, responsible Bidder(s). Based on the cost evaluation, a recommendation will be made to approve a single Bidder or make a multiple Bidder award. The evaluation committee may consider such factors as life-cycle costs, total cost of ownership, quality, and the suitability of an offering in meeting AEPA members' needs; or
   ii. Catalog Bid: Lowest responsive, responsible Bidder(s) is/are determined based on the price evaluation criteria; and by a "Core List" and/or by creating a "Market Basket Study" to compare overall pricing between Respondents. A "Market Basket" is a list of items typically purchased by AEPA Member Agencies and their Participating Entities that represent a cross-section of the types of those items purchased. The selection and quantity of line items evaluated will be at the sole discretion of the AEPA evaluators. Based on the cost evaluation, a recommendation will be made to approve a single Bidder or make a multiple Bidder award. The evaluation committee may consider such factors as life-cycle costs, total cost of ownership, quality, and the suitability of an offering in meeting AEPA members' needs.
   iii. Proposal: Identified weighted criteria for evaluation, including pricing, published in this part of the solicitation.

G. Contract Award and Implementation

An AEPA category committee will perform initial response review and evaluation and will prepare and make a recommendation to AEPA for its consideration and approval. Those selected Respondents who are approved by AEPA will then be considered by the individual AEPA Member Agencies for contract award. It should be noted that once AEPA has approved the response, a Respondent becomes a "Vendor Partner" for AEPA.

All respondents will be notified of the outcome of the solicitation. Vendors recommended for award by AEPA states will be posted on the AEPA website.

Once the approved Respondents have been notified, it is their responsibility to contact those AEPA Member Agencies (up to 30) who had indicated an interest in participating and sending them Part E Signature Forms with the contract for each state to complete. Each AEPA Member Agency will review, evaluate, and determine which, if any, it will award contracts to.

The approved Vendor Partner and the AEPA Member Agency will hold final contract negotiations, if necessary, to work out state-specific details of contract implementation including:

1. Acquiring additional information and having discussions on how the awarded contract will be executed.
2. Signing the contract with the AEPA Member Agency.
3. Jointly develop marketing strategies and a plan for contract roll-out activities to the AEPA Member Agency's Participating Entities (Advertising, flyers, website access, etc.).
4. Establish how orders will be processed, handled, and reported.

5. Contract management: Establish how and by whom the day-to-day contract management will be handled and who will be the AEPA Member Agency's representative.

It is not guaranteed that each AEPA Member Agency will enter into a contract with AEPA approved Vendor Partners. The final decision as to the appropriateness of a contract for a Member Agency rests solely with that AEPA Member Agency.

II. Responsibilities of a Vendor Partner

A. As an approved AEPA Vendor Partner, the following is expected in support of the contract:
   1. Designate and assign a dedicated senior-level contract manager (one authorized to make decisions) to each of the Member Agency accounts. This employee will have a complete copy and must have a working knowledge of the contract.
   2. Train and educate sales staff on what the AEPA cooperative contract promised, including pricing, who can order from the contract (by state), terms/conditions of the contract, and the respective ordering procedures for each state. It is expected that Vendor Partners will lead with AEPA contracts.
   3. Develop a marketing plan to support the AEPA contract in collaboration with respective AEPA Member Agencies. The plan should include, but not be limited to, a website presence, electronic mailings, sales flyers, brochures, mailings, catalogs, etc.
   4. Create an AEPA-specific sell sheet with a space to add a Member Agency logo and contact information for use by the Member Agencies and the Vendor Partner's local sales representatives to market within each state.
   5. Quarterly, complete the sales and administrative fee report (see attached PDF example) and submit to each Member Agency along with the respective administrative fees to be paid. If there are no sales, a $0 report is required.
   6. Report sales and administrative fees by participating state if requested by AEPA.
   7. Have ongoing communication with the Category Committee Chairperson, AEPA Member Agencies, and the Member Agencies Participating Entities.
   8. Annually attend two (2) AEPA meetings: Annual meeting which is typically in April or May and the Winter Meeting which is typically the week after Thanksgiving and has historically been held in conjunction with the Association of Educational Service Agencies (AESA) annual conference. At the Annual Meeting, Vendor Partners participate in a round table meeting with each of the AEPA Member Agencies. Vendor Partners that have paid the registration fees can participate in the meetings.
   9. Trade show support: Strongly encourage participation in national and local conference trade shows to promote the AEPA contracts such as, but not limited to, the Association of School Business Officials (ASBO), the National Institute of Governmental Purchasing (NIGP), and the National Association of Educational Procurement (NAEP).
   10. Increasing sales over the term of the contract with all participating AEPA Member Agencies.

III. Responsibilities of AEPA Member Agencies

A. In support of the Vendor Partner and respective contract, each AEPA Member Agency should provide the following support:
   1. Designate a staff member(s) that will serve as a point person for the AEPA program within that state.
   2. Provide a staff member to work collaboratively with the Vendor Partner to determine the best marketing plan for the respective Member Agency state. Marketing efforts may include but not be limited to the education and use of sales force, a website presence, electronic mailings, brochures, mailings, etc.
   3. Develop marketing materials for the Member Agency to use that would include representation of the awarded contracts. Materials may include, but not be limited to, a website presence, electronic mailings, sales flyers, brochures, mailings, catalogs, etc.

as determined by the respective Member Agency and what works best within their state.

4. Assist the Vendor Partner to jointly market the contract to potential Participating Entities within the state.
5. Work with the Vendor Partner to identify eligible Participating Entities within the state possibly including providing a list of potential customers.
6. Work with the Vendor Partner to identify and help manage costs associated with fulfilling this contract.
7. Attendance at the two (2) AEPA meetings which provides for an opportunity to interact with Vendor Partners.

IV. Category Specifications

1. Scope of Work

AEPA is seeking qualified, experienced contractor(s) who possess the necessary resources and technical capabilities to acquire, deliver and perform the required services, supplies, materials, equipment and labor to all participating member states (up to 30) in the category of Cyber Security & Training. Qualified vendors will be able to provide comprehensive cyber security services to members to include PK-12 educational, Higher Education Institutions and other public institutions. The selected vendor(s) will deliver a range of cyber security solutions aimed at protecting the organization's information assets and training staff on best practices to ensure a robust security posture.

a. Vendors may respond in part but are not limited to the following categories: Cyber Security Assessment and Planning; Network Security; Endpoint Security; Data Security; Identity and Access Management; Cloud Security; Security Monitoring and Incident Response; Cyber Security Training (Employee Training Programs and Phishing Simulations); Compliance and Reporting .
b. Types of services may include, but are not limited to the following services:
    a. Cyber Security Assessment and Planning
        i. Initial Security Assessment:
            1. Conduct a comprehensive assessment of the current security posture.
            2. Identify vulnerabilities, threats, and risks in a member's IT environment.
        ii. Security Plan Development:
            1. Develop a detailed security plan based on the assessment findings.
            2. Define security policies, procedures, and controls to mitigate identified risks.
            3. Provide recommendations for improvements and enhancements.
    b. Implementation of Security Measures
        i. Network Security:
            1. Implement firewalls, intrusion detection/prevention systems (IDS/IPS), and VPNs.
            2. Ensure secure network architecture and segmentation.
        ii. Endpoint Security:
            1. Deploy and manage anti-virus/anti-malware solutions.
            2. Implement endpoint detection and response (EDR) tools.
        iii. Data Security:
            1. Implement data encryption, both at rest and in transit.
            2. Establish data loss prevention (DLP) measures.
        iv. Identity and Access Management (IAM):
            1. Implement multi-factor authentication (MFA).
            2. Manage user access controls and permissions.
        v. Cloud Security:
            1. Ensure secure configuration and management of cloud services.
            2. Implement cloud-specific security measures and monitoring.

c. Security Monitoring and Incident Response
    i. Continuous Monitoring:
        1. Set up and manage a Security Information and Event Management (SIEM) system.
        2. Conduct regular vulnerability scanning and penetration testing.
    ii. Incident Response Plan:
        1. Develop and implement an incident response plan.
        2. Provide 24/7 incident response services.
        3. Conduct incident response drills and tabletop exercises.
d. Cyber Security Training
    i. Employee Training Programs:
        1. Develop and deliver cyber security awareness training for all employees.
        2. Conduct specialized training for IT staff and security teams.
    ii. Phishing Simulations:
        1. Conduct regular phishing simulation exercises.
        2. Provide feedback and additional training based on simulation results.
e. Compliance and Reporting
    i. Regulatory Compliance:
        1. Ensure compliance with relevant regulations such as GDPR, HIPAA, etc.
        2. Conduct regular audits and assessments to maintain compliance.
    ii. Reporting:
        1. Provide regular reports on security posture, incidents, and mitigation efforts.
        2. Deliver executive summaries and detailed technical reports as needed.

c. Deliverables
    a. Initial security assessment report.
    b. Comprehensive security plan.
    c. Implementation of security measures and configurations.
    d. Incident response plan and execution.
    e. Regular monitoring and vulnerability assessment reports.
    f. Training materials and records of completed training sessions.
    g. Compliance audit reports.
d. Vendor Qualifications
    a. Proven experience in delivering comprehensive cyber security services.
    b. Certified professionals (e.g., CISSP, CISM, CEH).
    c. Strong track record with references from similar projects.
    d. Capability to provide 24/7 support and incident response.
e. Budget
    a. Vendors should provide a detailed budget breakdown including:
        i. Initial assessment costs.
        ii. Implementation costs.
        iii. Ongoing support and maintenance fees.
        iv. Training program costs.
f. Proposal Submission Requirements
    a. Company profile and relevant experience.
    b. Detailed approach and methodology.
    c. Project plan with timelines.
    d. Cost proposal.
    e. References from similar projects.
g. Evaluation Criteria
    a. Technical expertise and experience.
    b. Quality and comprehensiveness of the proposal.
    c. Cost-effectiveness.

d. References and past performance.
e. Ability to meet project timelines.

By detailing the scope of work comprehensively, this RFP aims to attract qualified vendors who can enhance the Association of Educational Purchasing Agency Member's' cyber security posture effectively and efficiently.

All products offered must be considered new, unused, of the latest design and technology and from the most current and popular product lines available.

2. Anticipated AEPA Member Agency Participation

State	Participate? Yes/No/ Undecided	Other States Member Sells In
California	Yes	AZ, NV
Colorado	Yes	
Connecticut	Yes	ME, NH, NY, RI, VT
Florida	Yes	AL
Georgia	Yes	
Illinois	Yes	
Indiana	Yes	
Iowa	Yes	SD
Kansas	Yes	OK
Kentucky	Yes	AL, LA, MS, NC, TN
Massachusetts	No	
Michigan	Yes	
Minnesota	Yes	
Missouri	Yes	AR, LA, SD
Montana	Yes	ID
Nebraska	Yes	
New Jersey	Undecided	
New Mexico	Yes	
North Carolina	Yes	
North Dakota	Yes	
Ohio	Yes	
Oregon	Yes	
Pennsylvania	No	DE, HA, MD, NY
South Carolina	Yes	
Texas	Yes	
Virginia	Undecided	
Washington	Yes	AK, ID
West Virginia	Yes	
Wisconsin	Yes	
Wyoming	Yes	SD,UT

Please note that individual AEPA Member Agencies that have indicated that they intend to participate in any contract approved under this solicitation, does not guarantee or mean that the individual AEPA Member Agency will enter into a contract with any AEPA approved Vendor Partner. Each AEPA Member Agency will make that determination after reviewing Vendor Partner responses and AEPA's recommendation for acceptance and award. The AEPA Member Agency's contracting decision shall be final.

3. Anticipated Volume

Cyber Security & Training is a new category for AEPA. The resulting award will be an Indefinite Delivery,

Indefinite Quantity (IDIQ) contract(s). AEPA Member Agencies estimate approximately $4.5 million in sales in the first contract term. AEPA Member Agencies anticipate that purchase volumes will increase over the course of contract years two (2) through four (4). This information is provided as an aid to Respondents in preparing responses only. It is not to be considered a guarantee of volume under this RFP. The successful Vendor Partner's discount and pricing schedule shall apply regardless of the volume of business under the contract.

4. Voluntary Pre-Solicitation Conference Call

AEPA will host a voluntary pre-solicitation conference call for any interested Bidders or potential Bidders. The conference call times are set in the following schedule for each of the four contiguous United States time zones. No pre-registration will be required. Recording of the conference call will be posted on the AEPA Website.

Voluntary Pre-Solicitation Conference Call Schedule (All RFP Categories)

Solicitations	Date	Eastern	Central	Mountain	Pacific
AEPA 025 Voluntary Pre-Bid Conference Call - All RFP Categories	Mon Aug 19 2024	2:00 PM	1:00 PM	12:00 PM	11:00 AM

Conference Call Meeting Link:

https://us02web.zoom.us/j/81346015848?pwd=mcy1LR3uWAsWj8v86aBaOEDuA9y9XE.1

Meeting ID: 813 4601 5848
Passcode: 274yRg

Dial In Information:
- +1 301 715 8592 US (Washington DC)
- +1 305 224 1968 US

Meeting ID: 813 4601 5848
Passcode: 738244

5. Glossary of Terms and Abbreviations

Abbreviations and Acronyms for Standards and Regulations: Where abbreviations and acronyms are used in specifications or other contract documents, they shall mean the recognized name of the organizations responsible for the standards and regulations in the following list. Names, telephone numbers, and websites are subject to change and are believed to be accurate and up-to-date as of the date of the contract documents.

a. CRP - Cyber Resilience Program: A strategic and comprehensive approach designed to prepare, protect, respond to, and recover from cyber threats and disruptions.
b. Access Control: Mechanisms that restrict access to data or systems based on policies, ensuring only authorized users can access certain information.
c. Advanced Persistent Threat (APT): A prolonged and targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period.
d. Botnet: A network of infected devices controlled by an attacker to perform coordinated tasks, such as launching Distributed Denial of Service (DDoS) attacks.
e. Brute Force Attack: A method of hacking that involves trying all possible combinations to crack a password or encryption key.
f. Cyber Hygiene: Practices and steps that users take to maintain system health and improve online security, like regularly updating software and using strong passwords.

g. Cryptography: The practice of securing information by transforming it into an unreadable format, only reversible with a decryption key.
h. Data Breach: The unauthorized access and retrieval of sensitive information from a system or network.
i. Denial of Service (DoS): An attack that aims to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests.
j. Encryption: The process of converting information or data into a code to prevent unauthorized access.
k. Endpoint Security: Protecting network endpoints (such as desktops, laptops, and mobile devices) from cyber threats.
l. Firewall: A network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules.
m. Forensics: The application of investigative techniques to gather and preserve evidence from a computer system or network in a manner suitable for presentation in a court of law.
n. Governance, Risk, and Compliance (GRC): A strategy for managing an organization's overall governance, risk management, and compliance with regulations.
o. Honeypot: A security mechanism set to detect, deflect, or counteract attempts at unauthorized use of information systems by mimicking a real system.
p. Hash Function: A function that converts an input (or 'message') into a fixed-length string of bytes, typically for securing data integrity.
q. Identity and Access Management (IAM): A framework of policies and technologies to ensure that the right individuals access the right resources at the right times for the right reasons.
r. Incident Response: The approach taken by an organization to prepare for, detect, contain, and recover from a data breach or cyber attack.
s. Keylogger: A type of surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard.
t. Least Privilege: A principle that prescribes minimal user profile privileges on computers, based on users' job necessities, to prevent unauthorized access to sensitive information.
u. Malware: Malicious software designed to harm, exploit, or otherwise compromise a computer system. Examples include viruses, worms, and Trojan horses.
v. Multi-Factor Authentication (MFA): A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity.
w. Network Security: The practice of protecting a computer network from intruders, whether targeted attackers or opportunistic malware.
x. Penetration Testing: A simulated cyber attack against a computer system to check for exploitable vulnerabilities.
y. Phishing: A technique used by cybercriminals to trick individuals into providing sensitive information by pretending to be a trustworthy entity.
z. Quarantine: The isolation of files or programs that are suspected to be infected with malware to prevent further spread.
aa. Ransomware: A type of malware that encrypts a victim's files and demands payment (ransom) to restore access to the data.
bb. Risk Assessment: The process of identifying, analyzing, and evaluating risks to the organization's assets and operations.
cc. Security Information and Event Management (SIEM): A set of tools and services offering a holistic view of an organization's information security.
dd. Social Engineering: Manipulating people into performing actions or divulging confidential information through psychological manipulation.
ee. Two-Factor Authentication (2FA): A security process that requires two separate forms of identification to access a resource, enhancing security.
ff. Unified Threat Management (UTM): A security solution that provides multiple security functions within a single platform, such as firewall, antivirus, and intrusion detection.

gg. User Behavior Analytics (UBA): The process of tracking user behavior within a network to identify potentially malicious actions by users.
hh. Virtual Private Network (VPN): A service that creates a secure, encrypted connection between a user's device and a network, often used to protect data transmitted over public networks.
ii. Vulnerability: A weakness in a system, application, or network that can be exploited by a threat actor to perform unauthorized actions.
jj. Whitelisting: A security approach that allows only pre-approved applications, IP addresses, or other entities to access a system or network.
kk. XSS (Cross-Site Scripting): A type of security vulnerability found in web applications where an attacker can inject malicious scripts into content from otherwise trusted websites.
ll. Zero-Day Exploit: An attack that targets a previously unknown vulnerability in a software application, hardware, or firmware, before the developer has released a fix.
mm. Zero Trust: A security concept and framework that assumes that threats could be inside and outside the network, and thus, every access request must be verified, regardless of its origin.

6. Product | Category Specific Specifications

Item	Description
6.1.1	**Network Security** (e.g., Firewall Management, Intrusion Detection and Prevention, Virtual Private Network)
6.1.2	**Endpoint Security** (e.g., Antivirus, Antimalware, Endpoint Detection and response, Mobile Device Management, Patch Management)
6.1.3	**Application Security** (e.g.,Web Application Firewall, Secure Coding Practices, Application Vulnerability Scanning, Software Composition Analysis)
6.1.4	**Data Security** (e.g., Data Encryption, Data Loss Prevention, Backup and Recovery Solutions, Database Security)
6.1.5	**Identity and Access Management** (e.g.,Single Sign-On, Multi-Factor Authentication, Privileged Access Management, Identity Governance and Administration)
6.1.6	**Threat Intelligence** (e.g., Threat Intelligence Platforms, Cyber Threat Analysis, Incident Response, Threat Hunting)
6.1.7	**Penetration Testing**
6.1.8	**Security Audits**
6.1.9	**Security Operations Center** (e.g., SOC as a Service (SOCaaS), Security Information and Event Management (SIEM), Managed Detection and Response (MDR), Incident Management)
6.1.10	**Cloud Security** (e.g., Cloud Access Security Broker (CASB), loud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPP), Secure Cloud Configuration)
6.1.11	**Compliance and Risk Management** (e.g., Compliance Frameworks (e.g., GDPR, HIPAA, PCI-DSS), Risk Assessment and Management, Security Audits and Assessments, Policy Development and Management)
6.1.12	**Physical Security** (e.g., Security of Physical Assets, Access Control Systems,Surveillance Systems, Environmental Controls)
6.1.13	**Cyber Security Insurance**
6.1.14	**User Awareness** (e.g.,Phishing Simulation and Training,General Cyber Security Awareness Programs, Role-Based Training (e.g., executives, developers), Social Engineering Awareness)
6.1.15	**Technical Training** (e.g. Advanced Persistent Threat (APT) Detection, Malware Analysis and Reverse Engineering, Network Security Monitoring, Incident Response and Forensics)
6.1.16	**Compliance and Regulatory Training** (e.g. Data Protection Regulations, Industry-Specific Compliance Training, Legal and Ethical Aspects of Cyber Security, Governance, Risk, and Compliance (GRC) Training)
6.1.17	**Certification and Professional Development** (e.g. Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA))
6.1.18	**Simulation and Hands on Training** (e.g. Cyber Range Exercises, Red Team vs. Blue Team Exercises, Capture the Flag (CTF) Challenges, Real-World Scenario Simulations)

Item	Description
6.1.19	**Executive and Board Training** (e.g. Cyber Security Strategy and Governance, Crisis Management and Incident Response for Executives, Board-Level Cyber Security Briefings, Risk Management for Senior Leaders)
6.1.20	**Developer Security Training** (e.g. Secure Coding Practices, DevSecOps Integration, Code Review and Analysis, Application Security Testing)
6.1.21	Proposer should use IT industry standards to perform any assessments, including vulnerability **assessments and penetration testing**
6.1.22	Pursuant to federal and state law, the Company hereby certifies that: (1) the Company is not a "scrutinized company" (as defined by state and federal law); (2) the Company will not subcontract with any "scrutinized company" for any aspect of the performance of this Agreement; and (3) that any products or services to be provided under this Agreement do not originate with any "scrutinized company.

7. Pricing

AEPA has identified acceptable pricing methodologies that are to be utilized to submit pricing. Pricing strategy descriptions are found in Part A – AEPA Instructions and General Terms and Conditions. We request that the pricing response contain sufficiently detailed information to determine a realistic cost for AEPA member agencies. The Vendor Partner agrees that the cost for any item offered on this contract will be uniform for all states, and that any differences in pricing are due to state specific installation and labor costs, AEPA Member Agency's Administrative Fee, or other approved reasons. The respondent must provide their pricing as requested utilizing the various pricing methodologies specified. **The Vendor Partner must agree that they will offer prices equal to or better than what they ordinarily offer to individual entities or cooperatives with equal or lesser volume.**

AEPA is expecting pricing on the vendor's entire offering under the scope of this solicitation. Proposers are encouraged to offer optional pricing strategies ("Hot List", Volume discounts, Customized Price Lists, Specials), and additional financing options.

For services, vendors may respond with a discount off labor and material costs. Labor must be sufficiently itemized by title and include total rate (salary and fringe). Material costs must be itemized. Any Vendor Partner awarded under a time and materials pricing strategy must provide a "not to exceed" project quote to the purchasing Agency for work approval.

AEPA requires that pricing be returned using the Part F Excel Forms provided, or in an Excel format that contains the information requested in Part F.

8. Part F - Pricing Workbook

a. Pricing shall be completed on the provided pricing sheets (Microsoft Excel Workbook) with the individual tables to be completed as follows:
   i. F.1 – Catalog Discounts (Required)
   ii. F.2 - Price Schedule (Required)
   iii. F.3 – Services Price Schedule (Optional)
   iv. F.4 – Volume Discounts (Optional)

b. Pricing will be evaluated on a combination of items from all pricing schedules. Pricing evaluation may include other considerations, including the total cost of the acquisition and whether the Proposer's offering represents the best value. See Evaluation, Approval and Award in Part A – Terms and Conditions for additional information.

9. Evaluation

The AEPA Committee for this category will evaluate proposals based on the entire response, and according to the criteria detailed in Part A for AEPA's definition of Responsive and Responsible proposals.

A recommendation may be made to recommend a single response, or to recommend multiple offers based on differentiation of product or service. AEPA will vote as a whole to accept or not accept a committee's recommendation. Once accepted, each recommended response will go to the individual states for contract approval. Please note, pricing evaluation may include other considerations, including the total cost of the acquisition and whether the Proposer's offering represents the best value. The evaluation committee may consider such factors as life-cycle costs, total cost of ownership, quality, and the suitability of an offering in meeting AEPA members' needs.

Criteria	**Yes/No**
Complete Response to Solicitation	
Financial Viability	
Ability to provide good/services to 90% of participating agencies.	
Criteria	**Points**
Conformance to Terms and Conditions	5
Pricing EQUAL TO or BETTER THAN offered to individual entities or cooperatives with Equal or Lesser Volume	6
Quality and Suitability of Products, Services & Solutions Offered	5
Marketing Plan	5
Demonstrated Track Record of Performance in the Public Marketplace (may include reference checks)	5
Value Added Attributes	5
Comprehensive Coverage and Threat Protection	6
User Education, Awareness, Dashboard, Reporting Tools, Compliance and Regulatory Support	6
Incident Response, Recovery, Integration and Interoperability	6
Total Score - Technical	**49**
Cost Evaluation	51
Total Scores	**100**

Part E – Signature Forms

AEPA 025-F
Cyber Security and Training

Instructions

Contained herein are forms that **require a signature** from an authorized person at your company. All items found within this document are **mandatory**. Failure to sign the required areas, sections, or signature lines may lead AEPA to consider your company's proposal as **non-responsive**.

To submit the required signed forms, follow these steps:

1. Read the documents in their entirety.
2. Complete all forms and sign when required.
3. Return the forms and pages in their correct order and scan one (1) single PDF format titled ***"Part E – Signature Forms – Name of Responding Company"*** (i.e. one PDF document for all signature forms).
4. Submit Part E, along with other required documents in Bonfire.

*Note, a solicitation checklist has been provided to review with your submission.

The following sections will need to be completed prior to submission as one (1), single PDF titled "Part E – Signature Forms – Name of Responding Company".

Uniform Guidance "EDGAR" Certification Form – ****signature required***
Solicitation Affidavit – ****signature required***
Acceptance of Solicitation & Contract – ****signature required***

Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7. Clean Air Act and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended, contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein.		
Respondent Certification (By Item)	**Respondent Certification:** **YES**, I agree	**Initial**
1. Violation of Contract Terms and Conditions		
2. Termination for Cause of Convenience		
3. Equal Employment Opportunity		
4. Davis-Bacon Act		
5. Contract Work Hours and Safety Standards Act		
6. Right to Inventions Made Under a Contract or Agreement		
7. Clean Air Act and Federal Water Pollution Control Act		
8. Debarment and Suspension		
9. Byrd Anti-Lobbying Amendment		
10. Procurement of Recovered Materials		
11. Profit as a Separate Element of Price		
12. General Compliance with Participating Agencies		
13. Governing Law; Forum Selection.		

_____
Name of Business

_____
Signature of Authorized Representative

_____
Printed Name

_____
Date

Solicitation Affidavit

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

Authorized Representative (Please print or type)	Mailing Address
Title (Please print or type)	City, State, Zip
Signature of Authorized Representative	Date

Acceptance of Solicitation & Contract

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name		**Date**	
Address		**City, State Zip**	
Contact Person		**Title**	
Authorized Signature		**Title**	
Email		**Phone**	

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Solicitation Checklist

Instructions: Utilize the checklist below, reviewing to confirm that all the required documents have been uploaded to Public Purchase, in their ***specified/required format***, by the due date and time listed for this solicitation. ***Submissions not following the specified/required format may result in being marked non-responsive and may not be considered for evaluation.*** Respondents are reminded that failure to follow, comply with, and adhere to the enclosed instructions of this solicitation may result in their response being deemed non-responsive. AEPA, its Member Agencies, affiliate agencies, and authorized representatives are not responsible for bid proposals that are incomplete, unreadable, or received after the solicitation deadline submission date.

"x"	**Document Title, Uploaded to Bonfire** *(Respondent must submit documents in the required title/format)*	**Format of Uploaded Document**	**Notes**
	Bid Bond – if Required, see Part A if applicable.	Upload PDF copy of the bid security.	The original bid security must be received by Lakes Country Service Cooperative by due date and time.
	Part C – State-Specific Forms – ***Name of Responding Company***	Single, Scanned PDF	**New Jersey Only Requirement.** Signatures Required.
	Part D - Questionnaire – ***Name of Responding Company*** Includes: ● Company Information ● Service Questionnaire ● Exceptions ● Deviations	Single, Scanned PDF	**Required.**
	Part E – Signature Forms – ***Name of Responding Company*** Includes: ● Uniform Guidance "EDGAR" Certification ● Solicitation Affidavit ● Acceptance of Solicitation & Contract	Single, Scanned PDF	**Required.** Signatures required.
	Part F – Pricing Schedule – ***Name of Responding Company***	Excel Workbook	**Required.**
	Price List and/or Catalog – ***Name of Responding Company***	Upload PDF	**Required.**
	Exhibit A – Marketing Plan – ***Name of Responding Company***	Scanned PDF	**Optional.** Form not provided by AEPA, Respondent Created

Part F.1 – Catalog Discount for Items in a Commercially Available Catalog

AEPA #025-F Cybersecurity

Bidding Company Name: *Enter company name here*

Name of Catalog: *Enter catalog name here*

Note: Groupings to be defined by Bidder and can be by sub-category, manufacturer, etc.

Part F.1 is a REQUIRED FORM

No.	Grouping of Discount	Discount Offered for	Comments
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			

If more categories are needed, add a new tab with similar formatting.

Public Q&A

#14 - Exhibit A - Marketing Plan

SHI, Aug 13, 2024 11:29 AM EDT, Not Public - Pending
We are required to upload a Marketing Plan as Exhibit A. We do not see any reference to Exhibit A within the customer documents. Is there a certain format that must be followed? Is there specific information that you would like to see in this Marketing Plan?
Jane Eastes, Aug 27, 2024 6:37 AM EDT, Public - Answered
AEPA believes the marketing partnership between the Vendor Partner and State Member is critical to the success of the contract. Describe ways in which your company will collaborate with AEPA Member Agencies in marketing the resulting contract. The AEPA Questionaire (Part D) asks several questions about marketing. We are also looking for a more detailed description of the resources you have to go to market and the plan you have used and intend to use to reach AEPA participating members with details of your offerings as an AEPA awarded vendor • Process on how the contract will be launched to current and potential agencies. • The ability to produce and maintain in full color print advertisements in camera-ready electronic format, or electronic advertisements, including company logos and contact information. • Anticipated contract announcements, planned advertisements, industry periodicals, other direct or indirect marketing activities promoting the AEPA awarded contract. • How the contract award will be displayed/linked on the Respondent's website. Your response should be uploaded as a separate PDF and titled Exhibit A – Marketing Plan.

#17 - Administrative Fee

Clever, Aug 19, 2024 2:26 PM EDT, Not Public - Pending
Does the vendor have to pay BOTH AEPA and a state/regional cooperative a 2% transaction fee (so 4% total) or is it ONLY 2% to AEPA?
Jane Eastes, Aug 27, 2024 7:24 AM EDT, Public - Answered

No, the vendor does not have to pay Both AEPA and the AEPA State Member. The administrative fee is 2% and is paid to the AEPA participating state member who has signed a contract with the Vendor Partner.

#30 - Entering into an Agreement with AEPA

Clever, Aug 19, 2024 2:32 PM EDT, Not Public - Pending
Does entering into a cooperative agreement with AEPA disallow a vendor from working directly with districts or entities who also partner with AEPA in cases where the partner is willing to sign a contract directly with a vendor w/o an RFP or any contractual negotiating?
Jane Eastes, Aug 29, 2024 4:37 PM EDT, Public - Answered
AEPA participating districts or entities are able to use the contract awarded by the AEPA State Agency without doing their own agency solicitation. Once awarded by a state, the vendor then works directly with the participating district or entity to complete a sale using the contractual pricing in the AEPA contract.

#12 - Required Exhibit A: Marketing Plan

Network Technology Partners, Aug 20, 2024 2:01 PM EDT, Not Public - Pending
What components should be included in the required document, "Exhibit A: Marketing Plan" that is worth five points on the criteria scoring sheet?
Jane Eastes, Aug 27, 2024 6:35 AM EDT, Public - Answered
AEPA believes the marketing partnership between the Vendor Partner and State Member is critical to the success of the contract. Describe ways in which your company will collaborate with AEPA Member Agencies in marketing the resulting contract. The AEPA Questionaire (Part D) asks several questions about marketing. We are also looking for a more detailed description of the resources you have to go to market and the plan you have used and intend to use to reach AEPA participating members with details of your offerings as an AEPA awarded vendor. Examples of what we are looking for include: • Process on how the contract will be launched to current and potential agencies. • Process for ongoing communications with AEPA State lead agencies regarding marketing.

- The ability to produce and maintain in full color advertisements in camera-ready electronic format including company logos and contact information.
- Anticipated contract announcements, planned advertisements, industry periodicals, other direct or indirect marketing activities promoting the AEPA awarded contract.
- How the contract award will be displayed/linked on the Respondent's website.
- Continuous outreach efforts, including attendance at national or state conferences, email and social media campaigns, etc.

Your response should be uploaded as a separate PDF and titled Exhibit A – Marketing Plan.

#11 - Pre-bid zoom recordings

Network Technology Partners, Aug 21, 2024 12:27 PM EDT, Not Public - Pending

Can you please direct me to recordings of the two pre-bid meetings that took place on 8/19? Thanks

Jane Eastes, Aug 27, 2024 6:25 AM EDT, Public - Answered

We have made available the materials from the recent AEPA 025 pre-solicitation calls. You can now access the PowerPoint PDFs used during the calls, as well as the recording of the session. The PowerPoints are hosted on Bonfire and the call recordings are hosted on YouTube

Materials Available:

- PowerPoint PDFs
- Recording of the Call - https://youtu.be/00HGv_2kmT0

#33 - Product listing and pricing

Varmoda Tech LLC, Aug 22, 2024 3:59 AM EDT, Not Public - Pending

Regarding the AEPA RFP, is the focus primarily on providing products, services, or both? Are we required to list specific products that we intend to offer under this contract, or is the emphasis solely on the services we provide?

For the pricing section of the proposal, is AEPA requesting pricing for our products, services, or a combination of both? Could you clarify the expectations for how we should structure our pricing submission?

Jane Eastes, Aug 29, 2024 5:00 PM EDT, Public - Answered

For Cybersecurity Solutions:

To clarify the expectations for the AEPA RFP, is on providing both products and/or services.

- Products: If your RFP response is focused on products, you will be expected to detail the specific products you intend to offer, including their features, benefits, and pricing.
- Services: If your RFP response is focused on services, the emphasis would be on describing the scope of services, methodologies, and expertise your company can provide, along with the associated costs.
- Both: If the RFP response is for both products and services, your proposal should clearly differentiate between the two, detailing the specific products you'll offer as well as the related services, such as implementation, support, and maintenance.

#32 - Category F Cyber Security and Training References 1.10.1

SHI, Aug 22, 2024 5:45 PM EDT, Not Public - Pending

can references be provided for customer outside of our top 5 largest public entity customers (in case they aren't able to serve as a reference for any reason)?

Jane Eastes, Aug 29, 2024 4:55 PM EDT, Public - Answered

For Cybersecurity Solutions Category:

Please select references that best showcase your expertise in delivering cybersecurity solutions, particularly those with experience in K-12, higher education, and municipal sectors. These references should be able to provide valuable insights into your capabilities and past performance, even if they fall outside of your top five largest public entity customers.

#37 - Query

CCS Global Tech, Aug 26, 2024 4:13 PM EDT, Not Public - Pending

Q1: Regarding the F.1 Catalog Discounts Sheet, if we don't have a commercial catalog but have all our courses listed on our website, how should we present this in the Catalog Discount sheet?

Q2: For F.3, are we expected to present the costs per participant or per class? Additionally, how should we present per diem and mileage charges for onsite training delivery across 30 different states that will be ordering the services?

Jane Eastes, Aug 30, 2024 12:00 PM EDT, Public - Answered

For Cybersecurity Solutions Category:

Q.1 Response:

Since you do not have a commercial catalog and list all your courses on your website, please follow these guidelines to meet the requirements:

1. Price Workbook Submission:

o You are required to provide a price workbook as part of your submission. In this workbook, please include:

 A comprehensive list of your courses with titles, descriptions, and standard pricing.

 Any applicable discounts or special pricing structures for each course.

2. Website Catalog:

o You are welcome to include a link to the specific webpage listing all courses and their standard pricing. Please ensure this link is active and accessible. We will review this information, but it cannot be the only way our review committee can see the proposed product/service and pricing information.

Q.2 Response:

Clarification on Cost Presentation:

• Cost Per Participant vs. Per Class: Regarding section F.3, we encourage vendors to provide costs in both formats: per participant and per class when applicable. This will allow us to evaluate pricing options based on varying numbers of participants and classes. If there are specific requirements for one format over the other, please clarify so that all proposals can be reviewed with our evaluation criteria.

Per Diem and Mileage Charges:

• Per Diem and Mileage Charges: For on-site training delivery across the 30 different states, please ensure that your proposal includes a detailed breakdown of per diem and mileage charges. The review committee is particularly interested in understanding how these charges are calculated. Certain states may have limitations or cannot accommodate separate per diem or mileage charges. Include these costs within the total cost provided for each state. This will ensure the total costs are comprehensive and avoid potential discrepancies in cost allocation.

#35 - AEPA Bonfire Page/ Section: Informational

Tyler Technologies, Aug 27, 2024 6:23 PM EDT, Not Public - Pending

AEPA Bonfire Page/ Section: Informational asks for verification that we verify we downloaded 1-6 along with our section (Yes/ No). I don't see that we can verify that within Bonfire itself. Is the requirement to upload a separate document stating that question with a Yes/No answer? Or that we include it in the body of our RFP response?

Jane Eastes, Aug 29, 2024 5:38 PM EDT, Public - Answered

For All:

Vendors will be able to select a yes or no button to answer this question directly in Bonfire after you have started your submission process. You do not need to upload a document with the yes/no information, or include it in you RFP response.

#38 - Request for extension

SHI, Aug 27, 2024 7:53 PM EDT, Not Public - Pending

Based on the level of detail required to respond and the labor day holiday week, would the AEPA extend the deadline by 1-week after the addendum with questions and answers is posted? This extension will allow vendors the necessary time needed to put together the most thorough, compliant, and competitive response possible.

Jane Eastes, Aug 30, 2024 12:09 PM EDT, Public - Answered
AEPA is not able to provide an extension to the #025 solicitation at this time. We do understand and appreciate the time required to respond to a large cooperative solicitation. We encourage all vendors to do their best in the time allotted.

#43 - AEPA 025 Part D Questionnaire (Q-78CD), 1.4.1 Products & Services

Hamilton Telecommunications, Aug 29, 2024 10:52 AM EDT, Not Public - Pending
Can you please provide additional details on where the product category set forth in Part B - Specifications can be found for vendors interested in submitting a response for the Security Solutions and Cyber Security & Training categories? Thank you!
Jane Eastes, Sep 04, 2024 4:40 PM EDT, Public - Answered
These can be found when you "View Opportunity" in the AEPA Bonfire portal and then login. The filename F_-_Cyber_Security_&_Training_Part_A_Specifications_-_RFP.pdf is the file that can be downloaded. Specifications will be found in paragraph IV. Category Specifications of this document.

#47 - Regarding the Cyber Security & Training Part F.2 Price Schedule

ResoluteGuard, Aug 29, 2024 2:24 PM EDT, Not Public - Pending
F.1 in the Excel is required. We need clarification on Column B (Grouping of Discount) For Cyber Security services, (For example; MFA, EDR, Training, Vulnerability Assessment, etc) What is the Definition of “Grouping of Discount?” Our thought is that a line item would be a Bundle of Services (MFA and EDR) therefore the Bid requestor would receive a Discount versus paying individual fee for each service in worksheet F.2 Price Schedule. Also, on the F-1 worksheet, there are 40 lines, can we add more lines (rows) to this worksheet. Cybersecurity solutions involve the calculation of fees based upon device or endpoint count so we will need to add rows? Lastly, on the F-3 worksheet, it lists “Training.” For Employee Cybersecurity Awareness Training, are we to populate F-3 or should be listed in F-2?
Jane Eastes, Sep 04, 2024 6:47 PM EDT, Public - Answered

For Cyber Security Solutions & Training Category:

- What is the Definition of “Grouping of Discount?”

o Response: A grouping could be how a vendor bundles a number of line items for services and/or products being sold to members. Each vendor may group their catalog of services differently based on the entire catalog, users, devices, students/staff or tiers for each. You may provide one discount off all services or you could provide discounts based on different groups of services/product. Discounts in F.1 should be reflected in F.2 for each item "Bid Discount Percentage".

- on the F-1 worksheet, there are 40 lines, can we add more lines (rows) to this worksheet

o Response: You may add as many lines as required

- Lastly, on the F-3 worksheet, it lists “Training.” For Employee Cybersecurity Awareness Training, are we to populate F-3 or should be listed in F-2?

o Response: If Training services is a flat rate and has no per diem or mileage charges associated, for instance with virtual training then it could be listed in the F-2 Price Schedule. Otherwise you can list it in the F.3 Services Price Schedule.

#44 - Regarding the Cyber Security & Training

ResoluteGuard, Aug 29, 2024 2:27 PM EDT, Not Public - Pending

If accepted as an AEPA Vendor to accept bids, are we able to change the fee (lower or higher) as service fees change? Obviously, not after a bid is accepted by a requestor that we would change the fee. But, future Price Schedule changes. If this is allowed, is this restricted to a specific time period? Ex: Annually?

Jane Eastes, Sep 04, 2024 4:48 PM EDT, Public - Answered

AEPA does allow for price schedule changes using certain procedures. Information on the process to change or update pricing can be found on page 15 of the AEPA General Terms and Conditions (Part B). This can be found on Bonfire under Files and is the #3 informational document require to be downloaded.

#46 - Solicitation Checklist

CDW Government LLC, Aug 29, 2024 3:45 PM EDT, Not Public - Pending
On page 4 of Document E – Security Solutions Part A Specifications, Document Development states that “Respondents must scan and upload all documents to Bonfire following the Solicitation Checklist, along with any additional documents or fiels other than those listed below that may be requested and/or related to the solication.” Is the Solicitation Checklist available as a download?
Jane Eastes, Sep 04, 2024 5:09 PM EDT, Public - Answered
For Cybersecurity Solutions and Training: The Solicitation Checklist is available at the end of F - Cyber Security & Training Part E Signature Forms which is a required form to download and return with your response.

#45 - seeking a manufacturer of cybersecurity

Varmoda Tech LLC, Aug 30, 2024 12:13 PM EDT, Not Public - Pending
Is the agency primarily seeking a manufacturer of cybersecurity products for this opportunity, given the focus on annual sales, distributor locations, and customer support options, or are service providers specializing in cybersecurity and training also suitable to respond?
Jane Eastes, Sep 04, 2024 5:00 PM EDT, Public - Answered
For Cybersecurity Solutions Category: AEPA will accept a response from any type of vendor who can deliver the service as described in the Scope of Work found in F-Cybersecurity and Training Part A. As an RFP, AEPA will consider respondents who can fit the scope of work. As written: Scope of Work "AEPA is seeking qualified, experienced contractor(s) who possess the necessary resources and technical capabilities to acquire, deliver and perform the required services, supplies, materials, equipment and labor to all participating member states (up to 30) in the category of Cyber Security & Training. Qualified vendors will be able to provide comprehensive cyber security services to members to include PK-12 educational, Higher Education Institutions and other public institutions. The selected vendor(s) will deliver a range of cyber security solutions aimed at protecting the organization’s information assets and training staff on best practices to ensure a robust security posture." This section continues with details describing the types of services and training AEPA is looking for in a proposal.

Document Name: F - Cyber Security & Training Part A Specifications - RFP.pdf

Vendor Name	Contact Name	Address	Date Downloaded
22nd Century Technologies, Inc.	Shikha Sharma	8251 Greensboro Drive, Suite 900 McLean Virginia US 22102	2024-08-08 11:03:05
ActZero	Linda Kerr	2 Shaw Alley 5th Floor San Francisco CA US 94105	2024-08-21 09:28:02
Advanced Healthstyles Fitness Equipment, Inc.	Tyler Spieker	861 Southpark Drive, Suite 100 Littleton CO US 80120	2024-08-20 11:49:14
Advanced IT Concepts, LLC (AITC, LLC)	Brein Jones	12151 Science Drive Orlando Florida US 32826	2024-09-17 12:49:39
Alpine Frog, LLC	Michael Flood	6325 Falls of Neuse Rd Ste 35-403 Raleigh North Carolina US 27615	2024-08-13 11:14:54
APS Contracting, Inc	Svetozar Savreski	155-161 Pennsylvania Avenue Paterson NEW JERSEY US 07503	2024-08-22 14:43:03
Arbitr Services, LLC	Alexander Taft	3025 N 1st Ave Milton Florida US 32583	2024-09-03 08:52:46
Ardent Technologies, Inc.	Vas Appalaneni	6234 FAR HILLS AVENUE DAYTON Ohio US 45459	2024-08-04 12:35:35
BBR Printers	Bo Pomu	2203 Elston Avenue Chicago Illinois US 60602	2024-08-14 07:58:33
Beta Systems International	Joanne Briones	8070 Georgia Ave SUITE 212 Silver Spring Maryland US 20910	2024-09-11 20:53:13
Binary Consulting Group	Richard Watson	2808 Myrtlewood Dr Dumfries VA US 22026	2024-08-02 12:09:32
BuildCentral Inc	Karen Ericksen	320 W Ohio St Suite 300 Chicago ILLINOIS US 60654-6566	2024-08-03 01:44:17
Caetra.io	Michael Compisi	99 Garnsey Rd Pittsford New York US 14534	2024-08-20 10:56:44
calloway & Associates	cassandra johnson	8961 Harvest Oaks Drive Ste 201 Raleigh North Carolina US 27615	2024-08-30 09:30:24
CCS Global Tech	Raminder Singh	13475 Danielson Street, Suite 230 Poway California US 92064	2024-08-01 15:08:05
CCS Learning Academy	Raminder Singh	13475 Danielson Street, Suite 230 Poway California US 92064	2024-08-02 17:30:39
CDW Government LLC	Justin Schwier	200 N. Milwaukee Ave Vernon Hills Illinois US 60061	2024-08-01 16:07:09
Centripetal Networks	Jonathan Howard	145 Maplewood Ave 4th Floor Portsmouth NH US 03801	2024-08-12 10:09:27
ClassLink	Brian Kim	45 East Madison Avenue Clifton New Jersey US 07011	2024-09-01 09:32:18
Clever	Darcy Grabski	575 Market St Suite 1850 San Francisco CA US 94105	2024-08-07 12:04:36
Compunnel Software Group, Inc.	Nitisha Kainthola	103 Morgan Lane, Suite 102, Plainsboro, New Jersey, 08536 Plainsb	2024-08-15 07:42:58
Constructconnect	Michael Stubbs	3825 Edwards Rd., Suite 800 Cincinnati Ohio US 45209	2024-08-13 08:53:52
ConvergeOne, Inc.	Jay Patrick	10900 Nesbitt Avenue S Bloomington MN US 55437	2024-08-16 12:03:48
Cooperative Educational Services	John Tortelli	10601 Research Rd. NE Albuqeurque NM US 87123	2024-08-19 03:21:28
CTRLBridge, LLC	Tolu Olubunmi	1445 Woodmont Ln, NW Suite #2005 Atlanta GA US 30318	2024-08-23 14:53:18
Deledao	Kevin Kuckkan	3561 Homestead Road, Suite 424 Santa Clara California US 95051	2024-09-10 16:08:47
Deltek	Source Management		2024-08-02 15:37:31
Discount Two-Way Radio Corporation	Michelle Morris	555 W. Victoria Street Compton California US 90220	2024-09-12 14:21:11
Dodge Data and Analytics	April Hamilton	2860 S State Highway 161 Suite 160#501 Grand Prairie texas US 750	2024-08-09 01:09:48
Duro-Last	Kevin Blasesser	525 E Morley Dr Saginaw MI US 48601	2024-09-06 16:14:45
Enomis Consulting Group	Patricia Mae Sy		2024-08-12 13:56:26
Enterprise Pals, Inc.	Nazim Nashipudi		2024-09-05 07:10:43
Enterprise Risk Management, Inc. dba ERMProtect	Susie Crisp	800 S Douglas Road North Tower Suite 940 Coral Gables Florida US 3	2024-08-23 10:40:40
eRepublic, Inc.	Mary Lamoreaux	100 Blue Ravine Rd. Folsom California US 95630	2024-08-06 10:05:22

ESU Coordinating Council	Craig Peterson	412 W. 14th Ave PO BOX 858 Holdrege NE US 68949	2024-08-08 16:37:24
Executive Option, LLC	Jill Corley	2500 Anthem Village Drive Suite 200 Henderson Nevada US 89014	2024-09-04 16:58:30
Exela Technologies	Swapnil H	2701 E. Grauwyler Road Irving Texas US 75061	2024-08-12 10:17:56
Filament Information Security	Karen Mullins	1300 O Street Lincoln NE US 68508	2024-08-13 10:43:54
Fortalice Solutions, LLC	Bridget O'Connor	212 North McDowell Street Suite 212 Charlotte NC US 28204	2024-08-28 15:15:10
Generations Services Inc	Paul Litvin	220 West Parkway Unit 8a Pompton Plains NJ US 07444	2024-08-07 10:33:51
Global Roofing Group	Amara Boesch	2401 E Magnolia St Phoenix Arizona US 85034	2024-08-08 13:35:12
Guidepost Solutions	Leslie Lyons	2121 N. California Blvd Suite 800 Walnut Creek California US 94596	2024-08-21 13:42:27
Hamilton Telecommunications	Jennifer Dennis	1006 12th St. Aurora Nebraska US 68818	2024-08-07 11:55:28
Howard Technology Solutions	Brandey Boyd	PO Box 1590 Laurel Mississippi US 39441	2024-08-02 14:47:45
IBEX IT Business Experts, LLC	Tracy Grace	3295 River Exchange Drive Ste. 550 Norcross GA US 30092	2024-08-06 15:21:58
In Earth Consulting	Michelle Stevens	2600 Encina Irving Texas US 75038	2024-09-14 14:01:14
Infosec Institute	Lauren Shaw	3 Center Plaza Boston MA US 02110	2024-09-17 10:16:09
JR&Co., Inc	Tony Medina	1201 W. 31st St Suite 1 Kansas City Missouri US 64108	2024-09-10 13:53:43
Kudelski Security	Erwin Simon		2024-08-01 15:10:43
Kyocera Document Solutions America Inc	Mark Sarrao	225 Sand Road Fairfield New Jersey US 07004	2024-08-01 13:05:54
Lakeshore Learning Materials, LLC	Jennifer Doran	2695 E Dominguez St Carson California US 90895	2024-08-10 17:53:52
LanceSoft,Inc.	Prashant Arni	2121 Cooperative Way, Suite 130 Suite 130, Herndon VA US 20171	2024-08-07 07:28:34
Larsent & Toubro Limited	Mahesh Kaule		2024-08-23 08:07:51
Lattas	Mike Mullarky	111 8TH AVE W HUNTINGTON West Virginia US 25701	2024-08-22 15:13:19
Learn2Engage	Cheryl Powell	4250 Alafaya Trl Suite 212-111 Oviedo FL US 32765	2024-08-05 14:43:43
Lexmark International	Angie Edgerton	740 West New Circle Road Lexington KY US 40550	2024-08-21 17:20:32
Mavros LLC	Christopher Brown	10935 Estate Ln Suite 478 Dallas Texas US 75238	2024-09-09 08:17:23
MGT of America, LLC	Malony Allen	4320 West Kennedy Boulevard Suite 200 Tampa Florida US 33609	2024-08-02 12:45:04
Micro Strategies Inc	Debbie Faccenda	1140 Parsippany Blvd. Parsippany NJ US 07054	2024-08-05 08:12:33
MILNER Inc	Bob Tibbs	915 b interstate ridge Gainesville Georgia US 30501	2024-08-07 10:12:22
Network Technology Partners		16442 Village Plaza View Dr Wildwood Missouri US 63011	2024-08-02 11:13:05
Nextec Inc.	Beth Santana	4135 Pleasant Meadow Ct Suite 140 Herndon VA US 20170	2024-08-05 14:10:12
Orion Energy Systems	Jenifer Parke	2210 Woodland Drive Manitowoc WI US 54220	2024-09-03 10:04:56
PEPPM	Mark Carollo	90 Lawton Lane Milton PA US 17847	2024-08-02 09:05:43
Polyloom Corporation of America dba TenCate Grass N.A.	Ruth Hawley	255 Kraft Drive Dalton GA US 30721	2024-08-01 14:25:36
Premier Sports Lighting, LLC	Andrew Weathers	2100 Chespark Drive Gastonia North Carolina US 28052	2024-08-05 10:14:43
Printer Source Plus	Joe Sharpe	2903 W. Michigan Ave Jackson Michigan US 49202	2024-08-29 17:53:58
PWXPress	Mary Miller		2024-08-01 13:36:52
R&M Best Deals LLC	Romates Moise	10229 Strawberry Tetra Drive Riverview, FL FL US 33578	2024-08-13 11:48:53
R.A.D. Sports	Amanda Loggia	171 VFW Drive Rockland Massachusetts US 02370	2024-08-13 14:04:15

Repro Products	Justin Katz	4485 Atlanta Rd Smyrna GA US 30080	2024-08-06 13:14:16
ResoluteGuard	Jeffrey Schobel	417 Crescent Pky Sea Girt NJ US 08750	2024-08-19 14:10:02
RoofConnect Logistics Inc	Stacey Duwe	44 Grant 65 Sheridan Arkansas US 72150	2024-08-08 10:43:17
SBS-TS, Inc.	Todd Hargrave	1101 Belcher Rd S #F-1 Largo FL US 33771	2024-08-04 16:34:19
School Specialty LLC	Sarah Peterson	W6316 DESIGN DRIVE GREENVILLE Wisconsin US 54942	2024-08-02 10:20:07
SCHOOL WHOLESALE SUPPLIES LLC	JP Das	2120 Donelson Pike Nashville, TN 37210 Nashville TN US 37210	2024-08-13 05:56:55
Securance LLC	Paul Ashe	13916 Monroes Business Park Suite 102 Tampa Florida US 33635	2024-08-05 09:27:12
Security Effects	Frank Wood	9234 Kingston Pike #400 Knoxville TN US 37922	2024-08-02 08:42:50
Sentinel Technologies	Chris Bowen	Pennzoil Place 700 Milam St #1300 Houston Texas US 77002	2024-08-19 16:03:23
Sentinel Technologies, Inc	Kevin Cooper	2550 Warrenville Rd Downers Grove Illinois US 60515	2024-08-08 17:02:26
Serigor Inc	Jitender Sharma	400 East Pratt Street Suite #800 Baltimore MD US 21202	2024-08-09 13:50:49
SevenOutsource	Steve Walse	113 Barksdale Professional Center, Barksdale Barksdale Professional C	2024-08-03 03:06:24
Shay Enterprise	Tamara Shay	1789 Tavern Ln. Tacoma WA, 984 98402 Tacoma Washington US 984	2024-08-01 13:48:31
SHI	John Wetter	290 Davidson Ave, Somerset NJ US 08873	2024-08-02 16:59:11
Skillsoft	Sarah Rizvi	300 Innovative Way Suite 201 Nashua New Hampshire US 03062	2024-08-29 15:14:07
SMB Consultants LLC	Sherjil Baig	1576 President ST Glendale Hts IL US 60139	2024-08-12 10:26:54
SNVA LLC	SNVA LLC	Waldorf Waldorf MD US 20602	2024-08-14 01:53:57
Softchoice Corporation	David Butkiewicz	314 W Superior St Suite 400 Chicago Illinois US 60654	2024-08-06 18:10:35
Solutionz, Inc.	Amy Erber	4357 Park Drive Suite E Norcross Georgia US 30093	2024-08-21 16:26:09
Sophos	Craig Allen	3090 Nowitzki Way Dallas Texas US 75217	2024-08-26 14:18:02
South Western Communications, Inc.	Elaine George	4871 Rosebud Lane Newburgh Indiana US 47630	2024-08-21 16:22:32
Spiral Networks, Inc.	Julia Kushnir	3 Croydon Ct. Holmdel New Jersey US 07733	2024-09-13 08:27:18
Stragistics Technology, Inc.	Hughetta Dudley	6800 Poplar Avenue Suite 200 Memphis Tennessee US 38138	2024-09-03 13:34:39
Technology International, Inc.	Shaji Habib	1331South International Parkway, Ste 2251 Lake Mary Florida US 32	2024-08-08 01:16:19
Tillman Goods LLC	Justin Patterson		2024-09-08 23:25:37
TNT Construction Group LLC	Daniela Tolov	74 Semel Ave Garfield New Jersey US 07026	2024-09-09 13:13:32
Trifecta Consulting Group	Jason McKenzie	7901 4th St N Ste 13824 St Petersburg FL US 33702	2024-08-13 07:51:16
TruPointe Partners	Mason Sellers	6640 Carothers Pkwy Suite 410 Franklin Tennessee US 37067	2024-08-01 15:22:59
Twotrees Technologies	Susie Smith	200 North Emporia Suite 300 Wichita Kansas US 67202	2024-09-05 10:53:30
Tyler Technologies	Courtney Price	5519 53rd Street Tyler Technologies - suite 309 Lubbock Texas US 79	2024-08-03 05:14:48
US	Shane Lanier	221 Cable Industrial Way Carrollton Georgia US 30117	2024-08-01 16:53:07
US Modular Group East	Andy Alcarese	1414 Burke Rd Middle River MD US 21220	2024-08-22 12:02:29
USA General Contractors Corp	Lily Jimenez	167 Route 33 Manalapan NJ US 07726	2024-08-23 10:27:17
Varmoda Tech LLC	Manish Dadhich	44345 PREMIER PLZ, STE 120 ASHBURN, VA 20147 Ashburn Virginia	2024-08-05 08:40:57
VasSecCo	John Vasquez	7755 Center Ave Floor 11 ATTN: Vasquez Security Consulting Hunting	2024-08-19 18:30:46
Veeya, LLC.	Bill Kics	4561 E McDowell Rd Suite 100 Phoenix AZ US 85008	2024-09-10 16:10:34
VISUAL	TECH ZONE	5c1 vcs nagar 1st street gn mills Coimbatore TN US 64102	2024-08-03 01:47:34

vTech Solution Inc.	Vishnu Naruka	1100 H Street, N.W. Suite 850, Washington District of Columbia US 2	2024-08-02 10:48:44
W.E. BROWN BUSINESS GROUP	EMATCHIA BROWN	320 Lanier Ave W 257 Fayetteville Georgia US 30214	2024-08-12 16:36:30
Weatherproofing Technologies, Inc.	Laiv Levy	3735 Green Rd. Beachwood Ohio US 44122	2024-08-01 13:05:22
WELDINGMART, LLC	Robert Jones	W5021 Amy Avenue, Suite 7 Kaukauna WI US 54130	2024-08-16 12:55:38
White Rock Corp.	Steve Vanev	17 Gramercy Rd. Old Bridge New Jersey US 08857	2024-09-05 00:36:33
www.forward-edge.net	Denise Caccavari	2724 E Kemper Road Sharonville OH US 45241	2024-08-07 09:52:26

AEPA 025 - Solicitation Category → -F - Cybersecurity & Training
Opening Record

Active Submissions

	Part D - Questionnaire	Part E - Signature Forms	Part F - Pricing Workbook	Bid Security	Category Specific Requirements	Responsiveness Check - Send to Category Committee for Evaluation
Supplier	Pass/Fail	Pass/Fail	Pass/Fail	Pass/Fail	Pass/Fail	Pass/Fail
ActZero	Pass	Pass	Pass	Pass	Pass	Pass
Beta Systems International	Pass	Pass	Pass	Pass	Pass	Pass
Caetra.io	Pass	Pass	Pass	Pass	Pass	Pass
CCS Global Tech	Pass	Pass	Pass	Pass	Pass	Pass
CDW Government LLC	Pass	Pass	Pass	Pass	Pass	Pass
Clutch Solutions LLC	Pass	Pass	Pass	Pass	Pass	Pass
Enterprise Risk Management, Inc. dba ERMProtect	Pass	Pass	Pass	Pass	Pass	Pass

Executive Option, LLC	Pass	Pass	Pass	Pass	Pass	Pass
Fortalice Solutions, LLC	Pass	Pass	Pass	Pass	Pass	Pass
Hamilton Telecommunications	Pass	Pass	Pass	Pass	Pass	Pass
Infosec Institute	Pass	Pass	Pass	Pass	Pass	Pass
Network Technology Partners	Pass	Pass	Fail	Pass	Pass	Pass
ResoluteGuard	Pass	Pass	Pass	Pass	Pass	Pass
SHI	Pass	Pass	Pass	Pass	Pass	Pass
Twotrees Technologies, L.L.C.	Pass	Pass	Pass	Pass	Pass	Pass
Tyler Technologies	Pass	Pass	Pass	Pass	Pass	Pass
www.forward-edge.net	Pass	Pass	Pass	Pass	Pass	Pass

Eliminated Submissions

	Part D - Questionnaire	Part E - Signature Forms	Part F - Pricing Workbook	Bid Security	Category Specific Requirements	Responsiveness Check - Send to Category Committee for Evaluation
Supplier	Pass/Fail	Pass/Fail	Pass/Fail	Pass/Fail	Pass/Fail	Pass/Fail
vTech Solution Inc.	Pass	Fail	Fail	-	-	-

ActZero

	Q1	Q2	Q3	Q4
Goals	Ensure AEPA member agencies and ActZero reseller/distribution partners are fully informed about the new contract. Drive engagement with AEPA member agencies through educational and promotional content.	Generate sales leads and inquiries related to the AEPA contract. Drive engagement with AEPA member agencies through educational and promotional content.	Highlight ActZero's key benefits, such as better block rate, 24/7 SOC, and fewer alerts. Generate sales leads and inquiries related to the AEPA contract.	Strengthen ongoing partnerships with AEPA agencies to promote retention.
Audience	AEPA Member Agencies and ActZero Reseller/Distribution partners	AEPA Member Agencies and ActZero Reseller/Distribution partners	AEPA Member Agencies and ActZero Reseller/Distribution partners	AEPA Member Agencies and ActZero Reseller/Distribution partners
Theme	Getting started + ActZero and MDR basics	Securing Organizations Better (Safe, Speed, Quality)	Deliver Expertise to You	Cyber made Simple
Messages		• Better Block rate • Coverage across environment	• 24/7 SOC • Threat hunting • Incident Response Retainer	• Fewer alerts • Quick response • Quick deployment
Campaign/Activities	• Announce contract to reseller/distribution partners via social, email, and newsletters • Build distribution list for state-member agencies. • Create landing page for state-member agencies similar to this one. • Host kick-off call with state-member agencies • Build member sales toolkit. • Possible shows with partners: CoSN, FETC, TCEA	• Create and distribute targeted newsletter to AEPA member agencies. • Provide partners with AEPA co-branded collateral for events, tradeshows, conferences. • Create industry specific (K12, higher ed and local govt) collateral for partners and reseller partners. • Publicize contract with distributors via their channels (emails, news, events) • Possible shows with partners: ClutchCon	• Create and distribute targeted newsletter to AEPA member agencies. • Provide partners with AEPA co-branded collateral for events, tradeshows, conferences. • Create industry specific (K12, higher ed and local govt) collateral including case studies for partners and reseller partners. • Publicize contract with distributors via their channels (emails, news, events) • Possible shows with partners: TribalNet	• Create and distribute targeted newsletter to AEPA member agencies. • Provide partners with AEPA co-branded collateral for events, tradeshows, conferences. • Create industry specific (K12, higher ed and local govt) collateral including case studies for partners and reseller partners. • Publicize contract with distributors via their channels (emails, news, events) • Possible shows with partners: HECC

Part E – Signature Forms

AEPA 025-F
Cyber Security and Training

Instructions

Contained herein are forms that **require a signature** from an authorized person at your company. All items found within this document are **mandatory**. Failure to sign the required areas, sections, or signature lines may lead AEPA to consider your company's proposal as **non-responsive**.

To submit the required signed forms, follow these steps:

1. Read the documents in their entirety.
2. Complete all forms and sign when required.
3. Return the forms and pages in their correct order and scan one (1) single PDF format titled ***"Part E – Signature Forms – Name of Responding Company"*** (i.e. one PDF document for all signature forms).
4. Submit Part E, along with other required documents in Bonfire.

*Note, a solicitation checklist has been provided to review with your submission.

The following sections will need to be completed prior to submission as one (1), single PDF titled "Part E – Signature Forms – Name of Responding Company".

Uniform Guidance "EDGAR" Certification Form – ****signature required***
Solicitation Affidavit – ****signature required***
Acceptance of Solicitation & Contract – ****signature required***

Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7. Clean Air Act and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended, contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein.		
Respondent Certification (By Item)	**Respondent Certification: YES**, I agree	**Initial**
1. Violation of Contract Terms and Conditions	Yes	HL
2. Termination for Cause of Convenience	Yes	HL
3. Equal Employment Opportunity	Yes	HL
4. Davis-Bacon Act	Yes	HL
5. Contract Work Hours and Safety Standards Act	Yes	HL
6. Right to Inventions Made Under a Contract or Agreement	Yes	HL
7. Clean Air Act and Federal Water Pollution Control Act	Yes	HL
8. Debarment and Suspension	Yes	HL
9. Byrd Anti-Lobbying Amendment	Yes	HL
10. Procurement of Recovered Materials	Yes	HL
11. Profit as a Separate Element of Price	Yes	HL
12. General Compliance with Participating Agencies	Yes	HL
13. Governing Law; Forum Selection.	Yes	HL

ActZero

Name of Business

Hal Libby

Signature of Authorized Representative

Hal Libby

Printed Name

September 17, 2024

Date

Solicitation Affidavit

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

Hal Libby	2 Shaw Alley, 5th Foor
Authorized Representative (Please print or type)	Mailing Address
Co-Founder	San Francisco, CA, 94105
Title (Please print or type)	City, State, Zip
Hal Libby	September 17, 2024
Signature of Authorized Representative	Date

Acceptance of Solicitation & Contract

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	ActZero	**Date**	September 17, 2024
Address	2 Shaw Alley, 5th Foor	**City, State Zip**	San Francisco, CA, 94105
Contact Person	Linda Kerr	**Title**	Director, Marketing
Authorized Signature	Hal Libby	**Title**	Co-Founder
Email	h@actzero.ai	**Phone**	

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Solicitation Checklist

Instructions: Utilize the checklist below, reviewing to confirm that all the required documents have been uploaded to Public Purchase, in their ***specified/required format***, by the due date and time listed for this solicitation. ***Submissions not following the specified/required format may result in being marked non-responsive and may not be considered for evaluation.*** Respondents are reminded that failure to follow, comply with, and adhere to the enclosed instructions of this solicitation may result in their response being deemed non-responsive. AEPA, its Member Agencies, affiliate agencies, and authorized representatives are not responsible for bid proposals that are incomplete, unreadable, or received after the solicitation deadline submission date.

"x"	**Document Title, Uploaded to Bonfire** *(Respondent must submit documents in the required title/format)*	**Format of Uploaded Document**	**Notes**
	Bid Bond – if Required, see Part A if applicable.	Upload PDF copy of the bid security.	The original bid security must be received by Lakes Country Service Cooperative by due date and time.
	Part C – State-Specific Forms – ***Name of Responding Company***	Single, Scanned PDF	**New Jersey Only Requirement.** Signatures Required.
	Part D - Questionnaire – ***Name of Responding Company*** Includes: ● Company Information ● Service Questionnaire ● Exceptions ● Deviations	Single, Scanned PDF	**Required.**
	Part E – Signature Forms – ***Name of Responding Company*** Includes: ● Uniform Guidance "EDGAR" Certification ● Solicitation Affidavit ● Acceptance of Solicitation & Contract	Single, Scanned PDF	**Required.** Signatures required.
	Part F – Pricing Schedule – ***Name of Responding Company***	Excel Workbook	**Required.**
	Price List and/or Catalog – ***Name of Responding Company***	Upload PDF	**Required.**
	Exhibit A – Marketing Plan – ***Name of Responding Company***	Scanned PDF	**Optional.** Form not provided by AEPA, Respondent Created

Contents

1-AEPA - Marketing Discussion	1
1-5-Caetra.io AEPA 025 New Jersey Documents	4
2-CyMetric 101 - Schools	16
3-CyMetric Q and A Document for K-12 - Cyber Risk Management Software	17
4-Caetra Talking Points for Schools - General	27
5-Caetra School Application - District Risk	29
6-How Does CyMetric Work	31
7-CyMetric Product Overview General	37
1-F - Caetra.io Cyber Security Training Part E Signature Forms Executed	41

Marketing Concepts for Award Engagements

Caetra.io will work with specific AEPA agencies to craft a marketing model that would resonate with the respective region or territory. Because each region may have different objectives or engagement styles that work best for the constituent base, Caetra.io will utilize a variety of approaches to inform not only AEPA agencies but local Education Service Agencies (ESA) and discrete districts on why the CyMetric platform can support risk management, cyber program assessment, risk communication and risk remediation needs. Historically, Caetra.io has used a combination of direct email campaigns, educational webinar series, and co-promotions with managed security service provider vendors/partners, ESAs and our law firm partner organization. However, given the relationship the AEPA has with its member agencies and constituents, working with the AEPA to model something that they feel would work within specific geographies would likely be the best approach. We have been told by AEPA personnel that when communications come from the AEPA, they are generally opened/reviewed significantly more than emails coming directly from vendors. We would seek to leverage those relationships to maximize opportunities and people's time.

Marketing concepts aligned to the mission of the AEPA RFP (Cyber security):

- Webinar/Education Series: Risk management with attorney partners (e.g. "What to Expect When You Are Expecting: The Anatomy of a Data Incident"), Insurance Industry Risk Seminar, Real-Life Stories: Surviving a Ransomware Event with a K-12 District, How to Prevent and Prepare for Data Incidents, Educating the Administrator: Teaching What is Important and How to Ask the Right Questions of Your Cyber Governance and IT Team, What is the Dark Web and What Can be Found There?
- Traditional Outbound Email Campaigns
- Co-Promotion with Managed Security Service Providers Aligning Objectives for Data Privacy and Data Security

Partner/Customer Training Plan Initiatives

Caetra.io is responsible for training our business partners, agencies and end users on the use of the platform. Once they are conversant in the tool, they will be able to handle functional questions from the user base. Scheduled quarterly trainings serve as a refresh on existing functionality along with updates on new functionality built in or will be built into the platform. Caetra.io participates in sales/pre-sales calls with prospective customers to support agencies and business partners to the extent it is needed. Depending upon the model ultimately defined between agencies, the AEPA and Caetra.io, all entities can be provided access to a sandbox platform to test, train and experiment with the platform. All delivery personnel will be highly trained and capable of high levels of execution and efficiency with CyMetric. Should a customer choose to acquire CyMetric and begin to self-service their account, the proper engagement model can be designed that allows for proper handoff and training.

Due to the nature of the platform and the needs of customers, various modules are leveraged in stages. The stages can be broken down into the following rough outline:

1. Onboarding: system and data management, data risk analysis, system ownership, compliance objectives/control definition
2. Control ownership and approval (governance), control configuration, policy generation and approval
3. Assessment plan generation, assessment methods and objects, control scoring, findings definition, POAM report
4. Reporting and dashboard, program maintenance, program evolution

Each of these stages comprises a training element that is typically 60-90 minutes in duration. Caetra.io does not get many real-time requests for support – currently 1-2 messages per month. In many cases, real-time inquiries are handled by the chat feature built into the platform managed by Caetra.io personnel.Caetra.io has built in a comprehensive self-service help file available within the platform. Many questions are answered via those articles with new articles being created regularly.

CyMetric Sample Training Plan: Onboarding to Assessments

Part 1: CyMetric Set Up (60-90 Mins)

- Defining Organization Details
- Inputting Users and Contacts
- Reviewing Information Types and Systems
- Add/Edit Information Type
- Add/Edit Information System
- Understanding Control Owners
- Approving Controls
    - By Triggering Event
    - Bulk Approval
- System and Data Reports

Part 2: CyMetric Set Up: Continued (60-90 Mins)

- Review Approving Controls
- Configure Controls with Variables (if applicable)

- Create Multiple Configurations for a Control
- Apply Control Configurations to a System
- Generate Standards/Procedural Documents/Written Information security Plan
- Control Reports

Part 3: Assessing/Auditing Compliance Program (90 Mins)

- Building an Assessment Plan
- Executing an Assessment Plan
    - Define Methods and Objects
    - Rating/Scoring Control Implementation
    - Documenting Rationale for Rating
    - Appending documents/artifacts to the assessment
    - Adding/Documenting Findings (Issues) with Control Implementation
    - Saving/Editing Control Assessment
    - Applying Control Assessment to Multiple Systems
    - Closing an Assessment
- Generate Assessment Report/View Dashboard

AFFIRMATIVE ACTION QUESTIONNAIRE

1. Our company has a federal Affirmative Action Plan approval. ☐ Yes ☒ No

   If yes, please attach a copy of the plan to this questionnaire.

2. Our company has a New Jersey State Certificate of Employee Information Report. ☐ Yes ☒ No

   If yes, please attach a copy of the certificate to this questionnaire.

3. If you answered "***NO***" to both questions above, No. 1 and 2, you must apply for an Affirmative Action Employee Information Report – Form AA302.

Please visit the New Jersey Department of Treasury website for the Division of Public Contracts Equal Employment Opportunity Compliance:

https://www.nj.gov/treasury/contract_compliance/

a. Click on "Employee Information Report"
b. Complete and submit the form with the *appropriate payment* to:

Department of Treasury
Division of Purchase and Property
Contract Compliance and Audit Unit
EEO Monitoring P.O. Box 206
Trenton, New Jersey 08625-0206

All fees for this application are to be paid directly to the State of New Jersey. A copy shall be submitted to the ESCNJ prior to the execution or award of contract.

I certify that the above information is correct to the best of my knowledge.

Name of Company/Firm CAETRA.10, INC

Address 99 GARNSEY RD

City, State, Zip PITTSFORD NY 14534

Name of Authorized Agent MICHAEL COMPISI Title PRESIDENT

SIGNATURE Michael A Compisi Date 9/16/24

APPENDIX A
AMERICANS WITH DISABILITIES ACT OF 1990
Equal Opportunity for Individuals with Disability

The contractor and the Educational Services Commission of New Jersey (hereafter "owner") do hereby agree that the provisions of Title 11 of the Americans with Disabilities Act of 1990 (the "Act") (42 U.S.C. S121 01 et seq.), which prohibits discrimination on the basis of disability by public entities in all services, programs, and activities provided or made available by public entities, and the rules and regulations promulgated pursuant there unto, are made a part of this contract. In providing any aid, benefit, or service on behalf of the owner pursuant to this contract, the contractor agrees that the performance shall be in strict compliance with the Act. In the event that the contractor, its agents, servants, employees, or subcontractors violate or are alleged to have violated the Act during the performance of this contract, the contractor shall defend the owner in any action or administrative proceeding commenced pursuant to this Act. The contractor shall indemnify, protect, and save harmless the owner, its agents, servants, and employees from and against any and all suits, claims, losses, demands, or damages, of whatever kind or nature arising out of or claimed to arise out of the alleged violation. The contractor shall, at its own expense, appear, defend, and pay any and all charges for legal services and any and all costs and other expenses arising from such action or administrative proceeding or incurred in connection therewith. In any and all complaints brought pursuant to the owner's grievance procedure, the contractor agrees to abide by any decision of the owner which is rendered pursuant to said grievance procedure. If any action or administrative proceeding results in an award of damages against the owner, or if the owner incurs any expense to cure a violation of the ADA which has been brought pursuant to its grievance procedure, the contractor shall satisfy and discharge the same at its own expense.

The owner shall, as soon as practicable after a claim has been made against it, give written notice thereof to the contractor along with full and complete particulars of the claim, If any action or administrative proceeding is brought against the owner or any of its agents, servants, and employees, the *owner shall* expeditiously forward or have forwarded to the contractor every demand, complaint, notice, summons, pleading, or other process received by the owner or its representatives.

It is expressly agreed and understood that any approval by the owner of the services provided by the contractor pursuant to this contract will not relieve the contractor of the obligation to comply with the Act and to defend, indemnify, protect, and save harmless the owner pursuant to this paragraph.

It is further agreed and understood that the owner assumes no obligation to indemnify or save harmless the contractor, its agents, servants, employees and subcontractors for any claim which may arise out of their performance of this Agreement. Furthermore, the contractor expressly understands and agrees that the provisions of this indemnification clause shall in no way limit the contractor's obligations assumed in this Agreement, nor shall they be construed to relieve the contractor from any liability, nor preclude the owner from taking any other actions available to it under any other provisions of the Agreement or otherwise at law.

Company CAETRA.10, INC Name MICHAEL COMPISI

Signature [signature] Title PRESIDENT

Date: 9/16/24

ASSURANCE OF COMPLIANCE

Contact with Students

There may be times during the performance of this contract, where a contracted service provider may come in contact with students of the school district. The district fully understands it obligation to provide to all students and staff members, a safe educational environment. To this end, the district is requiring all bidders to sign a statement of Assurance of Compliance, acknowledging the bidder's understanding of the below listed requirements and further acknowledging the bidder's assurance of compliance with those listed requirements.

Anti-Bullying Reporting--Requirement

When applicable, the contracted service provider shall comply with all applicable provisions of the New Jersey Anti-Bullying Bill of Rights Act—N.J.S.A. 18A:37-13.1 et seq., all applicable code and regulations, and the Anti-Bullying Policy of the Board of Education. In accordance with N.J.A.C. 6A:16-7.7 (c), a contracted service provider, who has witnessed, or has reliable information that a student has been subject to harassment, intimidation, or bullying shall immediately report the incident to any school administrator or safe schools resource officer, or the School Business Administrator/Board Secretary.

Criminal History Background Checks—N.J.S.A. 18A:6-7.1--Requirement

When applicable, the contracted service provider, shall provide to the school district prior to commencement of contract, evidence or proof that each employee assigned to provide services and that comes in **regular contact** with students, has had a criminal history background check, and furthermore, that said background check indicates that no criminal history record information exists on file for that worker. Failure to provide a proof of criminal history background check for any employee coming in regular contact with students, prior to commencement of contact, may be cause for breach of contract. See NJDOE Broadcast 9/9/19.

Pre-Employment Requirements

When applicable, all contracted service providers, whose employees have **regular contact with students**, shall comply with the Pre-Employment Requirements in accordance with New Jersey P.L. 2018 c.5, N.J.S.A. 18A:6-7.6 et seq. Contracted service providers are to review the following New Jersey Department of Education Office of Student Protection—Pre-Employment Resource P.L. 2018 c.5 link below for guidance and compliance procedures.

https://www.nj.gov/education/crimhist/preemployment/

Name of Company CAETRA.10, INC.

Name of Authorized Representative MICHAEL COMPISI

Signature _____ Date 9/16/24

(Revised: January, 2016)

EXHIBIT A
MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE
N.J.S.A. 10:5-31 et seq. (P.L. 1975, C. 127)
N.J.A.C. 17:27
GOODS, PROFESSIONAL SERVICE AND GENERAL SERVICE CONTRACTS

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Except with respect to affectional or sexual orientation and gender identity or expression, the contractor will ensure that equal employment opportunity is afforded to such applicants in recruitment and employment, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Such equal employment opportunity shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this nondiscrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex.

The contractor or subcontractor will send to each labor union, with which it has a collective bargaining agreement, a notice, to be provided by the agency contracting officer, advising the labor union of the contractor's commitments under this chapter and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to N.J.S.A. 10:5-31 et seq., as amended and supplemented from time to time and the Americans with Disabilities Act.

The contractor or subcontractor agrees to make good faith efforts to meet targeted county employment goals established in accordance with N.J.A.C. 17:27-5.2.

The contractor or subcontractor agrees to inform in writing its appropriate recruitment agencies including, but not limited to, employment agencies, placement bureaus, colleges, universities, and labor unions, that it does not discriminate on the basis of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job related testing, as established by the statutes and court decisions of the State of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

In conforming with the targeted employment goals, the contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and layoff to ensure that all such actions are taken without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The contractor shall submit to the public agency, after notification of award but prior to execution of a goods and services contract, one of the following three documents:

- Letter of Federal Affirmative Action Plan Approval
- Certificate of Employee Information Report
- Employee Information Report Form AA302 (electronically provided by the Division and distributed to the public agency through the Division's website at https://www.nj.gov/treasury/contract_compliance/

The contractor and its subcontractors shall furnish such reports or other documents to the Division of Purchase & Property, CCAU, EEO Monitoring Program as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Division of Purchase & Property, CCAU, EEO Monitoring Program for conducting an investigation pursuant to N.J.A.C. 17:27-1.1 et seq.

Company CAETRA.10, INC. Name MICHAEL COMPISI

Signature [signature] Title PRESIDENT

Form AA302
Rev. 02/22

STATE OF NEW JERSEY

Division of Purchase & Property
Contract Compliance Audit Unit
EEO Monitoring Program

EMPLOYEE INFORMATION REPORT

IMPORTANT-READ INSTRUCTIONS CAREFULLY BEFORE COMPLETING FORM. FAILURE TO PROPERLY COMPLETE THE ENTIRE FORM AND TO SUBMIT THE REQUIRED $150.00 FEE MAY DELAY ISSUANCE OF YOUR CERTIFICATE. DO NOT SUBMIT EEO-1 REPORT FOR SECTION B, ITEM 11. For Instructions on completing the form, go to: https://www.nj.gov/treasury/contract_compliance/documents/pdf/forms/aa302ins.pdf

SECTION A - COMPANY IDENTIFICATION

1. FID. NO. OR SOCIAL SECURITY	2. TYPE OF BUSINESS	3. TOTAL NO. EMPLOYEES IN THE ENTIRE COMPANY
82-4157572	☐ 1. MFG ☐ 2. SERVICE ☐ 3. WHOLESALE ☐ 4. RETAIL ☒ 5. OTHER	1

4. COMPANY NAME: Caetra.io, Inc.
COMPANY E-MAIL: contact@caetra.io

5. STREET	CITY	COUNTY	STATE	ZIP CODE
99 Garnsey Rd	Pittsford	Monroe	NY	14534

6. NAME OF PARENT OR AFFILIATED COMPANY (IF NONE, SO INDICATE) — CITY — STATE — ZIP CODE
None

7. CHECK ONE: IS THE COMPANY: ☒ SINGLE-ESTABLISHMENT EMPLOYER ☐ MULTI-ESTABLISHMENT EMPLOYER

8. IF MULTI-ESTABLISHMENT EMPLOYER, STATE THE NUMBER OF ESTABLISHMENTS IN NJ

9. TOTAL NUMBER OF EMPLOYEES AT ESTABLISHMENT WHICH HAS BEEN AWARDED THE CONTRACT: 1

10. PUBLIC AGENCY AWARDING CONTRACT — CITY — COUNTY — STATE — ZIP CODE

Official Use Only	DATE RECEIVED	INAUG.DATE	ASSIGNED CERTIFICATION NUMBER

SECTION B - EMPLOYMENT DATA

11. Report all permanent, temporary and part-time employees ON YOUR OWN PAYROLL. Enter the appropriate figures on all lines and in all columns. Where there are no employees in a particular category, enter a zero. Include ALL employees, not just those in minority/non-minority categories, in columns 1, 2, & 3. *DO NOT SUBMIT AN EEO-1 REPORT.*

JOB CATEGORIES	ALL EMPLOYEES	PERMANENT MINORITY/NON-MINORITY EMPLOYEE BREAKDOWN												
	COL. 1	COL. 2	COL. 3	********* MALE*********						********* FEMALE*********					
	Total	Male	Female												
	(Cols.2 &3)			BLACK	HISPANIC	AMER INDIAN	ASIAN	NON MIN	2 OR MORE RACES	BLACK	HISPANIC	AMER INDIAN	ASIAN	NON MIN	2 OR MORE RACES
Officials/ Managers	1	1						1							
Professionals															
Technicians															
Sales Workers															
Office & Clerical															
Craftworkers (Skilled)															
Operatives (Semi-skilled)															
Laborers (Unskilled)															
Service Workers															
TOTAL															
Total employment From previous Report (if any)															
	The data below shall NOT be included in the figures for the appropriate categories above.														
Temporary & Part-Time Employees															

12. HOW WAS INFORMATION AS TO RACE OR ETHNIC GROUP IN SECTION B OBTAINED?
☒ 1. Visual Survey ☐ 2. Employment Record ☐ 3. Other (Specify)

13. DATES OF PAYROLL PERIOD USED
From: 08/26/2024 To: 09/06/2024

14. IS THIS THE FIRST Employee Information Report Submitted?
1. YES ☒ 2. NO ☐

15. IF NO, DATE LAST REPORT SUBMITTED
MO. DAY YEAR

SECTION C - SIGNATURE AND IDENTIFICATION

16. NAME OF PERSON COMPLETING FORM (Print or Type)	SIGNATURE	TITLE	DATE MO / DAY / YEAR
Michael Compisi		President	09 / 16 / 2024

17. ADDRESS NO. & STREET	CITY	COUNTY	STATE	ZIP CODE	PHONE (AREA CODE, NO.,EXTENSION)
99 Garnsey Rd	Pittsford	Monroe	NY	14534	585 - 955 - 4905

Educational Services Commission of New Jersey

Business Office

1660 Stelton Road, Floor 2
Piscataway, New Jersey 08854

Chapter 271
Political Contribution Disclosure Form

(Contracts that Exceed $17,500.00)
Ref. N.J.S.A. 19:44A-20.26

The undersigned, being authorized and knowledgeable of the circumstances, does hereby certify that CAETRA.10, INC. (Business Entity) has made the following **reportable** political contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26 during the twelve (12) months preceding this award of contract:

Reportable Contributions

Date of Contribution	Amount of Contribution	Name of Recipient Elected Official/ Committee/Candidate	Name of Contributor

The Business Entity may attach additional pages if needed.

X **No Reportable Contributions** (Please check (✔) if applicable.)

I certify that CAETRA.10, INC. (Business Entity) made no reportable contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26.

Certification

I certify that the information provided above is in full compliance with Public law 2005 – Chapter 271.

Name of Authorized Agent MICHAEL COMPISI

Signature _____ Title PRESIDENT

Business Entity CAETRA.10, INC.

Prohibited Russia-Belarus Activities & Iran Investment Activities

Person or Entity	CAETRA · 10, INC

Part 1: Certification

COMPLETE PART 1 BY CHECKING **ONE OF THE THREE BOXES BELOW**

Pursuant to law, any person or entity that is a successful bidder or proposer, or otherwise proposes to enter into or renew a contract, for goods or services must complete the certification below prior to contract award to attest, under penalty of perjury, that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list or Chapter 25 list as a person or entity engaging in prohibited activities in Russia, Belarus or Iran. Before a contract for goods or services can be amended or extended, a person or entity must certify that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list. Both lists are found on Treasury's website at the following web addresses:

https://www.nj.gov/treasury/administration/pdf/RussiaBelarusEntityList.pdf
www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf.

As applicable to the type of contract, the above-referenced lists must be reviewed prior to completing the below certification.

A person or entity unable to make the certification must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran. The person or entity must cease engaging in any prohibited activities and provide an updated certification before the contract can be entered into.

If a vendor or contractor is found to be in violation of law, action may be taken as appropriate and as may be provided by law, rule, or contract, including but not limited to imposing sanctions, seeking compliance, recovering damages, declaring the party in default, and seeking debarment or suspension of the party.

CONTRACT AWARDS AND RENEWALS

☒	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate appears on the N.J. Department of Treasury's lists of entities engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3 or in investment activities in Iran pursuant to P.L. 2012, c. 25 ("Chapter 25 List"). I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf.* (Skip Part 2 and sign and complete the Certification below.)
CONTRACT AMENDMENTS AND EXTENSIONS	
☐	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate is listed on the N.J. Department of the Treasury's lists of entities determined to be engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3. I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf.* (Skip Part 2 and sign and complete the Certification below.)
IF UNABLE TO CERTIFY	
☐	*I am unable to certify as above because the person or entity and/or a parent entity, subsidiary, or affiliate is listed on the Department's Russia-Belarus list and/or Chapter 25 Iran list. I will provide a detailed, accurate, and precise description of the activities as directed in Part 2 below, and sign and complete the Certification below. Failure to provide such will prevent the award of the contract to the person or entity, and appropriate penalties, fines, and/or sanctions will be assessed as provided by law.*

Part 2: Additional Information

PLEASE PROVIDE FURTHER INFORMATION RELATED TO PROHIBITED ACTIVITIES IN RUSSIA OR BELARUS AND/OR INVESTMENT ACTIVITIES IN IRAN.

You must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran in the space below and, if needed, on additional sheets provided by you.

Part 3: Certification of True and Complete Information

I, being duly sworn upon my oath, hereby represent and state that the foregoing information and any attachments there, to the best of my knowledge, are true and complete. I attest that I am authorized to execute this certification on behalf of the above-referenced person or entity.

*I acknowledge that the <**Name of Contracting Unit**> is relying on the information contained herein and hereby acknowledge that I am under a continuing obligation from the date of this certification through the completion of any contracts with the <**Name of Contracting Unit**> to notify the <**Name of Contracting Unit**> in writing of any changes to the answers of information contained herein.*

*I acknowledge that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I recognize that I am subject to criminal prosecution under the law and that it will also constitute a material breach of my agreement(s) with the <**Name of Contracting Unit**> and that the <**Name of Contracting Unit**> at its option may declare any contract(s) resulting from this certification void and unenforceable.*

Full Name (Print)	MICHAEL A COMPISI	**Title**	PRESIDENT
Signature		**Date**	9/16/2024

Statement of Suspension or Debarment

STATE OF NEW JERSEY/ STATE OF NEW YORK
Specify, of other

COUNTY OF MONROE

I, MICHAEL COMPISI of the (City, Town, Borough)

of PITTSFORD State of NEW YORK of full age,

being duly sworn according to law on my oath depose and say that:

I am PRESIDENT of the firm

of CAETRA. 10, INC. the Bidder

making the Proposal for the above named projects, and that I executed the said Proposal with full authority to do so; that said Bidder is not at the time of the making this bid included on the New Jersey State Treasurer's or the Federal Government's List of Debarred, Suspended or Disqualified Bidders or the State Department of Labor and Workforce Development; Prevailing Wage Debarment List as a result of action taken by any State or Federal Agency.

Name of Contractor: CAETRA. 10, INC.
(Company Name)

By: _____
(Signature of authorized representative)

Subscribed and sworn to before me

This 16th day of September, 20 24

_____
(Seal) Notary Public of New Jersey/
Specify Other State

My Commission expires 8/31 20 26

KAREN M TROST
Notary Public, State of New York
Qualified In Monroe County
No. 01TR4676206
My Commission Expires August 31, 2026

STATEMENT OF OWNERSHIP DISCLOSURE

N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

Name of Organization: CAETRA.10, INC.
Organization Address: 99 GARNSEY RD, #
City, State, ZIP: PITTSFORD NY 14534

Part I Check the box that represents the type of business organization:

- Sole Proprietorship (skip Parts II and III, execute certification in Part IV)
- Non-Profit Corporation (skip Parts II and III, execute certification in Part IV)
- (X) For-Profit Corporation (any type)
- Limited Liability Company (LLC)
- Partnership
- Limited Partnership
- Limited Liability Partnership (LLP)
- Other (be specific): _____

Part II Check the appropriate box

(X) The list below contains the names and addresses of all stockholders in the corporation who own 10 percent or more of its stock, of any class, or of all individual partners in the partnership who own a 10 percent or greater interest therein, or of all members in the limited liability company who own a 10 percent or greater interest therein, as the case may be. (**COMPLETE THE LIST BELOW IN THIS SECTION**)

OR

( ) No one stockholder in the corporation owns 10 percent or more of its stock, of any class, or no individual partner in the partnership owns a 10 percent or greater interest therein, or no member in the limited liability company owns a 10 percent or greater interest therein, as the case may be. (**SKIP TO PART IV**)

(Please attach additional sheets if more space is needed):

Name of Individual or Business Entity	Home Address (for Individuals) or Business Address
HARRIS BEACH PLLC	99 GARNSEY RD PITTSFORD NY 14534

Part III DISCLOSURE OF 10% OR GREATER OWNERSHIP IN THE STOCKHOLDERS, PARTNERS OR LLC MEMBERS LISTED IN PART II

If a bidder has a direct or indirect parent entity which is publicly traded, and any person holds a 10 percent or greater beneficial interest in the publicly traded parent entity as of the last annual federal Security and Exchange Commission (SEC) or foreign equivalent filing, ownership disclosure can be met by providing links to the website(s) containing the last annual filing(s) with the federal Securities and Exchange Commission (or foreign equivalent) that contain the name and address of each person holding a 10% or greater beneficial interest in the publicly traded parent entity, along with the relevant page numbers of the filing(s) that contain the information on each such person. **Attach additional sheets if more space is needed**.

Website (URL) containing the last annual SEC (or foreign equivalent) filing	Page #'s

Please list the names and addresses of each stockholder, partner or member owning a 10 percent or greater interest in any corresponding corporation, partnership and/or limited liability company (LLC) listed in Part II **other than for any publicly traded parent entities referenced above**. The disclosure shall be continued until names and addresses of every non-corporate stockholder, and individual partner, and member exceeding the 10 percent ownership criteria established pursuant to N.J.S.A. 52:25-24.2 has been listed. **Attach additional sheets if more space is needed.**

Stockholder/Partner/Member and Corresponding Entity Listed in Part II	Home Address (for Individuals) or Business Address
HARRIS BEACH PLLC.	99 GARNSEY RD, PITTSFORD NY 14534

Part IV Certification

I, being duly sworn upon my oath, hereby represent that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I acknowledge: that I am authorized to execute this certification on behalf of the bidder/proposer; that the ***ESCNJ and/or its members*** is relying on the information contained herein and that I am under a continuing obligation from the date of this certification through the completion of any contracts with the ***ESCNJ and/or its members*** to notify the ***ESCNJ and/or its members*** in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the, permitting the ***ESCNJ and/or its members*** to declare any contract(s) resulting from this certification void and unenforceable.

Full Name (Print):	MICHAEL A COMPISI	Title:	PRESIDENT
Signature:		Date:	9/26/2024

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

caetra.io™
Simplifying Compliance, Reducing Risk

CyMetric reflects and facilitates district cybersecurity strategy and drives the process to achieve the overall mission

cymetric™ **RISK MANAGEMENT AND COMPLIANCE PLATFORM**

CyMetric is a one-stop shop for understanding and documenting the strategy, accountability, activities and status of the cybersecurity program.

The CyMetric platform is a centralized repository that:

- Defines activities that satisfy the requirements of state or federal privacy laws or cybersecurity frameworks written in language technology and risk resources understand
- Documents the cybersecurity and privacy program components that District and State stakeholders need to understand
- Directly ties District network and security processes to elements of their cybersecurity and data privacy program
- Produces reports that articulate the status of the program
- Demonstrates progress of the cybersecurity program over time
- Adapts to changes in state laws or mandates by proactively delivering updated program recommendations reflecting the latest guidance

TO LEARN MORE ABOUT HOW CYMETRIC CAN HELP YOU SUPPORT YOUR SCHOOL:

www.caetra.io | (833) 955-4900

CyMetric Functionality Questions and Answers for K-12 School Districts

Numerous state laws require educational agencies to adopt a policy on data security and privacy that aligns with the state's data security and privacy standard. Many states are choosing the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) as the standard for educational agencies but that is not the only option. CyMetric is a risk management and compliance platform that helps schools districts and organizations from any industry define, document, manage, evaluate and evolve their cybersecurity and privacy programs. Additionally, CyMetric is a communication tool that enables technology leaders and Data Protection Officers to communicate district risk and maturity of their cyber/privacy programs to stakeholders leveraging graphical dashboards and reports digestible by non-technical personnel. The following content outlines common questions Caetra.io has been asked by our customers as to the applicability and capabilities of the CyMetric platform.

1. Does Caetra.io have experience working with school districts to help them with risk management and compliance initiatives?

Caetra.io has been working with New York State school districts to assist them with Education law 2-d and 8 NYCRR 121 since 2020 and is also working with other K-12 entities in other states with their cybersecurity and privacy challenges. While the K-12 space is not the only market the CyMetric platforms services, it is a very important vertical for the company. Caetra.io currently has 44 school districts subscribing to the CyMetric platform across multiple states.

K-12 Districts Currently Subscribing to CyMetric		
Beacon CSD	Highland Falls-Fort Montgomery CSD	Port Jervis CSD
Bedford CSD	Honeoye Falls Lima CSD	Poughkeepsie CSD
Berks County Intermediate Unit 14	Hyde Park CSD	Red Hook CSD
Byram Hills CSD	Liberty CSD	Rhinebeck CSD
Dover UFSD	Livingston Manor CSD	Rondout Valley CSD
Dutchess BOCES	Marlboro CSD	Roscoe CSD
East Irondequoit CSD	Monroe Woodbury CSD	Sag Harbor CSD
East Rochester UFSD	Monticello CSD	Spackenkill CSD
Eastern Suffolk BOCES	Northwest Tri-County Intermediate Unit 5	Sullivan County BOCES
Eldred CSD	Oley Valley SD	Sullivan West CSD
Fallsburg CSD	Onteora CSD	Tri Valley CSD
Florida UFSD	Orange-Ulster County BOCES	Washingtonville CSD
Gates Chili CSD	Pawling CSD	Webutuck CSD
Greenwood Lake UFSD	Pine Bush CSD	Yorktown CSD
Highland CSD	Pittsford CSD	

2. How does the product help determine the current profile of a district's cybersecurity activities and at what level?

CyMetric helps Districts, and Educational Service Agencies (ESAs) determine their current cybersecurity profile at several stages during the use of the product through a process of definitions and assessments. Our response will be according to each level.

On boarding and initial engagement with CyMetric

CyMetric has, native to the platform, the ability to define the risk associated with the data stored by each organization. These data elements are associated with systems. From this, the overall risk each system creates for the organization is calculated and reported both on screen and in reports which can be provided to various stakeholders for review and approval. As discussed above, new school district customers can leverage the considerable efforts their district colleagues already utilizing CyMetric and borrow from their information systems inventory list, risk classification of these systems, and the data elements that they store. Accordingly, through this process, each scholastic entity has completed both a FIPS 199 and FIPS 200 risk process for all their student, teacher and principal data storing systems with minimal effort. A comprehensive information system and data map is delivered through this process.

The definition of the systems defined by the above process also automatically generates the required NIST or CIS controls needed to meet the obligations of state privacy and security laws or simply implement best practices. CyMetric allows scholastic entities to uniquely configure the controls they use to satisfy the cybersecurity categories and subcategories described by the NIST CSF to suit their specific risk profile. Again, customers under this agreement will benefit from the work of the other Data Protection Officers (DPO) and also have available to them the default configurations for the controls many of their district peers have chosen for their programs. This is particularly valuable for Districts moving from an ad hoc security program to a programmatic one as some of the definition process will be new to them. This will give new customers a baseline to start from and provide peace of mind that these choices are being used by others as reasonable configurations for district security programs. As their program matures, they can then alter selections to meet the unique needs of their district. For DPOs more versed in this process, they can contribute to and improve the selection choices and advance the security profiles for other Districts.

Finally, CyMetric allows Districts to document the procedures they use to support their security controls which defines how they are implementing the controls that support the NIST CSF and state or federal mandates. CyMetric enables districts to add technical or operational procedures to each control along with assigning ownership of the control to a unique individual or role so that they can ensure procedures are followed and reflect the latest developments in their cybersecurity program. The procedures can be viewed within CyMetric or produced as reports for review and collaboration. Defining proper processes and establishing accountability across

the district promotes broader adoption and execution of the security program supporting compliance initiatives.

Security Program Maintenance and Implementation

A CyMetric feature that has resonated with many of our school district customers is the ability to develop a phased implementation program of their final system security plan. Native to the platform are all the recommended NIST 800-53 controls required to fulfill the five categories of the CSF as well as the privacy requirements of state laws or federal laws should they get passed. Numerous districts have elected to develop the maturity or implementation of some controls faster than others. CyMetric worked with K-12 district DPOs and cybersecurity professionals to segment the CSF controls into four unique phases prioritizing controls that would best address vulnerabilities. This segmentation allows these districts to focus on the controls that best address their immediate risk concerns. The definition of the four phases was produced as a result of audits of several districts along with the domain expertise of cybersecurity professionals that refined the models. Using this approach, the evolution of the program can be measured both against the complete stack of controls required by the law and the phases to show how the program is maturing against the system security plan.

CyMetric helps district personnel keep their program current by easily enabling users to update the system security plan to reflect new systems being brought online, defining new data elements stored in their computing environment, modify risk classifications or even add supplemental security controls to the program to reflect changed circumstances or changes in the threat landscape. CyMetric's structured database ensures that any change to the way a system or control is configured will propagate across the entire platform. This process is typically managed by multiple spreadsheets creating error points that are eliminated by the CyMetric structure. Additionally, if the risk analysis shows that a particular system requires a different approach to that control, the system allows the user to create a unique configuration for that system and create special procedures that apply only to it. Accordingly, the platform is both as general and as specific as it needs to be for every system it supports.

CyMetric also allows users to regenerate their system security plan and procedural documents with a simple wizard. After new controls, configurations, systems, or data types are added, our customers can create new versions of their system security program documentation in less than a minute. Before, with spreadsheets, this could take organizations weeks to accomplish.

Assessments and Audits

An important design function of CyMetric is its association of controls with the unique requirements of each regulation and framework it supports. Because measuring or evaluating controls are the basis for determining compliance, this association is significant because when an organization measures the maturity of its controls, we can automatically measure the overall compliance to a regulation or security framework. Customers can assess their controls either globally across all systems or on a system by system level. This allows CyMetric to report on the organization's overall performance with respect to its compliance obligations or to the security

framework it is seeking to implement. Scoring is automatically calculated and where a control has implementation issues or findings, CyMetric reports on the organization's plan for remediation as well as how that finding impacts the organization's ability to satisfy each requirement of the regulation or framework.

Other approaches to assessments are questionnaire based and solicit interviewee opinion about the organizations' ability to deliver on its responsibilities and capabilities. The primary shortcoming of this approach is that it is not based upon objective measurements of the constituent controls required by the mandate. Accordingly, when a significant cybersecurity event occurs and specific controls are identified as not being properly implemented, the organization will not be able to defend or justify its prior assessments because the individual controls were never actually measured or evaluated in accordance with best practices.

A further power of CyMetric is that it stores each assessment. When performing a new assessment, users can appreciate what was previously determined and either carry those findings forward or edit them to reflect any changes. Utilizing previously evaluated controls saves a significant amount of work and creates efficiencies allowing for districts to do more with less resources.

General Features

- Linking to source documents. CyMetric offers its user several opportunities to create links to external documents. When defining systems, performing assessments or creating procedures, users can, in addition to adding any rich text they deem appropriate, hyper-link to a reference or demonstrative document which is stored on a server or location controlled by the organization. This has two benefits. It allows an organization to maintain "a single source of truth" by keeping only one instance of the reference document. It also reduces risk for the organization because the content is protected in only one place and only those authorized to access that document can do so.
- Multifactor Authentication. Although no student, teacher or principal data is expected to be stored in CyMetric, we still appreciate the risk presented by documenting a system security plan and any findings associated with the controls that support that plan. To protect this information, we have implemented MFA as an option so that users can better protect their information.
- An existing userbase of DPO's and CISO's from neighboring BOCES, RICs and Districts to interact with and improve Districts' cybersecurity programs. Since CyMetric normalizes security and privacy requirements to a set of controls, Districts have a common lexicon and set of activities that they can work with and seek to achieve. No one needs to wonder what others are doing or how they are doing it. They can work together to improve the protection of private data.
- Tracks trends within the district cybersecurity and privacy program by enabling year-to-year comparisons of audits to see how the program is evolving and where resources need to be applied to ensure risks are being properly addressed.

- The CyMetric approach of utilizing a standard set of controls and assessment process allows the consortium to comprehend how the collective group of school districts are performing in the context of their peers. The concept of "big data" is not new but being able to utilize anonymized data to share security program maturity ratings across the statewide audience is very powerful. The consortium can understand how districts in their respective regions are performing and where they are having challenges with implementation. This will help the consortium develop professional development and training programs, negotiate better contracts with third-party vendors who can support districts in the areas where they have deficiencies and keep NYSED informed with overall performance of the state.

3. Can the product generate a Target Profile for common desired cybersecurity outcomes?

Yes. As described above, CyMetric has within it the analysis of the lawyers from Harris Beach PLLC and presents a target profile of desired cybersecurity outcomes to meet various state laws and cyber frameworks designed to protect student and staff data. Goals for effective implementation can be defined at the district level with CyMetric providing reports that define how well the districts are meeting those targets. Moreover, thanks to the efforts of other district DPOs and the BOCES with which they work, there is a phased implementation or maturity plan that lets them execute their programs in defined and manageable stages while measuring how far along they are towards their long-term target profile.

4. Describe how the product can create an action plan to identify necessary steps and prioritize the mitigation of gaps.

CyMetric meets this requirement during the assessment phase described above. In addition to measuring and scoring the functional effectiveness of a control, the assessor can also document any findings or issues discovered regarding the control and score the severity of those issues. Further, the organization has the ability to document its remediation plan and its anticipated closure date. All of this is then produced in an editable Plan of Action and Milestone (POAM) report. The POAM also aligns these findings with the requirements of the regulation or framework the control supports so an organization can appreciate the risks associated with the findings both from a cybersecurity standpoint and from a regulatory perspective.

5. Describe the ease of implementation.

Ease of use and understanding for users at any skill level

The CyMetric tool is generally very easy to use and navigate. It was designed using contemporary approaches to user experience to minimize the training requirements needed to get started. The ease of use from an interface perspective is supported by Caetra.io training programs to help contextualize why districts need to execute processes and procedures that are a part of their respective programs. Technical resources enjoy the benefit of CyMetric's translation of regulatory requirements into procedural language they can understand. CyMetric

promotes collaboration between business units within an organization seeking to support enterprise-wide involvement in the security and compliance process.

Ease of customization, without training or skills required

Customizing system security plans or specific controls to reflect the unique needs of a district is easy to accomplish. Each CyMetric instance reflects the specific environment of a district in terms of the applications, systems and risk profile identified in the security plan. Districts can use a baseline version of controls and control configurations as a starting point but modify those elements as required by their needs. While it is straightforward to make customizations or changes to a district's program without training, the concept of doing so is still covered in the CyMetric training program delivered to users.

Ease of IT Administration, integration of Directory Services and/or access management system

As a cloud-based application, CyMetric is easily managed and configured. Users can be added or removed from the system depending upon their role and all of this is managed from a dashboard. CyMetric is a completely independent and secure system protected by its own two factor authentication process so that even if the organization suffers a breach, the CyMetric platform will remain self-contained. As a result, CyMetric does not integrate with Directory Services or other access management systems and users will need their own unique passwords.

6. What is the ability of the application to show the level of risk across all activities? Explain

CyMetric has the ability to demonstrate the level of risk across all activities in two ways. First, the platform has a risk module where customers can identify and document risks their information systems pose to the organization. The second way the level of risk is identified is during an assessment. As described above, the organization can document and rank in terms of severity, the implication of any findings associated with a control or process. Since the controls are further associated by the Harris Beach attorneys to the regulation or framework, any defects or gaps in the framework or regulation are revealed and understood by the organization. Moreover, since the risk is expressed in both cybersecurity and legal terms, the risk can be appreciated by a broader group of stakeholders. CyMetric's entire approach is a legal or risk-based methodology. It is unique in its ability to deliver on this requirement.

7. How does the product help prioritize and scope the school district's business objectives and priorities?

CyMetric helps prioritize and scope a school district's business objectives and priorities initially by phasing the maturity plan for the controls that will ultimately comprise the entire system security and privacy plan that supports state laws and cyber framework objectives. This phased strategy was developed by District DPOs and ESA experts and reflects the priorities and scope for each phase that were deemed most important. While this approach reflects the considered prioritization and scope of a few regions, it does not need to be the exclusive plan for all Districts

on the platform. CyMetric has the capability of creating different phased plans depending upon the risks and priorities of different ESA or other supporting entities. Districts have also prioritized their efforts based upon the mission criticality of the systems within their environment. Caetra.io does not have any influence on what those systems are but the CyMetric platform supports whatever priority criteria the districts move forward with.

Following an assessment, CyMetric can further help scope and prioritize the District's objectives by allowing it to prioritize the findings deemed either most significant or the controls viewed as least mature. Since all of these controls are ultimately mapped back to the regulations and frameworks which require them, the school district's business and legal obligations are both appreciated and able to be met.

8. Describe how the product can audit and manage district data privacy policies to align with current policies?

CyMetric has built into it the ability to generate program documents that set forth all the actions a scholastic entity must perform to meet the security and privacy requirements of their cyber security program or state laws. In the event that there are no standard controls that address privacy or notification requirements, the attorneys at our partner Harris Beach create special controls that meet the privacy requirements or custom needs of a cyber security mandate or program objective. Thus, unlike products that support only the NIST CSF, CyMetric executes on all the legal requirements of any law. CyMetric is the only platform that has these custom privacy controls integrated into the general security plan which has been vetted by a law firm. This fulfills our vision of allowing our customers to focus on the activities of security and privacy and let the product take over the function of demonstrating and aligning those activities with policies and the law. As with other aspects of the assessment process, the data privacy and notification elements of the law are also a part of the audit function facilitated by the CyMetric platform.

9. Describe the alignment with functions-controls-processes?

At its core, CyMetric is a control, procedure and process driven platform in its approach to security and data privacy. The policy and standards documents are then created from this set of controls so there is always perfect alignment between all three. Mechanistically at the customer level, CyMetric's database stores the inventory of the district's systems and controls required for those systems. Further, the controls are directly associated with the regulation or framework the organization is trying to meet ensuring the alignment between the systems, controls and procedures needed for meeting obligations. From this, general standards or policy documents are created with language created from templates created by the lawyers at Harris Beach. The policy or standards language integrated into CyMetric is essentially a wrapper surrounding the controls and processes the organization intends to implement. An added benefit of the product is that after new systems or compliance obligations are added, a simple refresh button can be clicked and all the policies, functions and controls are updated, with version control to reflect those changes. These processes and capabilities ensure that alignment is always current.

10. Provide a description of your training model and support system.

Implementation/Onboarding Support: Due to the cloud-based architecture of the CyMetric platform, there is no hardware or software implementation requirements to get CyMetric up and running. To assist with expedited deployment and rapid time to value, Caetra.io offers its school software title inventory with its corresponding baseline data mapping and data risk profile to all school districts that use the CyMetric platform. School districts will select the software titles they use in their district and Caetra.io will import those titles into their specific instance of the CyMetric platform. This process expedites district onboarding reducing significant data entry time in documenting and mapping their environment. It also facilitates the production of deliverables required by the state.

Additionally, should districts require supplemental resources outside of their districts, Caetra.io's network of service provider partners and domain experts/consultants can be introduced to provide immediate and ongoing support for districts to get them where they need to go.

Training: Caetra.io has developed a three-phase, web-based training program specific to K-12 entities that it has already implemented and delivered to existing customers. The CyMetric application also has substantial in-app/online support tools available for users to utilize for self-service training. CyMetric incorporates the use of Intercom, an online support tool enabling customers to contact Caetra.io support via an instant messaging chat function for real-time support with Caetra.io personnel. Intercom also has built-in support documentation detailing product use guidance as well as configuration, operational, and other business considerations.

On-Going Support: Caetra.io strives to ensure its customers are fully equipped to maximize their investment in the CyMetric platform. In addition to onboarding training, online tools and tutorials are continually being added to the platform to support on-going education and use case support.

Regional based refresh/new feature trainings could be scheduled to ensure all personnel are current with the use and capability of the CyMetric platform.

Additional features and functions will be added to CyMetric over time based upon our current development road map and input from the CyMetric user base. Caetra.io produces outbound newsletter announcements of feature enhancements, insights on scenario use-case functionality and scheduled maintenance as a practice to ensure customers are informed on all matters related to CyMetric. Caetra.io will also share insights from our business partner/ownership group law firm that are relevant to the K-12 school district community.

System security - Security Updates and Patch schedules

The application is designed and implemented using modern security design implementation patterns. Customer data is encrypted at rest and TLS is enforced on all communications from the browser to the application instance.

Each quarter, the application dependencies are reviewed and updated to ensure all known security issues are addressed. In addition, new critical security issues are addressed as soon as identified and an analysis indicates the issue impacts the platform.

The application leverages a public 3rd party cryptographic library to authenticate each user during the server-side logon process. Once a user is authenticated, an authorization token is generated and managed via an expiring JavaScript web token (jwt). The jwt and associated server-side allow list validate each request is authorized. Authorization is further enforced at the server and database level to limit access to relevant customer data. On user logout or session expiration, the token is invalidated and purged from the allow list.

11. Does the product have the multi-tenant capability to manage all districts from a single platform?

Because each district is required to have its own security and privacy program in place, all districts/ESAs will have their own instance of the CyMetric application. Districts can invite external entities (ESAs/Third-Party vendors) to access the district instance to provide inputs, assessments and other functions in support of the districts. The inverse of this is also accurate where an ESA can be the principal manager of a district instance and invite school district personnel to the district's discrete CyMetric instance. A true multi-tenant model is not available at the time.

12. Describe the compatibility with other systems.

While our platform is designed to support APIs and uses APIs in its operation, it is a self-contained platform that allows its customers to design policies, system security plans to document their computing environment to assess their security and privacy controls independent of other systems. To date, software products that monitor system security and network status do not currently associate security activities with unique controls rendering compatibility as not an essential element to the automation of the CyMetric platform. Should network security and network monitoring products evolve to accomplish that objective, Caetra.io could align that capability with the CyMetric platform.

13. What other features does the platform bring to the table?

Regulation Monitoring: The lawyers of Harris Beach provide ongoing management and insight to the list of controls associated with the regulation so that as regulations or their interpretation change, the list is updated to reflect the law firm's latest understanding of the legal requirements of each regulation. The monitoring of regulations and the controls is not something districts need to manage as Caetra.io and the CyMetric platform will take care of that for them. School districts or any other organization have the ability to accept or reject these recommendations depending upon the advice they receive from their counsel or the special circumstances of their system environment.

14. How does Caetra.io price the CyMetric platform?

Caetra.io offers its CyMetric platform as a compliance-as-a-service subscription license model. The annual subscription price is based upon the regulation a customer is seeking to comply with. There is no limit to the number of users that can access the tool, no limit on the number of systems that can be populated into the platform or any other limitation that may be imposed by

other platforms. For the purposes of this proposal, the license structure is based upon district acquisition for Education Law 2-d and its regulatory element, 8 NYCRR Part 121 along with the four "phases" of CSF controls that have been designed by a team of New York State school district DPOs to assist with building a structured system security program in manageable phases. The latter of these options is optional to utilize.

Caetra.io has crafted an aggressive pricing schedule for school districts across New York State. Pricing is based upon school district size to accommodate challenges districts have based upon their respective sizes as well as accommodate any services that may be required to support the tool.

15. Is any software required on the client to optimally use your software?

Only an industry standard browser (Chrome, Microsoft Edge, Firefox, Apple Safari) is required to use CyMetric.

CyMetric Talking Points for K-12 School Districts

Mission: Risk Reduction. The primary District goal is to implement cyber frameworks (e.g. NIST CSF) as well as state required control elements into a data security and privacy program. However, there may be areas of specific risk that a District may want to address as a priority like ransomware or cybersecurity insurance acquisition. CyMetric's built in flexibility enables Education Service Agencies (ESAs) and Districts the capability to focus their implementation strategy on immediate threats and risks most important to Districts and thus phase their implementation of the program in a way that is achievable and meaningful. Moreover, since a framework is a prism for viewing the controls that define the functions of the framework, it allows for the custom design of controls that address the functions of the framework without being constrained to a one size fits all approach. ESAs can define custom control sets based on functions within the framework that target specific threat vectors (ransomware) or business focused risk factors (cybersecurity insurance) to address specific needs.

SHORT TERM:

- Questionnaire or environmental assessment-based solutions tend to provide a superficial look at where an organization is with its security program implementation. The execution or measurement of a program cannot be achieved without understanding what activities or controls need to be fulfilled at the system level.
- For public schools, CyMetric defines all of the elements and tasks necessary to meet state mandates out of the box.
- Enables the inventorying of software/hardware assets along with a detailed data map with associated risk profiles. Much of this inventory definition can be automated leveraging the work of other data protection officers.
- Automatically generates framework controls AND the controls for complying with a state's data privacy and notification requirements. CyMetric is the only tool that can supply both the framework control set and the state privacy and notification control sets required to meet the expectations of the law.
- Aligns the controls to the specific elements of the framework and state laws that are being satisfied by the implemented controls - **all legally vetted by a nationally recognized law firm ensuring the output supports the requirements of the law.**
- Standardizing the approach to meeting the compliance obligation makes supporting the mandate easier to manage from an ESA perspective while allowing for District resources to share the workload.
- Dynamically produces procedural/departmental policy documents that reflect the requirements of your district and of state mandates.
- CyMetric does not limit the number of users who can access and interact with the platform. Unlimited district internal and external resources can use CyMetric as a part of their program execution.

- Supports custom phases of implementation for control sets. Districts can work at a pace they define with a set of controls that will form the foundation of their program while they work toward full compliance over time. This allows for setting achievable, realistic goals that districts can accomplish and report on. Beyond this, Districts can add additional controls to address any unique risk they may encounter.

MEDIUM TERM:

- When districts are ready to evaluate or assess their cyber/privacy program, CyMetric automatically assembles the controls that need to be audited in one repository eliminating the need for multiple spreadsheets. The tool also enables users to define how and what they are auditing enabling documentation of the program that is used for reporting. CyMetric produces detailed reports and highlights remediation plans for issues with the program found during the assessment process (Plan of Action and Milestone – POAM Report) along with a dashboard highlighting the status of the program.
- Districts can farm out work (control evaluation, gap analysis, policy review, etc.) to external sources to offload some of the management of their compliance program.
- If states alter the requirements of the law or indicates areas of focus for auditing the program, CyMetric updates the platform automatically to ensure districts programs are current with the latest control sets.
- Districts can enhance their individual programs with supplemental controls that address specific needs or risks they have.

LONG TERM:

- Districts can review previous audits/assessments to track their program over time looking for trends or other data points that provide insight on their program.
- In some cases, specific control assessments can be repurposed/reapplied to their audits without having to re-evaluate the control.
- Should a District need to develop compliance programs for other obligations (e.g. NY SHIELD, HIPAA, CPRA, etc.), CyMetric aligns those obligations to the controls already in place consolidating multiple programs reducing the workload to add a new obligation.
- ESAs have visibility into their component District bases to produce reports that allow for regional comparisons with their peer groups. Also, ESAs will be able to see regional trends or needs that may warrant enhanced services that can be provided by the ESA (e.g. professional development programs, new security tools to offer, etc.).



cymetric™

Don't let cybersecurity compliance place your district at risk.

Reduce District risk with CyMetric, a cloud-based delivery tool for ongoing regulatory guidance and security program management.

- Creates a common core for compliance across regions while allowing for district independence
- Automate the development of your standards, practices and procedures for your data privacy and cybersecurity program
- Enables the development of multi-year implementation models to phase in a program that supports district risk and system priorities
- Deploy, assess and evolve your program based upon your system risk, available resources and regulatory or security framework requirements

Protect personal identifiable information and sensitive data with an automated tool enabling you to ace your compliance objectives.

Visit us: www.caetra.io **Book a demo: 833.955.4900**

caetra.io™ Simplifying Compliance. Reducing Risk.

cymetric™

www.caetra.io

How does it benefit the school district?

One of the biggest challenges with any regulation or cybersecurity program is translating it into actions needed to be taken by an organization to meet the law or program requirements.

Cybersecurity frameworks like the NIST CSF, are high level models that provide guidance on security/operational areas (Identify/Protect/Detect/Respond/Recover) that organizations need to focus on in order to have a robust data security program. Frameworks generally do not provide any insight as to how to accomplish that goal – leaving districts having to guess as to how to meet the framework's goals.

CYMETRIC TAKES THE GUESSWORK OUT OF THE PROCESS

Defines processes and controls that satisfy the requirements of your cyber program

- By defining specific processes, procedures and functions (controls) that need to be put into place, CyMetric gives technology directors at the district level (or educational service agency) explicit direction in a language they can understand.

Meets requirement for system inventory to support audits

- The tool outputs system security plan documents that define the data privacy and data security program to which each district attests. All functions and capabilities have been legally vetted by nationally recognized law firm Harris Beach PLLC. to ensure the software platform satisfies the applicable laws that are licensed.

Provides assessment mechanism tool integrated into the platform

- Once districts become empowered to evaluate the implementation and status of the program at the control level, school boards can understand where risks lie and how to prioritize them with their available resources. Caetra.io, the company that provides CyMetric, also provides regulation monitoring to update and reflect any changes to the law or guidance on its implementation with respect to state privacy and data security laws.

From an educational service agency (ESA) perspective, the goal is to create a baseline standard for compliance programs across their region (in place of unique programs for each district) that can be better supported through value-added services potentially delivered from the ESA. Each district can customize their programs based upon their unique circumstances; but the core will be consistent.

caetra.io™
Simplifying Compliance, Reducing Risk



How does CyMetric Work?

The essence of CyMetric is that it translates the legal requirements of any regulation or standard into discrete actions that an IT group can both understand and implement. Further, it allows the customer to measure how well their cybersecurity and privacy program is implemented so that the strength or maturity of it can be gauged. CyMetric produces a set of specific controls or processes which support not only the security requirements or supported regulations but also the unique privacy requirements of each law as well. These controls are selected from the National Institute of Standards and Technologies (NIST) SP 800-53 publication, the Center for Internet Security v8 control set or were written and validated by attorneys at a nationally recognized law firm.

CyMetric does the following:

1. Automates the definition of processes and controls that satisfy regulatory or security framework requirements eliminating the need for organization personnel or lawyers to translate the regulation or company policy documents.

2. Standardizes compliance programs on a single set of processes, procedures and controls enabling organizations to easily incorporate other compliance requirements (e.g. NY SHIELD, HIPAA, GDPR, CCPA/CPRA, CMMC) into their program if the need arises.

3. Meets the standard requirement for system inventory and data classification to support audits. CyMetric can leverage outputs from other tools that define software and hardware assets and import them into CyMetric eliminating significant amounts of data entry required to develop an asset inventory.

4. Provides a program assessment mechanism tool integrated into the platform enabling organizations to migrate away from spreadsheet-based program management.

5. Supports the dynamic nature of cybersecurity and privacy program requirements. By creating a centralized repository for all facets of the program, company programs stay current with the changing threat landscape. Updating program documentation and adjusting parameters of their security profile is managed by a few clicks of a mouse. Program evaluation content, system reports, supporting artifacts and documents are easily accessible for facts on demand.

6. Allows for establishing designed phases for program implementation so organizations can build their program in a manageable and time appropriate manner based upon available resources, budget and other factors.

7. Increases efficiency by enabling an unlimited number of users access to the tool at the organizational level. Organizations are free to leverage their internal human assets as well as external resources like consultants and third-party vendors to help manage their programs.

8. Tracks trends within the organization's cybersecurity and privacy program by enabling year-to-year comparisons of audits to see how the program is evolving and where resources need to be applied to ensure risks are being properly addressed.



STAKEHOLDERS

Every control or defined procedure is directly associated with the elements of the regulation it has mapped to. Accordingly, an organization and its many stakeholders understand not only the discrete requirements of these protection functions, but also how, when viewed as a whole, the security program is performing. Thus, for the technologists, they know exactly what they need to do to improve the program and can fully document the procedures they will use to implement each control. For stakeholders who are less technologically focused, they can see a visualization of the program arranged around the requirements of a regulation or security program they are implementing.

CyMetric also delivers all of the required elements specified in the myriad regulations imposed on organizations: asset inventory of information systems, documentation of the data types or information types stored within the organization's environment, plus assigns a risk profile to those assets. Additionally, CyMetric outputs policy and procedural documents that define organizational cybersecurity and privacy programs in support of company policies.

Lastly, CyMetric provides the mechanism to define how well the cybersecurity and privacy program has been implemented through an audit or assessment process evaluating the processes and procedures defined by the program. The outputs from the assessment process present stakeholders with insight as to what aspects of their program are well defined and where there are risks/exposures that need to be addressed. With the relative nascence of most cybersecurity and privacy mandates, should regulators, government agencies or any other entity make changes to the requirements of the law or what a company should be doing to meet the requirements of the law, Caetra.io will monitor for any such changes in the regulation and will push out updates to CyMetric customers. This will ensure that they always have the latest recommendations on how to comply with the law.



ASSESSMENT

An important design function of CyMetric is its association of controls with the unique requirements of each regulation and framework it supports. Because measuring or evaluating controls is the basis for determining compliance, this association is significant because when an organization measures the maturity of its controls, CyMetric can automatically measure the overall compliance to a regulation or security framework. Customers can assess their controls either globally across all systems or on a system by system level. This allows CyMetric to report on the organization's overall performance with respect to its compliance obligations or to the security framework it is seeking to implement. Scoring is automatically calculated and where a control has implementation issues or findings, CyMetric reports on the organization's plan for remediation as well as how that finding impacts the organization's ability to satisfy each requirement of the regulation or framework.

Other approaches to assessments are questionnaire based and solicit interviewee opinion about the organizations' ability to deliver on its responsibilities and capabilities. The primary shortcoming of this approach is that it is not based upon objective measurements of the constituent controls required by the mandate. Accordingly, when a significant cybersecurity event occurs and specific controls are identified as not being properly implemented, the organization will not be able to defend or justify its prior assessments because the individual controls were never actually measured or evaluated in accordance with best practices.

In addition to measuring and scoring the functional effectiveness of a control, the assessor can also document any findings or issues discovered regarding the control and score the severity of those issues. Further, the organization has the ability to document its remediation plan and its anticipated

closure date. All of this is then produced in an editable Plan of Action and Milestone (POAM) report. The POAM also aligns these findings with the requirements of the regulation or framework the control supports so an organization can appreciate the risks associated with the findings both from a cybersecurity standpoint and from a regulatory perspective.



POSITIVE OUTCOMES

Today's hyper-networked and highly-regulated world asks more and more of the executives that conduct business in it. Business leaders need to depend on their technology infrastructure to keep the bad actors at bay and rely on their compliance personnel to monitor the many regulations designed to protect the data they keep. CyMetric integrates the law into the software, producing controls and policies that meet the rigor required by the regulations and align with the technology infrastructure needs outlined by industry standards. CyMetric reduces the dependency on legal counsel to craft controls and policies that may be undermined or even redundant.

By leveraging CyMetric, not only to build your controls and policies but also to update them as regulations change, your compliance personnel can focus their efforts on more impactful initiatives; and your company can focus on strategic initiatives to grow the business.

Contact Us



Email: contact@caetra.io

Phone: 833.955.4900

cymetric™

Caetra.io CyMetric Risk Management Platform Overview

The essence of CyMetric is that it translates the requirements of any regulation or cyber security standard into discrete actions that an IT group can both implement and understand. Further, it allows the customer to measure how well their cybersecurity and privacy program is implemented so that the strength or maturity of it can be gauged. For the school districts and Educational Service Agencies (ESA), CyMetric prescribes a set of specific controls or processes that align to industry standard cyber frameworks like the NIST CSF and SOC2 as well as control sets like Center for Internet Security (CIS) and NIST 800-53. Additionally, the CyMetric platform also is able to provide regulatory insight on aligning with state or federal mandates focused on privacy, notification and other contemporary requirements that do not have standard controls that address them. These custom privacy and notification-oriented controls were written and validated by attorneys at our business partner, the Harris Beach PLLC law firm and integrated into the CyMetric platform ensuring that regulatory compliance is part of the solution. Any federal or state mandate or custom requirement (cyber insurance, contractual obligations, etc.) can be mapped within CyMetric providing a roadmap to meeting those business or operational requirements.

Every control or defined procedure is directly associated with either the elements of a regulation or the preferred cyber framework the organization is implementing. Accordingly, a school district and its many stakeholders understand not only the discrete requirements of these protection functions, but also how, when viewed as a whole, the security program is performing. Thus, for the technologists, they know exactly what they need to do to improve the program and can fully document the procedures they will use to implement each control. For stakeholders who are less technologically focused, they can see a visualization of the program arranged around the requirements of a regulation or cyber framework.

CyMetric delivers insight on how to comply with all of the required elements specified in state and federal privacy and cyber security laws: asset inventory of information systems, documentation of the data types or information types stored within the school districts' environment, plus assigns a risk profile to those assets. Additionally, CyMetric outputs standards/procedural documents that define districts' cybersecurity and privacy programs in support of district policies. Lastly, CyMetric provides the mechanism to define how well the cybersecurity and privacy program has been implemented through an audit or assessment process evaluating the processes and procedures defined by the program. The outputs from the assessment process present stakeholders with insight as to what aspects of their program are well defined and where there are risks/exposures that need to be addressed. With the relative nascence of cyber security and privacy laws, these mandates can be fairly fluid. Should state or federal agencies make changes to the requirements of a mandate or what an organization should

be doing to meet the requirements of the mandate, Caetra.io will monitor for any such changes in the regulation and will push out updates to CyMetric customers. This will ensure that they always have the latest recommendations on how to comply with the law.

CyMetric is currently being used by over 45 New York school districts to meet the requirements of Part 121, Education Law 2-d and the NIST CSF. In working with the various Data Protection Officers from our customer base, Caetra.io has integrated into its CyMetric platform an optional, phased implementation model for the controls required by these standards. This model is based upon a general risk assessment of the schools and an agreed upon prioritization of the controls. The phased implementation model enables districts to focus their initiatives on mission critical applications and priority controls at program initiation while building upon that model as their resources and budget permit. Districts can maximize the value of their efforts while collaborating with their colleagues in other school districts on how to best implement each control.

CyMetric streamlines cybersecurity efforts school districts.

CyMetric does the following:

- Automates the definition of processes and controls that satisfy the regulatory requirements, cyber/privacy program objectives, cyber insurance requirements and cyber framework objectives eliminating the need for district personnel or lawyers to translate the regulation or district policy documents.
- Standardizes compliance programs on a single set of processes, procedures and controls enabling districts to easily incorporate other compliance requirements (e.g. NY SHIELD, HIPAA) into their program if the need arises.
- Meets the requirement for system inventory and data classification to support audits. Leveraging a Caetra.io managed inventory of over 1500 software titles, school districts select which systems they utilize in their environment which are, in turn, imported into CyMetric eliminating significant amounts of data entry required to develop an asset inventory.
- Provides a program assessment mechanism tool integrated into the platform enabling districts to migrate away from spreadsheet-based program management.
- Supports the dynamic nature of cybersecurity and privacy program requirements. By creating a centralized repository for all facets of the program, district programs stay current with the changing threat landscape. Updating program documentation and adjusting parameters of their security profile is managed by a few clicks of a mouse. Program evaluation content, system reports, supporting artifacts and documents are easily accessible for facts on demand.
- Allows for establishing designed phases for program implementation so districts can build their program in a manageable and time appropriate manner based upon available resources, budget and other factors.

- Increases efficiency by enabling an unlimited number of users access the tool at the district level. Districts are free to leverage their internal human assets as well as external resources like Education Service Agency personnel and third-party vendors to help manage their programs.
- Tracks trends within the district cybersecurity and privacy program by enabling year-to-year comparisons of audits to see how the program is evolving and where resources need to be applied to ensure risks are being properly addressed.

CyMetric is developed from the ground up with optimal security and privacy processes in place.

Customer data security, integrity, and availability are essential elements of the CyMetric application. CyMetric is architected and designed to ensure customer data is protected from access and disclosure to unauthorized external and internal entities. As part of Caetra's continual efforts, the CyMetric application undergoes periodic 'white hat' penetration testing to identify any possible areas of weakness and to ensure they are not exploitable. Finally, the Caetra Operations team has enacted internal policies and procedures to ensure employees follow industry standards for protecting and preventing unauthorized disclosure of customer data.

The CyMetric application is built with technologies used by many Fortune 1000 companies. The application is designed and implemented using modern security design implementation patterns. Customer data is encrypted at rest and TLS is enforced on all communications from the browser to the application instance. Security certificates ensure the information cannot be decrypted or subverted by external parties.

Each quarter, the application dependencies are reviewed and updated to make certain all known security issues are addressed. In addition, new critical security issues are addressed as soon as identified and an analysis indicates how the issue impacts the platform.

The application leverages a public 3rd party cryptographic library to authenticate each user during the server-side logon process. Once a user is authenticated, an authorization token is generated and managed via an expiring JavaScript web token (jwt). The jwt and associated server-side "allow list" validates each request is authorized. Authorization is further enforced at the server and database level to limit access to relevant customer data. On user logout or session expiration, the token is invalidated and purged from the allow list.

The CyMetric software stack is hosted on Heroku's Platform as a Service (PaaS) offering. Heroku has a dedicated security team constantly monitoring and updating the platform as needed. Due to the nature of PaaS, Heroku's security policies are automatically applied to CyMetric.

In addition, CyMetric uses several Amazon Web Service (AWS) offerings to securely store certain types of customer data such as compliance report pdfs and images in an external cloud service. Further, the CyMetric application ensures that the information stored in the AWS platform is protected by implementing AWS best practices for identity and access management (IAM) and 'least privilege' authorization by enforcing the minimal level of user rights required to perform the user's role.

The CyMetric application provides strong data security built into its architecture. All customer provided compliance data is stored in a Postgres (PostgreSQL) database hosted on Heroku. Postgres is a mature relational database with strong security features utilizing industry best practices ensuring the data is secure. To ensure that customer data is protected at the customer, user, and database levels the CyMetric application uses Postgres' private schemas providing isolation of customer data, role-based access control limiting access to the database, and row level security restricting access within the database. Lastly, all Postgres database data files and backups are 'encrypted at rest' where the data is encrypted on the disk as well as in the shared buffers to ensure that the data cannot be accessed outside of the application.

Data protection and disaster recovery measures ensure that the CyMetric application and customer data will be available and recoverable in the event a catastrophic incident impacting the data center hosting CyMetric. CyMetric builds on Heroku and Amazon's native durability, availability, and disaster recovery services. This, combined with the Caetra Operations Team's recovery procedures, ensures that Caetra is able to transfer data from backups to alternative data centers and restart the application with limited manual actions.

What platforms does the product work in?

CyMetric is a cloud-based software as a service platform. As such, CyMetric works on any platform that supports a web browser.

What are the technical requirements?

CyMetric is a cloud-based application and requires no technical infrastructure, hardware or other components to be installed or put into place in order to utilize the application. CyMetric does require the use of a contemporary web browser to run effectively. The web browsers currently supported by CyMetric are:

- Google Chrome
- Microsoft Edge
- Apple Safari
- Mozilla Firefox

Browsers should be running the most recent versions provided by the manufacturer to maximize security and browser capability.

Part E – Signature Forms: Caetra.io, Inc.

AEPA 025-F
Cyber Security and Training



Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7. Clean Air Act and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended, contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein.		
Respondent Certification (By Item)	**Respondent Certification:** YES, I agree	**Initial**
1. Violation of Contract Terms and Conditions	YES, I AGREE	MAC
2. Termination for Cause of Convenience	YES, I AGREE	MAC
3. Equal Employment Opportunity	YES, I AGREE	MAC
4. Davis-Bacon Act	YES, I AGREE	MAC
5. Contract Work Hours and Safety Standards Act	YES, I AGREE	MAC
6. Right to Inventions Made Under a Contract or Agreement	YES, I AGREE	MAC
7. Clean Air Act and Federal Water Pollution Control Act	YES, I AGREE	MAC
8. Debarment and Suspension	YES, I AGREE.	MAC
9. Byrd Anti-Lobbying Amendment	YES, I AGREE	MAC
10. Procurement of Recovered Materials	YES, I AGREE	MAC
11. Profit as a Separate Element of Price	YES, I AGREE	MAC
12. General Compliance with Participating Agencies	YES, I AGREE	MAC
13. Governing Law; Forum Selection.	YES, I AGREE	MAC

CAETRA.IO, INC.
Name of Business

Signature of Authorized Representative

MICHAEL A. COMPISI
Printed Name

9/16/2024
Date

Solicitation Affidavit

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

MICHAEL A. COMPISI	99 GARNSEY RD
Authorized Representative (Please print or type)	Mailing Address
PRESIDENT	PITTSFORD NY 14534
Title (Please print or type)	City, State, Zip
[signature]	9/16/2024
Signature of Authorized Representative	Date

Acceptance of Solicitation & Contract

Association of Educational PURCHASING AGENCIES

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	CAETRA • IO, INC	**Date**	9/15/2024
Address	99 GARNSEY RD	**City, State Zip**	PITTSFORD NY 14534
Contact Person	MICHAEL COMPISI	**Title**	PRESIDENT
Authorized Signature	Michael S	**Title**	PRESIDENT
Email	MCOMPISI@CAETRA.IO	**Phone**	585.955.4905

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Solicitation Checklist

Instructions: Utilize the checklist below, reviewing to confirm that all the required documents have been uploaded to Public Purchase, in their ***specified/required format***, by the due date and time listed for this solicitation. ***Submissions not following the specified/required format may result in being marked non-responsive and may not be considered for evaluation.*** Respondents are reminded that failure to follow, comply with, and adhere to the enclosed instructions of this solicitation may result in their response being deemed non-responsive. AEPA, its Member Agencies, affiliate agencies, and authorized representatives are not responsible for bid proposals that are incomplete, unreadable, or received after the solicitation deadline submission date.

"x"	**Document Title, Uploaded to Bonfire** *(Respondent must submit documents in the required title/format)*	**Format of Uploaded Document**	**Notes**
	Bid Bond – if Required, see Part A if applicable.	Upload PDF copy of the bid security.	The original bid security must be received by Lakes Country Service Cooperative by due date and time.
	Part C – State-Specific Forms – ***Name of Responding Company***	Single, Scanned PDF	**New Jersey Only Requirement.** Signatures Required.
X	**Part D - Questionnaire –** ***Name of Responding Company*** Includes: ● Company Information ● Service Questionnaire ● Exceptions ● Deviations	Single, Scanned PDF	**Required.**
X	**Part E – Signature Forms –** ***Name of Responding Company*** Includes: ● Uniform Guidance "EDGAR" Certification ● Solicitation Affidavit ● Acceptance of Solicitation & Contract	Single, Scanned PDF	**Required.** Signatures required.
X	**Part F – Pricing Schedule –** ***Name of Responding Company***	Excel Workbook	**Required.**
X	**Price List and/or Catalog –** ***Name of Responding Company***	Upload PDF	**Required.**
X	**Exhibit A – Marketing Plan –** ***Name of Responding Company***	Scanned PDF	**Optional.** Form not provided by AEPA, Respondent Created

Contents

1-CDW Government AEPA RFP 025 Marketing Plan 2024 1
1-DB CDWG New Jersey Affirmative Action Questionnaire 7
2-DB CDWG New Jersey Assurance of Compliance 9
3-DB CDWG New Jersey Exhibit A Mandatory Equal Opportunity Language 10
4-DB CDWG New Jersey Debarment Form 11
5-DB CDWG New Jersey Political Contribution Disclosure Form 12
6-DB CDWG New Jersey Russia Belarus Activities and Iran Investment Activ 16
7-DB CDWG New Jersey Statement of Ownership Disclosure 19
8-CDWG New Jersey Americans with Disabilities Act 21
APPENDIX A 21
1-CDW Government AEPA RFP 025 Cybersecurity Exceptions 22
2-CDW Locations Listing 23
3-CDW Sales Team 27
CDW Education Sales Team 27
Education Leadership Team 28
Slide Number 3 29
EDU Sales Support 30
EDU Sales Support 31
Higher Education Leadership & Inside Account Managers 32
HiEd Regional Leaders West 33
HiEd Pacific Region 34
HiEd Northwest Region 35
HiEd For Profit 36
HiEd West Field Team 37
HiEd Regional Leaders Central 38
HiEd Gulf Coast Region 39
HiEd Dairyland Region 40
HiEd Midwest Region 41
HiEd Ohio Valley Region 42
HiEd Regional Leaders East 43
HiEd South East Region 44
HiEd Atlantic Region 45
HiEd Northeast Region 46
HiEd HBCU 47
HiEd East Field Team 48

K12 Leadership & Inside Account Managers 49
K12 Regional Leaders West 50
K12 Western States Region 51
K12 California North 52
K12 California South 53
K12 California Field Team 54
K12 Regional Leaders Central 55
K12 Heartland Region 56
K12 North Central Region 57
K12 Ohio Valley Region 58
K12 Midwest Region 59
K12 Central Field Team 60
K12 Regional Leaders South 61
K12 Gulf Coast Region 62
K12 Texas Majors 63
K12 Texas Territory 64
K12 South Field Team 65
K12 Regional Leaders Northeast 66
K12 Keystone Region 67
K12 New England Region 68
K12 New York Region 69
K12 Northeast Field Team 70
K12 Regional Leaders Southeast 71
K12 Atlantic Region 72
K12 Southeast Region 73
K12 Southeast FL/GA Region 74
K12 Southeast Field Team 75
Education Academy/Residency Leaders & Inside Account Managers 76
EDU Regional Leaders Academy/Residency 77
K12 Residency 78
HiEd Residency 79
Shelton Residency 80
HiEd Academy 81
K12 Academy 82
Education Customer Enablement Team 83
EDU Customer Enablement Team 84
EDU Customer Enablement Team 85
CDW Amplified for Education 86

EDU Customer Enablement Team 87
EDU Customer Enablement Team 88
Amplified for Education 89
Amplified IT for Education 90
Amplified IT for Education 91
AIT Sales Enablement Team 92
EDU Customer Enablement Team 93
AIT Sales Enablement Team 94
Customer Enablement, Education Solutions Team 95
Slide Number 70 96
Customer Enablement, CDW Local Education Solutions 97
EDU Customer Enablement Team 98
K12 Google Customer Success Team 99
Slide Number 74 100
EDU Customer Enablement Team 101
Slide Number 76 102
Slide Number 77 103
EDU Customer Enablement Team 104
Education Business Development 105
Slide Number 80 106
Education Additional Resources 107
EDU Project Management Team 108
Education Maps 109
Campus Intern Coverage Map 110
THANK YOU! 111
4-CDW Government AEPA RFP 025 Proposal Response 112
CDW Government Overview 115
Large Onsite Inventories 116
CDW Cybersecurity Risk Management Services 117
Breadth of Capabilities 117
Cyber Security and Training Solutions 119
Technology Training with CDW 119
Security Solutions 121
Our Knowledge Goes Deep 121
Meet Our Security Experts 122
Security Assessment Team 122
Security Delivery Engineers 122
Data Loss Prevention Solution Architects 122

Security Solution Architects 122
Certifications 123
Our World-Class Technology Partnerships 126
Attachments 127
Attachment A: CDW Security Capabilities 127
Attachment B: CDW_WFD Catalog 127
Attachment A: CDW Security Capabilities (11 pages) 128
Attachment B: CDW_WFD Catalog (93 pages) 140
CDW_WFD Catalog - Limited_CybrS and IT_Framew.pdf
Category: Cyber Security 144
Administering Information Protection and Compliance in Microsoft 365 (SC-400T00) 145
View schedule and pricing on cdw.com 145
Advanced Linux Kernel Internals 147
View schedule and pricing on cdw.com 147
Android Attack and Defend 148
View schedule and pricing on cdw.com 148
Assembly for Reverse Engineers 149
View schedule and pricing on cdw.com 149
Attacking and Securing Java / JEE Web Applications 150
View schedule and pricing on cdw.com 150
Automated Network Defense 152
View schedule and pricing on cdw.com 152
Related Courses: 152
Behavioral Malware Analysis 153
View schedule and pricing on cdw.com 153
CAP: Certified Authorization Professional 154
View schedule and pricing on cdw.com 154
CBROPS - Understanding Cisco Cybersecurity Operations Fundamentals 155
View schedule and pricing on cdw.com 155
CCSP: Certified Cloud Security Professional 157
View schedule and pricing on cdw.com 157
Certified CMMC Professional (CCP) 158
View schedule and pricing on cdw.com 158
CISSP: Certified Information Systems Security Professional 159
View schedule and pricing on cdw.com 159
CompTIA Advanced Security Practitioner (CASP+) 161

View schedule and pricing on cdw.com 161
CompTIA Cyber Security Analyst (CySA+) 162
View schedule and pricing on cdw.com 162
CompTIA PenTest+ 163
View schedule and pricing on cdw.com 163
CompTIA Security+ 164
View schedule and pricing on cdw.com 164
CSSLP: Certified Secure Software Lifecycle 165
View schedule and pricing on cdw.com 165
Cyber Risk Management Overview 167
View schedule and pricing on cdw.com 167
DevSecOps for Security Practitioners 168
View schedule and pricing on cdw.com 168
EC Council Certified Ethical Hacker (CEH) 170
View schedule and pricing on cdw.com 170
EC Council Certified Hacking Forensic Investigator (CHFI) 172
View schedule and pricing on cdw.com 172
EC Council Certified Network Defender (CND) 174
View schedule and pricing on cdw.com 174
EC-Council ICS SCADA Cybersecurity 175
View schedule and pricing on cdw.com 175
Endpoint Live Forensics 176
View schedule and pricing on cdw.com 176
Evasive Techniques and Breaching Defenses 177
View schedule and pricing on cdw.com 177
Event Monitoring and Incident Detection 178
View schedule and pricing on cdw.com 178
Exploring the OWASP Top 10 180
View schedule and pricing on cdw.com 180
Hacker Methodologies for Security Professionals 182
View schedule and pricing on cdw.com 182
HCISPP: HealthCare Information Security and Privacy Practitioner 183
View schedule and pricing on cdw.com 183
Incident Analysis 184
View schedule and pricing on cdw.com 184
Related Courses: 185
Introduction to Security Analysis 186

View schedule and pricing on cdw.com 186
iOS Attack and Defend 187
View schedule and pricing on cdw.com 187
ISACA Certified Information Security Manager (CISM) 188
View schedule and pricing on cdw.com 188
Linux Kernel Internals 189
View schedule and pricing on cdw.com 189
Machine Learning Operations (MLOps) and AI Security 190
View schedule and pricing on cdw.com 190
Malware Reverse Engineering 192
View schedule and pricing on cdw.com 192
Microsoft Azure Security Technologies (AZ-500T00) 193
View schedule and pricing on cdw.com 193
Microsoft Cybersecurity Architect (SC-100T00) 195
View schedule and pricing on cdw.com 195
Microsoft Identity and Access Administrator (SC-300T00) 197
View schedule and pricing on cdw.com 197
Microsoft Security Operations Analyst (SC-200T00) 199
View schedule and pricing on cdw.com 199
Microsoft Security, Compliance, and Identity Fundamentals (SC-900T00) 201
View schedule and pricing on cdw.com 201
Network Forensics and Investigation I 202
View schedule and pricing on cdw.com 202
Related Courses: 202
Network Forensics and Investigation II 204
View schedule and pricing on cdw.com 204
Related Courses 204
OffSec PEN-200 - Penetration Testing with Kali Linux (OSCP) 205
View schedule and pricing on cdw.com 205
Python for Reverse Engineers 206
View schedule and pricing on cdw.com 206
Related Courses 206
SCOR - Implementing and Operating Cisco Security Core Technologies 207
View schedule and pricing on cdw.com 207
Secure Web App Development Overview - Java / JEE 209
View schedule and pricing on cdw.com 209

Securing Web Applications Overview 211
View schedule and pricing on cdw.com 211
Security Engineering on AWS 213
View schedule and pricing on cdw.com 213
SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention 214
View schedule and pricing on cdw.com 214
SISE - Implementing and Configuring Cisco Identity Services Engine 216
View schedule and pricing on cdw.com 216
SSCP: Systems Security Certified Practitioner 218
View schedule and pricing on cdw.com 218
Threat Hunting with Python 219
View schedule and pricing on cdw.com 219
Related Courses 219
Understanding Operating Systems 220
View schedule and pricing on cdw.com 220
Category: IT and Security Frameworks 221
Application Security and Development (STIG) 222
View schedule and pricing on cdw.com 222
Certified CMMC Professional (CCP) 224
View schedule and pricing on cdw.com 224
CompTIA A+ 225
View schedule and pricing on cdw.com 225
Related Courses 226
Database Security (STIG) 227
View schedule and pricing on cdw.com 227
HCISPP: HealthCare Information Security and Privacy Practitioner 229
View schedule and pricing on cdw.com 229
Information Assurance (STIG) Overview 230
View schedule and pricing on cdw.com 230
ISACA Certified Information Security Manager (CISM) 232
View schedule and pricing on cdw.com 232
ITIL Foundation 233
View schedule and pricing on cdw.com 233
1-DB 21-F - Cyber Security Training Part E Signature Forms 235

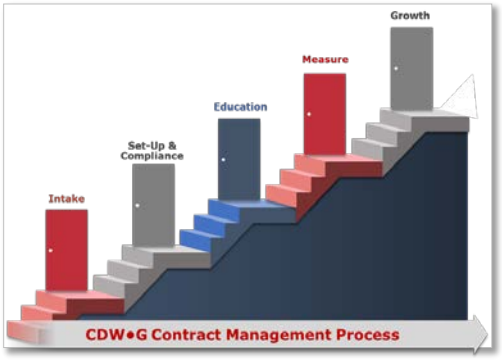
AEPA Marketing Plan Draft

Since 2003, CDW•G has worked closely with AEPA and its members to forge deep, customer relationships that act as the foundation for our mutual success. Coupled with our marketing capabilities and committed sales force, we have driven year over year contract growth. And in this time, we've gained extensive knowledge around AEPA members' needs. We have used this knowledge to create custom solutions to achieve customers' objectives. This relentless focus on innovation and our customer intimacy provide CDW•G with unparalleled insight in preparing an effective market plan – one that promotes growth and new user adoption. If awarded, our in-depth marketing approach offers the national reach and resources of a Fortune 500 company while maintaining focused member attention to address nuanced requirements.

We look forward to continuing our partnership with AEPA. To this effect, we have outlined an integrated marketing plan that seeks to seamlessly maintain current members while simultaneously expanding contract sales without sacrificing customer support.

Ensuring Contract Vibrancy and Relevance (Our Capabilities and Resources)

Specialized Resources



Some vendors, even large suppliers, do not dedicate resources to contract management. Instead, these companies rely on the sales team to manage compliance issues and reporting. We can imagine that this results in delayed responses, unreliable support, and in worst cases, faulty reporting.

CDW•G understands the role that vendor contract management plays in the member experience and reputation of a major cooperative like AEPA. Therefore, we invest significantly in the quality and reliability of our contract management process. We deploy a systematic yet adaptive approach that spans the contract lifecycle – ensuring contact vibrancy and longevity. The following five phases comprise this approach: Intake, Set-up & Compliance, Education, Measure, and Growth.

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW•G").

To support this process, we maintain an ecosystem of dedicated coworkers, CDW•G's program management department. This team is singularly devoted to managing contract, distinct from those responsibilities of our sales force. Members of the program management department work full-time to maintain contract compliance and administer contract procedures, including contract launch. Keeping our contract management within one group makes oversight and structured processes easy to implement, allowing CDW•G to standardize our contract management processes and share best practices – in turn reducing risks and improving efficiencies.



CDW•G's Program Manager, **Jeff Hagen**, has an in-depth working knowledge of AEPA's Technology Contract structure and member landscape. If awarded, he will collaborate with CDW•G's marketing department to create awareness and training campaigns to enable our national sales force.

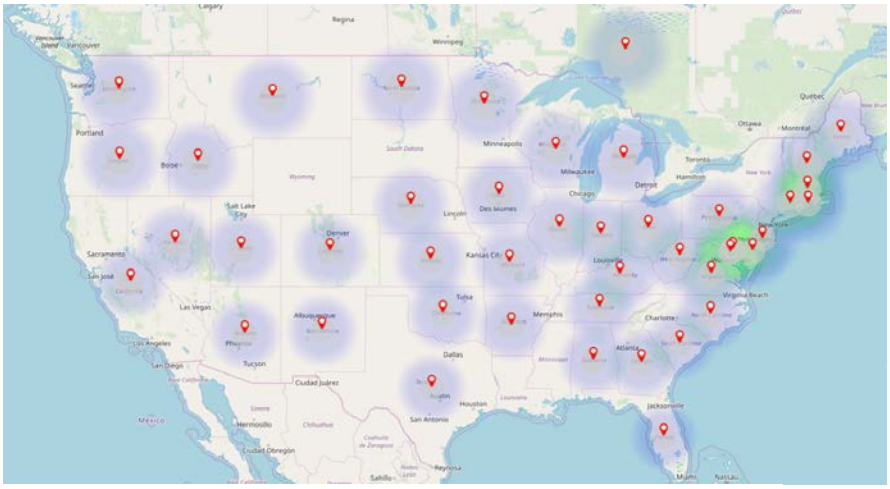
Established, Tenured Sales Force

AEPA agreements offer their users the simplicity, efficiency, and value of a national cooperative while accommodating the nuanced, region-specific members. Likewise, at CDW•G we structure our sales organization to address the unique needs of our customers based on their segment and region.

- First, our inside account managers and our field sellers are trained to **become experts within the public sector segment they support** – K-12, Higher Education, State & Local government, Federal government and Healthcare.
- To further support their customers, we have **divided the salesforce into distinct geographic regions** to ensure that sellers are prepared to support the local landscape.
- There are **over 1,000 sales coworkers and over 1,600 total coworkers** serving State, Local, and Education customers.

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW•G").



Map depicts geographic coverage of all coworkers supporting CDW•G.

We create an optimal customer experience by fostering collaboration and genuine investment in our customer's goals. While we may have a national presence, we operate at the local level – dedicated to creating true impact for each customer. Many larger organizations may see this expanded sales force and their expertise as an unnecessary expense but, at CDW•G, we believe collaboration with our customers is the foundation to our mutual success.

Our Marketing Solutions

Recognized industry-wide for their technology solutions campaigns, our marketing team was recently named a finalist for Content Marketing Project of the Year by the Content Marketing Institute, the largest and longest-running international content marketing awards program in the world.



Our marketing team offers several solutions to support our AEPA marketing strategy. These include:

- **Advertising & Cobranded Materials.** CDW•G can work with AEPA and member agencies to develop customer facing collateral (digital and print) and email campaigns.
- **Customer Webinars and Events.** Topical webinars and events allow AEPA members to see, hear and participate in discussion events on topics ranging from security to classroom transformation.
- **Publications.** CDW•G partners with industry experts to publish sector-specific online and hardcopy magazines for State (StateTech), K-12 (EdTech Focus on K-12) and Higher Education (EdTech Focus on Higher Education) customers.

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW•G").

- **Corporate Communications** CDW•G can generate a spotlight media piece detailing the CDW•G AEPA Agreement. These can be shared with coworkers and select media publications.
- **Omnichannel Marketing.** Engaging across multiple platforms such as social media, applications, email, and blogs connects us with current and potential customers on more touchpoints. Done well, omnichannel marketing creates an enhanced user experience and cohesive brand message that drives people to action.
- **Artificial Intelligence and Smart Messaging.** CDW•G's Strategic Initiatives practice leads our AI and smart messaging efforts with the aid of Kronologic. Using AI and scripted messaging strategy, Kronologic syncs AEPA members and their dedicated account manager to help distribute contract, product and services updates while taking the next step to schedule one-on-one conversations at the convenience of the customer. Using integrated management and reporting tools, Kronologic assists with booking meetings – including scheduling, rescheduling and proposing new times.
- **Influencer Marketing and Social Messaging Apps.** CDW•G leverages a coworker advocacy tool that spans social media. Known as the CDW Social Squad, it engages coworkers across the company and provides access to curated social media content that is ready to share across their personal social media networks, including LinkedIn, Twitter, and Facebook.
- **Video Marketing.** Video marketing is one of, if not the most important trend today. In a survey done by Impactbnc.com, 68% of respondents replied that they most preferred to learn about a new product or service via short video. CDW•G has the ability to facilitate video marketing campaigns to promote contract awareness and adoption

Aligned with our contract management process, we have developed a prescriptive go-to-market to position the AEPA and CDW•G value-add to customers, current and new, across our State and Local, and Education segments. Our messaging will include the following themes:

- Increased value in the form of savings
- Extensive, quality, product and services catalog
- A proven, successful partnership between AEPA and CDW•G
- Streamlined contract maintenance – reduce burden on administrative resources
- Consultative, holistic approach to achieve the goals of our customers and their communities
- Enhanced user experience and customer service
- IT Procurement Solution with National Reach yet Local Focus

Seamless Agreement Transition (Contract Launch Process)

Internal Contract Set-Up and Compliance

Seamless transition from the previous agreement to the new agreement is critical to success, as it secures the foundation necessary for continued success. Upon award, CDW•G will efficiently transition AEPA member agencies from the current contract to the new contract, as we have the framework in place to ensure seamless transition. Contract stand-up also includes creation of

Commented [EW1]: This needs to be updated.

Commented [EW2]: Shorten this section

Commented [EH3]: Do we still use Kronologic?

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW•G").

internal and external resources to aid our customers and sales teams in transitioning to the new agreements. Our sellers will be fully equipped to aid members with the transition and Jeff Hagen will also be accessible to address questions from AEPA members. We will update our existing contract landing page (accessible at: cdwg.com/AEPA022) to reflect any additional capabilities related to AEPA RFP #025. We have already created a sample contract landing page that is ready to go live on Day 1. Please access it at: cdwg.com/AEPA022

Commented [EH4]: This landing page still works. Should we revise as noted?

Seller Awareness, Training, and Enablement

The first step in our awareness and transition plan is to train our salesforce on the new agreement. Sales enablement training will cover contract scope, membership and new contract requirements so that they can not only inform their customers, but also help them to navigate the new landscape. Our sellers will then be equipped with relevant collateral to inform members.

Such collateral includes digital emails, as well as digital and printed documents. Collateral will communicate the details of the new agreement, reiterate the benefits of the contract vehicles, and showcase products, services, and solutions available to members. Once trained, our account team will drive awareness through call and email campaigns to aid current members transition seamlessly to the new agreement.

Existing Member Awareness and Transition

Often in times of change, customers become concerned about the impending contract expiration and its implications for their business. As a current AEPA technology provider with a direct line to current members, CDW•G can prevent this estrangement. Our account managers act as expert resources for members for recommendations on technology as well as which contracts to purchase them on. The size of our salesforce coupled with their customer intimacy will allow us to quickly and efficiently manage the agreement transition while positioning members for growth. Additionally, our reporting capabilities ensure that we have the necessary customer information to successfully implement member-focused awareness campaigns. Our sales force, program management practice, familiarity with the contract, and detailed launch plan act to eliminate any potential transition pains.

Contract Acceleration Process (Growth)

AEPA benefits its members through innovative sourcing which provides members access to a wide range of brands at competitive discounts while also eliminating the time and cost associated with bid creation and solicitations. AEPA assumes the administrative workload which frees up its members to focus on strategic initiatives. At CDW•G, we help to amplify these benefits through our sales, program management, and marketing capabilities.

Building on AEPA's innovation, CDW•G will help to recruit new members through enablement and engagement activities that showcase the benefits of the AEPA and CDW•G partnership. Aiding customers in consolidating their contract portfolio into a few, or even one contract, removes complexity and positions the AEPA Technology Catalog contract as a single source for members' technology needs. CDW•G can aid this effort through its extensive sales presence, reporting capabilities, focused account planning, and strategic, segment-oriented resources.

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW•G").

Target Identification

Accurate customer identification is at the core of an effective recruitment campaign. It allows us to align resources and marketing initiatives around those customers whose needs align with the benefits of the AEPA contract. We have automated many aspects of the reporting process so that data informs the way we do business, especially in contract promotion. We will use our capabilities to identify those existing members and eligible customers who can benefit from the AEPA Technology Catalog contract (e.g., those consistently releasing individual bids, those managing diverse and complicated contract portfolios). Equipped with this information, we can ensure that we optimize our potential to grow the contract.

Account Development

Our business development teams work with customers to define opportunities, better understand the needs and challenges of today and tomorrow and bring resources and expertise from across CDW•G to help customers visualize and create solutions that meet the needs of their mission. Our business development team will work in conjunction with our account teams to pinpoint those accounts with the most potential for growth. For each target customer, we will develop a business plan that addresses their needs while leveraging the AEPA contract. Tactical areas of consideration will include eProcurement and web preferences, supplier diversity requirements, current and future IT projects, piggyback agreements with custom terms, co-branded marketing campaigns, and topical webinars.

Specialized Resources

To aid our business development and account teams, CDW•G maintains coworkers dedicated to specific solution areas. As accounts mature and expand, our business development and accounts teams will integrate these coworkers into their account development plans to foster further growth. These coworkers specialize in the following solution areas:

- eSports
- Classroom Transformation
- Connected Campus
- Cybersecurity
- Public Safety

Conclusion

We are continually working to expand the AEPA footprint among eligible customers, opening up new avenues for adoption. Our marketing efforts are fully committed to generating organic growth for the next contract iteration while maintaining the positive brand image AEPA has established. We appreciate the collaboration and look forward to the opportunity to continue our partnership.

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW•G").

AFFIRMATIVE ACTION QUESTIONNAIRE

1. Our company has a federal Affirmative Action Plan approval. ☑ Yes ☐ No

If yes, please attach a copy of the plan to this questionnaire.

2. Our company has a New Jersey State Certificate of Employee Information Report. ☑ Yes ☐ No

If yes, please attach a copy of the certificate to this questionnaire.

3. If you answered "***NO"*** to both questions above, No. 1 and 2, you must apply for an Affirmative Action Employee Information Report – Form AA302.

Please visit the New Jersey Department of Treasury website for the Division of Public Contracts Equal Employment Opportunity Compliance:

https://www.nj.gov/treasury/contract_compliance/

a. Click on "Employee Information Report"
b. Complete and submit the form with the *appropriate payment* to:

Department of Treasury
Division of Purchase and Property
Contract Compliance and Audit Unit
EEO Monitoring P.O. Box 206
Trenton, New Jersey 08625-0206

All fees for this application are to be paid directly to the State of New Jersey. A copy shall be submitted to the ESCNJ prior to the execution or award of contract.

I certify that the above information is correct to the best of my knowledge.

Name of Company/Firm CDW Government LLC

Address 230 N. Milwaukee Avenue
City, State, Zip Vernon Hills, IL 60061

Name of Authorized Agent Dario Bertocchi Title VP Contracting Operations
SIGNATURE _____ Date 9/11/24

U.S. Department of Labor

Office of Federal Contract Compliance Programs
Chicago District Office
230 South Dearborn Street Suite 434
Chicago, IL 60604

Sent via Email

April 21, 2020 R00301025

Christina Leahy
President and CEO
CDW Government LLC
75 Tristate International
Lincolnshire, IL 60069-4420

Dear Ms. Leahy:

The U.S. Department of Labor, Office of Federal Contract Compliance Programs (OFCCP), recently completed a compliance evaluation of your equal employment opportunity policies and practices at CDW Government LLC, 75 Tristate International, Lincolnshire, IL 60069-4420

During the compliance evaluation process, we found no apparent violations of Executive Order 11246, as amended; Section 503 of the Rehabilitation Act of 1973, as amended; the Vietnam Era Veterans' Readjustment Assistance Act of 1974, as amended; or Executive Order 13496. The Director of OFCCP or the Regional Director may modify this determination within 45 calendar days of the issuance of this letter.

OFCCP appreciates the cooperation of you and your staff as well as the timely submission of requested documents during the conduct of the compliance review.

Sincerely,

Tim Roark

Timothy Roark
Acting District Director

cc via email: Angelia Green, Sr. Inclusion Specialist at angeg@cdw.com

ASSURANCE OF COMPLIANCE

Contact with Students

There may be times during the performance of this contract, where a contracted service provider may come in contact with students of the school district. The district fully understands it obligation to provide to all students and staff members, a safe educational environment. To this end, the district is requiring all bidders to sign a statement of Assurance of Compliance, acknowledging the bidder's understanding of the below listed requirements and further acknowledging the bidder's assurance of compliance with those listed requirements.

Anti-Bullying Reporting--Requirement

When applicable, the contracted service provider shall comply with all applicable provisions of the New Jersey Anti-Bullying Bill of Rights Act—N.J.S.A. 18A:37-13.1 et seq., all applicable code and regulations, and the Anti-Bullying Policy of the Board of Education. In accordance with N.J.A.C. 6A:16-7.7 (c), a contracted service provider, who has witnessed, or has reliable information that a student has been subject to harassment, intimidation, or bullying shall immediately report the incident to any school administrator or safe schools resource officer, or the School Business Administrator/Board Secretary.

Criminal History Background Checks—N.J.S.A. 18A:6-7.1--Requirement

When applicable, the contracted service provider, shall provide to the school district prior to commencement of contract, evidence or proof that each employee assigned to provide services and that comes in **regular contact** with students, has had a criminal history background check, and furthermore, that said background check indicates that no criminal history record information exists on file for that worker. Failure to provide a proof of criminal history background check for any employee coming in regular contact with students, prior to commencement of contact, may be cause for breach of contract. See NJDOE Broadcast 9/9/19.

Pre-Employment Requirements

When applicable, all contracted service providers, whose employees have **regular contact with students**, shall comply with the Pre-Employment Requirements in accordance with New Jersey P.L. 2018 c.5, N.J.S.A. 18A:6-7.6 et seq. Contracted service providers are to review the following New Jersey Department of Education Office of Student Protection—Pre-Employment Resource P.L. 2018 c.5 link below for guidance and compliance procedures.

https://www.nj.gov/education/crimhist/preemployment/

Name of Company CDW Governmnet LLC

Name of Authorized Representative Dario Bertocchi

Signature  Date VP Contracting Operations

(Revised: January, 2016)

EXHIBIT A
MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE
N.J.S.A. 10:5-31 et seq. (P.L. 1975, C. 127)
N.J.A.C. 17:27
GOODS, PROFESSIONAL SERVICE AND GENERAL SERVICE CONTRACTS

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Except with respect to affectional or sexual orientation and gender identity or expression, the contractor will ensure that equal employment opportunity is afforded to such applicants in recruitment and employment, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Such equal employment opportunity shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this nondiscrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex.

The contractor or subcontractor will send to each labor union, with which it has a collective bargaining agreement, a notice, to be provided by the agency contracting officer, advising the labor union of the contractor's commitments under this chapter and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to N.J.S.A. 10:5-31 et seq., as amended and supplemented from time to time and the Americans with Disabilities Act.

The contractor or subcontractor agrees to make good faith efforts to meet targeted county employment goals established in accordance with N.J.A.C. 17:27-5.2.

The contractor or subcontractor agrees to inform in writing its appropriate recruitment agencies including, but not limited to, employment agencies, placement bureaus, colleges, universities, and labor unions, that it does not discriminate on the basis of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job related testing, as established by the statutes and court decisions of the State of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

In conforming with the targeted employment goals, the contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and layoff to ensure that all such actions are taken without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The contractor shall submit to the public agency, after notification of award but prior to execution of a goods and services contract, one of the following three documents:

- Letter of Federal Affirmative Action Plan Approval
- Certificate of Employee Information Report
- Employee Information Report Form AA302 (electronically provided by the Division and distributed to the public agency through the Division's website at https://www.nj.gov/treasury/contract_compliance/

The contractor and its subcontractors shall furnish such reports or other documents to the Division of Purchase & Property, CCAU, EEO Monitoring Program as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Division of Purchase & Property, CCAU, EEO Monitoring Program for conducting an investigation pursuant to N.J.A.C. 17:27-1.1 et seq.

Company CDW Government LLC Name Dario Bertocchi

Signature  Title VP Contracting Operations

Statement of Suspension or Debarment

STATE OF NEW JERSEY/ Connecticut
Specify, of other

COUNTY OF Fairfield

I, Dario Bertocchi **of the (City, Town, Borough)**

of _____ **State of** Connecticut **of full age,**

being duly sworn according to law on my oath depose and say that:

I am VP Contracting Operations **of the firm**

of CDW Government LLC **the Bidder**

making the Proposal for the above named projects, and that I executed the said Proposal with full authority to do so; that said Bidder is not at the time of the making this bid included on the New Jersey State Treasurer's or the Federal Government's List of Debarred, Suspended or Disqualified Bidders or the State Department of Labor and Workforce Development; Prevailing Wage Debarment List as a result of action taken by any State or Federal Agency.

Name of Contractor: CDW Government LLC
(Company Name)

By: _____
(Signature of authorized representative)

Subscribed and sworn to before me

This 11th **day of** Sept **, 20** 24

Carmen Castro
_____
(Seal) Notary Public of CT/
Specify Other State

CARMEN CASTRO
STATE OF CONNECTICUT
NOTARY PUBLIC
COMMISSION #SNPC.0183170
EXPIRES FEBRUARY 28, 2026

My Commission expires 02/28 **20** 24

CARMEN CASTRO
Notary Public, State of Connecticut
My Commission Expires 02/28/2026

Educational Services Commission of New Jersey

Business Office

1660 Stelton Road, Floor 2
Piscataway, New Jersey 08854

Chapter 271
Political Contribution Disclosure Form

(Contracts that Exceed $17,500.00)
Ref. N.J.S.A. 19:44A-20.26

The undersigned, being authorized and knowledgeable of the circumstances, does hereby certify that _____(Business Entity) has made the following **reportable** political contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26 during the twelve (12) months preceding this award of contract:

Reportable Contributions

Date of Contribution	Amount of Contribution	Name of Recipient Elected Official/ Committee/Candidate	Name of Contributor

The Business Entity may attach additional pages if needed.

_____

☑**No Reportable Contributions** (Please check (✔) if applicable.)

I certify that CDW Government LLC (Business Entity) made no reportable contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26.

Certification

I certify that the information provided above is in full compliance with Public law 2005 – Chapter 271.

Name of Authorized Agent Dario Bertocchi

Signature _____ Title VP Contracting Operations

Business Entity CDW Government LLC

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

Contractor Instructions

Business entities (contractors) receiving contracts from a public agency that are NOT awarded pursuant to a "fair and open" process (defined at N.J.S.A. 19:44A-20.7) are subject to the provisions of P.L. 2005, c. 271, s. 2 (N.J.S.A. 19:44A-20.26). This law provides that 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

- any State, county, or municipal committee of a political party
- any legislative leadership committee*[1]
- any continuing political committee (a.k.a., political action committee)
- any candidate committee of a candidate for, or holder of, an elective office:
    - of the public entity awarding the contract
    - of that county in which that public entity is located
    - of another public entity within that county
    - or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county

The disclosure must list reportable contributions to any of the committees that exceed $300 per election cycle that were made during the 12 months prior to award of the contract. See N.J.S.A. 19:44A-8 and 19:44A-16 for more details on reportable contributions.

N.J.S.A. 19:44A-20.26 itemizes the parties from whom contributions must be disclosed when a business entity is not a natural person. This includes the following:

- individuals with an "interest" ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit
- all principals, partners, officers, or directors of the business entity or their spouses
- any subsidiaries directly or indirectly controlled by the business entity
- IRS Code Section 527 New Jersey based organizations, directly or indirectly controlled by the business entity and filing as continuing political committees, (PACs)

When the business entity is a natural person, "a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity." [N.J.S.A. 19:44A-20.26(b)]. The contributor must be listed on the disclosure.

Any business entity that fails to comply with the disclosure provisions shall be subject to a fine imposed by ELEC in an amount to be determined by the Commission which may be based upon the amount that the business entity failed to report.

The enclosed list of agencies is provided to assist the contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor's responsibility to identify the specific committees to which contributions may have been made and need to be disclosed. The disclosed information may exceed the minimum requirement.

The enclosed form, a content-consistent facsimile, or an electronic data file containing the required details (along with a signed over sheet) may be used as the contractor's submission and is disclosable to the public under the Open Public Records Act.

The contractor must also complete the attached Stockholder Disclosure Certification. This will assist the agency in meeting its obligations under the law. **NOTE: This section does not apply to Board of Education contracts.**

P.L. 2005, c. 271

[1] N.J.S.A. 19:44A-3(s): "The term "legislative leadership committee" means a committee established, authorized to be established, or designated by the President of the Senate, the Minority Leader of the Senate, the Speaker of the General Assembly or the Minority Leader of the General Assembly pursuant to section 16 of P.L. 1993, c. 65 (C. 19:44A-10.1) for the purpose of receiving contributions and making expenditures."

(Unofficial version, Assembly Committee Substitute to A-3013, First Reprint*)

AN ACT authorizing units of local government to impose limits on political contributions by contractors and supplementing Title 40A of the New Jersey Statutes and Title 19 of the Revised Statutes.

BE IT ENACTED by the Senate and General Assembly of the State of New Jersey:

40A:11-51 1. a. A county, municipality, independent authority, board of education, or fire district is hereby authorized to establish by ordinance, resolution or regulation, as may be appropriate, measures limiting the awarding of public contracts there from to business entities that have made a contribution pursuant to P.L. 1973, c. 83 (C. 19:44A-1 et seq.) and limiting the contributions that the holders of a contract can make during the term of a contract, notwithstanding the provisions and parameters of sections 1 through 12 of P.L. 2004, c. 19 (C. 19:44A-20.2 et al.) and section 22 of P.L. 1973, c. 83 (C. 19:44A-22).

b. The provisions of P.L. 2004, c. 19 shall not be construed to supersede or preempt any ordinance, resolution or regulation of a unit of local government that limits political contributions by business entities performing or seeking to perform government contracts. Any ordinance, resolution or regulation in effect on the effective date of P.L. 2004, c. 19 shall remain in effect and those adopted after that effective date shall be valid and enforceable.

c. An ordinance, resolution or regulation adopted or promulgated as provided in this section shall be filed with the Secretary of State.

19:44A-20.26 2. a. Not later than 10 days prior to entering into any contract having an anticipated value in excess of $17,500, except for a contract that is required by law to be publicly advertised for bids, a State agency, county, municipality, independent authority, board of education, or fire district shall require any business entity bidding thereon or negotiating therefor, to submit along with its bid or price quote, a list of political contributions as set forth in this subsection that are reportable by the recipient pursuant to the provisions of P.L. 1973, c. 83 (C.19:44A-1 et seq.) and that were made by the business entity during the preceding 12 month period, along with the date and amount of each contribution and the name of the recipient of each contribution. A business entity contracting with a State agency shall disclose contributions to any State, county, or municipal committee of a political party, legislative leadership committee, candidate committee of a candidate for, or holder of, a State elective office, or any continuing political committee. A business entity contracting with a county, municipality, independent authority, other than an independent authority that is a State agency, board of education, or fire district shall disclose contributions to: any State, county, or municipal committee of a political party; any legislative leadership committee; or any candidate committee of a candidate for, or holder of, and elective office of that public entity, of that county in which that public entity is located, of another public entity within that county, or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county, or any continuing political committee.

The provisions of this section shall not apply to a contract when a public emergency requires the immediate delivery of goods or services.

b. When a business entity is a natural person, a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by any person or other business entity having an interest therein shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by: all principals, partners, officers, or directors of the business entity or their spouses; any subsidiaries directly or indirectly controlled by the business entity; or any political organization organized under section 527 of the Internal Revenue Code that is directly or indirectly controlled by the business entity, other than a candidate committee, election fund, or political party committee, shall be deemed to be a contribution by the business entity.

c. As used in this section:
"business entity" means a natural or legal person, business corporation, professional services corporation, limited liability company, partnership, limited partnership, business trust, association or any other legal commercial entity organized under the laws of this State or of any other state or foreign jurisdiction;

"interest" means the ownership or control of more than 10% of the profits or assets of a business entity of 10% of the stock in the case of a business entity that is a corporation for profit, as appropriate; and

P.L. 2005, c. 271

"State agency" means any of the principal departments in the Executive Branch of the State Government, and any division, board, bureau, office, commission or other instrumentality within or created by such department, the Legislature of the State and any

office, board, bureau or commission within or created by the Legislative Branch, and any independent State authority, commission, instrumentality or agency.

d. Any business entity that fails to comply with the provisions of this section shall be subject to a fine imposed by the New Jersey Election Law Enforcement Commission in an amount to be determined by the commission which may be based upon the amount that the business entity failed to report.

19:44A-20.13 3. a. Any business entity making a contribution of money or any other thing of value, including an in-kind contribution, or pledge to make a contribution of any kind to a candidate for or the holder of any public office having ultimate responsibility for the awarding of public contracts, or to a political party committee, legislative leadership committee, political committee or continuing political committee, which has received in any calendar year $50,000 or more in the aggregate through agreements or contracts with a public entity, shall file an annual disclosure statement with the New Jersey Election Law Enforcement Commission, established pursuant to section 5 of P.L. 1973, c. 83 (C. 19:44A-5), setting forth all such contributions made by the business entity during the 12 months prior to the reporting deadline.

b. The commission shall prescribe forms and procedures for the reporting required in subsection a. of this section which shall include,
but not be limited to:

(1) the name and mailing address of the business entity making the contribution, and the amount contributed during the 12 months prior to the reporting deadline;

(2) the name of the candidate for or the holder of any public office having ultimate responsibility for the awarding of public contracts, candidate committee, joint candidates committee, political party committee, legislative leadership committee, political committee or continuing political committee receiving the contribution; and

(3) the amount of money the business entity received from the public entity through contract or agreement, the dates, and information identifying each contract or agreement and describing the goods, services or equipment provided or property sold.

c. The commission shall maintain a list of such reports for public inspection both at its office and through its Internet site.

d. When a business entity is a natural person, a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by any person or other business entity having an interest therein shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by: all principals, partners, officers, or directors of the business entity, or their spouses; any subsidiaries directly or indirectly controlled by the business entity; or any political organization organized under section 527 of the Internal Revenue Code that is directly or indirectly controlled by the business entity, other than a candidate committee, election fund, or political party committee, shall be deemed to be a contribution by the business entity.

As used in this section:

"Business entity" means a natural or legal person, business corporation, professional services corporation, limited liability company, partnership, limited partnership, business trust, association or any other legal commercial entity organized under the laws of this State or of any other state or foreign jurisdiction; and

"Interest" means the ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit, as appropriate.

e. Any business entity that fails to comply with the provisions of this section shall be subject to a fine imposed by the New Jersey Election Law Enforcement Commission in an amount to be determined by the commission which may be based upon the amount that the business entity failed to report.

4. This act shall take effect immediately.

*Note: Bold italicized statutory references of new sections are anticipated and not final as of the time this document was prepared. Statutory compilations of N.J.S.A. 18A:18A-51 is anticipated to show a reference to N.J.S.A. 40:11-51 and to N.J.S.A. 19:44A-20.26.

Prohibited Russia-Belarus Activities & Iran Investment Activities

Person or Entity	CDW Government LLC

Part 1: Certification

COMPLETE PART 1 BY CHECKING **ONE OF THE THREE BOXES BELOW**

Pursuant to law, any person or entity that is a successful bidder or proposer, or otherwise proposes to enter into or renew a contract, for goods or services must complete the certification below prior to contract award to attest, under penalty of perjury, that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list or Chapter 25 list as a person or entity engaging in prohibited activities in Russia, Belarus or Iran. Before a contract for goods or services can be amended or extended, a person or entity must certify that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list. Both lists are found on Treasury's website at the following web addresses:

https://www.nj.gov/treasury/administration/pdf/RussiaBelarusEntityList.pdf
www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf.

As applicable to the type of contract, the above-referenced lists must be reviewed prior to completing the below certification.

A person or entity unable to make the certification must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran. The person or entity must cease engaging in any prohibited activities and provide an updated certification before the contract can be entered into.

If a vendor or contractor is found to be in violation of law, action may be taken as appropriate and as may be provided by law, rule, or contract, including but not limited to imposing sanctions, seeking compliance, recovering damages, declaring the party in default, and seeking debarment or suspension of the party.

CONTRACT AWARDS AND RENEWALS

☑	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate appears on the N.J. Department of Treasury's lists of entities engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3 or in investment activities in Iran pursuant to P.L. 2012, c. 25 ("Chapter 25 List"). I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf.* (Skip Part 2 and sign and complete the Certification below.)
CONTRACT AMENDMENTS AND EXTENSIONS	
☑	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate is listed on the N.J. Department of the Treasury's lists of entities determined to be engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3. I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf.* (Skip Part 2 and sign and complete the Certification below.)
IF UNABLE TO CERTIFY	
☐	*I am unable to certify as above because the person or entity and/or a parent entity, subsidiary, or affiliate is listed on the Department's Russia-Belarus list and/or Chapter 25 Iran list. I will provide a detailed, accurate, and precise description of the activities as directed in Part 2 below, and sign and complete the Certification below. Failure to provide such will prevent the award of the contract to the person or entity, and appropriate penalties, fines, and/or sanctions will be assessed as provided by law.*

Part 2: Additional Information

PLEASE PROVIDE FURTHER INFORMATION RELATED TO PROHIBITED ACTIVITIES IN RUSSIA OR BELARUS AND/OR INVESTMENT ACTIVITIES IN IRAN.

You must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran in the space below and, if needed, on additional sheets provided by you.

Part 3: Certification of True and Complete Information

I, being duly sworn upon my oath, hereby represent and state that the foregoing information and any attachments there, to the best of my knowledge, are true and complete. I attest that I am authorized to execute this certification on behalf of the above-referenced person or entity.

*I acknowledge that the **Educational Services Commission of New Jersey (ESCNJ)** is relying on the information contained herein and hereby acknowledge that I am under a continuing obligation from the date of this certification through the completion of any contracts with the **ESCNJ** to notify the **ESCNJ** in writing of any changes to the answers of information contained herein.*

*I acknowledge that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I recognize that I am subject to criminal prosecution under the law and that it will also constitute a material breach of my agreement(s) with the **ESCNJ** and that the **ESCNJ** at its option may declare any contract(s) resulting from this certification void and unenforceable.*

Full Name (Print)	Dario Bertocchi	**Title**	VP Contracting Operations
Signature		**Date**	9/11/24

STATEMENT OF OWNERSHIP DISCLOSURE

N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

Name of Organization: CDW Government LLC
Organization Address: 230 N. Milwaukee Avenue
City, State, ZIP: Vernon Hills, IL 60061

Part I Check the box that represents the type of business organization:

☐ Sole Proprietorship (skip Parts II and III, execute certification in Part IV)

☐ Non-Profit Corporation (skip Parts II and III, execute certification in Part IV)

☐ For-Profit Corporation (any type) ☒ Limited Liability Company (LLC)

☐ Partnership ☐ Limited Partnership ☐ Limited Liability Partnership (LLP)

☐ Other (be specific): _____

Part II Check the appropriate box

☐ The list below contains the names and addresses of all stockholders in the corporation who own 10 percent or more of its stock, of any class, or of all individual partners in the partnership who own a 10 percent or greater interest therein, or of all members in the limited liability company who own a 10 percent or greater interest therein, as the case may be. (**COMPLETE THE LIST BELOW IN THIS SECTION**)

OR

☒ No one stockholder in the corporation owns 10 percent or more of its stock, of any class, or no individual partner in the partnership owns a 10 percent or greater interest therein, or no member in the limited liability company owns a 10 percent or greater interest therein, as the case may be. (**SKIP TO PART IV**)

(Please attach additional sheets if more space is needed):

Name of Individual or Business Entity	Home Address (for Individuals) or Business Address

Part III DISCLOSURE OF 10% OR GREATER OWNERSHIP IN THE STOCKHOLDERS, PARTNERS OR LLC MEMBERS LISTED IN PART II

If a bidder has a direct or indirect parent entity which is publicly traded, and any person holds a 10 percent or greater beneficial interest in the publicly traded parent entity as of the last annual federal Security and Exchange Commission (SEC) or foreign equivalent filing, ownership disclosure can be met by providing links to the website(s) containing the last annual filing(s) with the federal Securities and Exchange Commission (or foreign equivalent) that contain the name and address of each person holding a 10% or greater beneficial interest in the publicly traded parent entity, along with the relevant page numbers of the filing(s) that contain the information on each such person. **Attach additional sheets if more space is needed**.

Website (URL) containing the last annual SEC (or foreign equivalent) filing	Page #'s

Please list the names and addresses of each stockholder, partner or member owning a 10 percent or greater interest in any corresponding corporation, partnership and/or limited liability company (LLC) listed in Part II **other than for any publicly traded parent entities referenced above**. The disclosure shall be continued until names and addresses of every non-corporate stockholder, and individual partner, and member exceeding the 10 percent ownership criteria established pursuant to N.J.S.A. 52:25-24.2 has been listed. **Attach additional sheets if more space is needed.**

Stockholder/Partner/Member and Corresponding Entity Listed in Part II	Home Address (for Individuals) or Business Address

Part IV Certification

I, being duly sworn upon my oath, hereby represent that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I acknowledge: that I am authorized to execute this certification on behalf of the bidder/proposer; that the ***ESCNJ and/or its members*** is relying on the information contained herein and that I am under a continuing obligation from the date of this certification through the completion of any contracts with the ***ESCNJ and/or its members*** to notify the ***ESCNJ and/or its members*** in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the, permitting the ***ESCNJ and/or its members*** to declare any contract(s) resulting from this certification void and unenforceable.

Full Name (Print):	Dario Bertocchi	Title:	VP Contracting Operations
Signature:		Date:	9/11/24

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

APPENDIX A
AMERICANS WITH DISABILITIES ACT OF 1990
Equal Opportunity for Individuals with Disability

The contractor and the Educational Services Commission of New Jersey (hereafter "owner") do hereby agree that the provisions of Title 11 of the Americans with Disabilities Act of 1990 (the "Act") (42 U.S.C. S121 01 et seq.), which prohibits discrimination on the basis of disability by public entities in all services, programs, and activities provided or made available by public entities, and the rules and regulations promulgated pursuant there unto, are made a part of this contract. In providing any aid, benefit, or service on behalf of the owner pursuant to this contract, the contractor agrees that the performance shall be in strict compliance with the Act. In the event that the contractor, its agents, servants, employees, or subcontractors violate or are alleged to have violated the Act during the performance of this contract, the contractor shall defend the owner in any action or administrative proceeding commenced pursuant to this Act. The contractor shall indemnify, protect, and save harmless the owner, its agents, servants, and employees from and against any and all suits, claims, losses, demands, or damages, of whatever kind or nature arising out of or claimed to arise out of the alleged violation. The contractor shall, at its own expense, appear, defend, and pay any and all charges for legal services and any and all costs and other expenses arising from such action or administrative proceeding or incurred in connection therewith. In any and all complaints brought pursuant to the owner's grievance procedure, the contractor agrees to abide by any decision of the owner which is rendered pursuant to said grievance procedure. If any action or administrative proceeding results in an award of damages against the owner, or if the owner incurs any expense to cure a violation of the ADA which has been brought pursuant to its grievance procedure, the contractor shall satisfy and discharge the same at its own expense.

The owner shall, as soon as practicable after a claim has been made against it, give written notice thereof to the contractor along with full and complete particulars of the claim, If any action or administrative proceeding is brought against the owner or any of its agents, servants, and employees, the *owner shall* expeditiously forward or have forwarded to the contractor every demand, complaint, notice, summons, pleading, or other process received by the owner or its representatives.

It is expressly agreed and understood that any approval by the owner of the services provided by the contractor pursuant to this contract will not relieve the contractor of the obligation to comply with the Act and to defend, indemnify, protect, and save harmless the owner pursuant to this paragraph.

It is further agreed and understood that the owner assumes no obligation to indemnify or save harmless the contractor, its agents, servants, employees and subcontractors for any claim which may arise out of their performance of this Agreement. Furthermore, the contractor expressly understands and agrees that the provisions of this indemnification clause shall in no way limit the contractor's obligations assumed in this Agreement, nor shall they be construed to relieve the contractor from any liability, nor preclude the owner from taking any other actions available to it under any other provisions of the Agreement or otherwise at law.

Company CDW Government LLC Name Dario Bertocchi

Signature  Title VP Contracting Operations

Date: 9/17/24

Exceptions

Instructions:

1. If "no" is marked with an "X" below, complete this form by signing it at the bottom.
2. If "yes" is marked with an "X" below, insert answers into the form shown below, providing narrative explanations of exceptions. *(To insert more rows, hit the tab key from the last field in the last row and column.)*
3. If adding pages, the company name and identifying information as to which item the response refers must appear on each page.
4. Exceptions to local, state or federal laws cannot be accepted under this solicitation.

	No, this respondent does not have exceptions to the Terms and Conditions incorporated in Parts A and B of this IFB.
x	**Yes**, this respondent has the following exceptions to the Terms and Conditions incorporated in Parts A and/or B of this solicitation.

IFB Section and Page Number	Outline Number	Term and Condition	Exception
Part A, Page 20		Limitation of Liability	CDW•G is not proposing a specific language exception at this time. Rather, CDW•G would request, upon award, the opportunity to discuss the incorporation of a mutually agreeable limitation of liability clause - commiserate with the clause currently contained in our current 022 contract. CDW•G appreciates the opportunity to discuss implementing such a clause and is eager to work with AEPA and its members to build a competitive and mutually beneficial contract.
Part B, Page 2 Part C, Page 1		Administrative Fee(s)	CDW•G is unable to track & report sales falling under the "Value Added Services" component of its proposal response. Accordingly, CDW•G will not be able to remit Administrative Fees to AEPA or its Member Agencies for such purchases.

CDW US Locations	
Office Location	**Address and Phone Number**
Illinois – Vernon Hills *Executive Office* *Central Distribution Center*	200 N. Milwaukee Ave. Vernon Hills, IL 60061 Phone: 847.371.6090
Nevada – Las Vegas *Western Distribution Center*	3201 E Alexander Rd. North Las Vegas, NV 89030 Phone: 800.800.4239
Arizona – Tempe	40 E. Rio Salado Pkwy. Suite 200 Tempe, AZ 85281 Phone: 800.800.4239
California – Irvine	2020 Main St. Suite 760 Irvine, CA 92614 Phone: 800.800.4239
California – San Diego	4980 North Harbor Dr. Suite 200 San Diego, CA 92106 Phone: 800.800.4239
Colorado – Centennial	6300 South Syracuse Way Suite 725 Centennial, CO 80111 Phone: 800.800.4239
Connecticut - Shelton	2 Corporate Dr. Suite 800 Shelton, CT 06484 Phone: 800.800.4239
Florida – Boca Raton	5201 Congress Ave. Boca Raton, FL 33487 Phone: 800.800.4239
Florida - Tampa	201 N. Franklin St. Floor 37 Tampa, FL 33602 Phone: 800.800.4239
Illinois - Chicago	625 W. Adams Street Chicago, IL 60661 Phone: 847.465.6000
Illinois – Elk Grove Village	1441 Touhy Ave. Elk Grove Village, IL 60007 Phone: 800.800.4239
Illinois – Rosemont	5505 Pearl St. Suite 400 Rosemont, IL 60018 Phone: 800.800.4239
Indiana – Carmel	880 Monon Green Blvd. Carmel, IN 46032 Phone: 800.800.4239
Iowa – West Des Moines	5550 Wild Rose Ln., Suite 410 West Des Moines, IA 50266

CDW US Locations	
Office Location	**Address and Phone Number**
	Phone: 800.800.4239
Kansas – Overland Park	10801 Mastin Blvd. Suite 900 Overland Park, KS 66210 Phone: 800.800.4239
Maryland – Columbia	8890 McGaw Rd. Columbia, MD 21045 Phone: 800.800.4239
Maryland – Crofton	2151 Priest Bridge Dr. Crofton, MD 21114 Phone: 800.800.4239
Michigan - Detroit	1000 Town Center Suite 1800 Southfield, MI 48075 Phone: 800.800.4239
Michigan – Grand Rapids	4690 E. Fulton St. Suite 203 Ada, MI 49301 Phone: 800.800.4239
Minnesota – Bloomington	7760 France Ave S. Suite 1310 Bloomington, MN 55435 Phone: 800.800.4239
Missouri – St. Louis	101 South Hanley St. Suite 575 St. Louis, MO 63105 Phone: 800.800.4239
Nebraska – Omaha	14301 FNB Pkwy. Suite 400 Omaha, NE 68154 Phone: 800.800.4239
New Jersey – Bell Works	101 Crawfords Corner Road Suite 1316, 3rd Floor Holmdel, NJ 07733 Phone: 800.800.4239
New Jersey – Cherry Hill	3 Executive Campus Suite 400 Cherry Hill, NJ 08002 Phone: 800.800.4239
New York – New York	72 Madison Ave. New York, NY 10010 Phone: 800.800.4239
New York – Pittsford	1250 Pittsford Victor Rd. Building 100, Suite 124 Pittsford, NY 14534 Phone: 800.800.4239
North Carolina – Charlotte	11301 Carmel Commons Blvd. Suite 114 Charlotte, NC 28226 Phone: 800.800.4239

CDW US Locations	
Office Location	**Address and Phone Number**
North Carolina - Greensboro	804 Green Valley Rd. Suite 104 Greensboro, NC 27408 Phone: 800.800.4239
North Carolina - Raleigh	2245 Gateway Access Point Suite 202 Raleigh, NC 27607 Phone: 800.800.4239
Ohio – Cleveland	6450 Rockside Woods Blvd. S. Suite 120 Independence, OH 44131 Phone: 800.800.4239
Ohio – Columbus	655 Metro Place South Suite 600/601 Dublin, OH 43017 Phone: 800.800.4239
Oregon — Portland	5550 S Macadam Ave. Suite 320 Portland, OR 97239 Phone: 503.598.3928
South Dakota – Sioux Falls	5900 S. Western Ave. Suite 104 Sioux Falls, SD 57108 Phone: 800.800.4239
Tennessee – Nashville	310 Seven Springs Way Brentwood, TN 37027 Phone: 800.800.4239
Texas – Austin	10900 Stonelake Blvd Building 2 Suite 100 Austin, TX 78759 Phone: 800.800.4239
Texas – Dallas	5908 Headquarters Dr. Suite 400 Plano, TX 75024 Phone: 800.800.4239
Texas – Houston	1616 S. Voss Rd. Suite 301 Houston, TX 77057 Phone: 800.800.4239
Texas – San Antonio	10100 Reunion Pl. Suite 500 San Antonio, TX 78216 Phone: 800.800.4239
Virginia - McLean	7927 Jones Branch Drive McLean, VA 22102 Phone: 800.800.4239
Washington – Seattle	10900 NE 8th St. Suite 1660 Bellevue, WA 98004 Phone: 800.800.4239
	4321 W. College Ave.

CDW US Locations	
Office Location	**Address and Phone Number**
Wisconsin – Appleton	Suite 400 Appleton, WI 54914 Phone: 800.800.4239
Wisconsin – Madison	5525 Nobel Dr. Fitchburg, WI 53711 Phone: 800.800.4239
Wisconsin – Milwaukee	790 N. Milwaukee St. Suite 400B Milwaukee, WI 53202 Phone: 800.800.4239



CDW Education Sales Team

K12 & Higher Education

Education Leadership Team



Kristen Peon
Sales Manager Assistant - HiEd
krispeo@cdw.com
(312) 705-8722



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Adrienne Griffith
Sales Manager Assistant – K12
Calendar Support – Joe Simone
adrgrif@cdw.com
(203) 851-7071



Joe Simone
Vice President - K12 & Higher Education
Email: joe@cdw.com Phone: (773) 706-6081
Home Office: Shelton, CT



Alex Miles Director, K12 West
Email: alemile@cdw.com Phone: (312) 705-4052
Home Office: Chicago



Jeff Grey Director, K12 Southeast
Email: jeffgre@cdwg.com Phone: (203) 851-7111
Home Office: Shelton, CT



Toni Hargis Director, K12 Central
Email: toni.hargis@cdw.com Phone: (312) 705-1891
Home Office: Chicago, IL



Eric Goff Director, K12 Northeast
Email: ericgof@cdw.com Phone: (312) 705-9101
Home Office: Chicago, IL



Ashley DiCiurcio Director, K12 South
Email: ashleyd@cdw.com Phone: (877) 765-2940
Home Office: Chicago, IL



Michael Durand Director, HiEd East
Email: michdur@cdw.com Phone: (203) 851-7041
Home Office: Shelton, CT



Tony DiGrazia Director, HiEd West
Email: anthdig@cdw.com Phone: (312) 547-2726
Home Office: Chicago, IL



Amanda Mellens Director, HiEd Central
Email: amanneu@cdw.com Phone: (312) 705 -0942
Home Office: Chicago



Tony Vitale Director, Customer Enablement, EDU
Email: tonyvit@cdw.com Phone: (312) 705-3253
Home Office: Chicago, IL



Kim Ciaccio Executive Project Manager, EDU
Email: kimbhay@cdw.com Phone: (312) 705-5268
Home Office: Chicago, IL

LOCALIZE IT

K12 SALES LEADERSHIP



ALEX MILES
K12 West



TONI HARGIS
K12 Central





ERIC GOFF
K12 Northeast



ASHLEY DiCIURCIO
K12 South



JEFF GREY
K12 Southeast

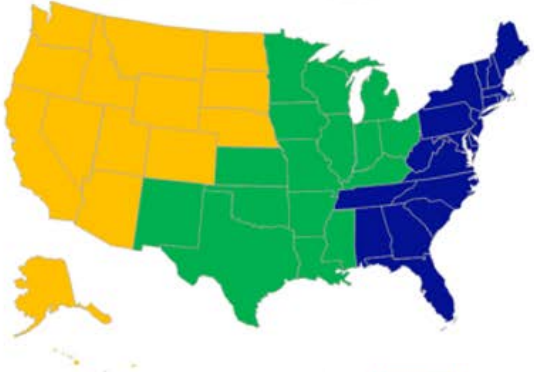
HI-ED SALES LEADERSHIP



TONY DiGRAZIA
Hi-Ed West



MIKE DURAND
Hi-Ed East





AMANDA MELLENS
Hi-Ed Central



TONY VITALE
Director
Customer Enablement-EDU
Amplified IT

CDW Education

EDU Sales Support



Lindsey Merlo
Manager, Sales Operations– K12 West
Email: linhedl@cdw.com
Phone: (847)-371-3741
Home Office: Chicago, IL



Liz Krause
Sales Operations Supervisor
Ohio Valley & Western States
lizkrau@cdwg.com
(312) 705-8146



Mary Boland
Sales Operations Supervisor
California South
maritor@cdwg.com
(312) 705-0626



Mike Lanfear
Sales Operations Supervisor
California North
miklanf@cdwg.com
(312)547-2844

K12 Sales Operations Team



Moises Rivera
Manager, Sales Operations– K12 East
Email: moisesc@cdw.com
Phone: (847)-371-7696
Home Office: Chicago, IL



Adam Finch
Sales Operations Supervisor
Atlantic & Southeast
adamfin@cdwg.com
203-851-7028



Courtney Irizarry
Sales Operations Supervisor
Heartland & North Central
couriri@cdw.com
(312) 705-5217



Danielle Lodovico
Sales Operations Supervisor
Keystone & New England
danilod@cdw.com
(203) 851-7196



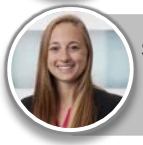
Jeremy Allen
Sales Ops Supervisor
Midwest
jeralle@cdwg.com
(312) 705-8592



Jordan Harrison
Sr. Sales Operations Supervisor
Amplified & GCS
jordhar@cdw.com
(847) 968-9937



Julie Johnston
Sales Operations Supervisor
Gulf Coast & FL/GA
julie.johnston@cdwg.com
(847)465-6000



Madison Lospinoso
Sr. Sales Operations Supervisor
NYC-DOE
madilos@cdw.com
(856) 330-3097



Reina Marcos
Sales Operations Supervisor
Texas – TX & TE
reinmar@cdw.com
(847) 968-9938



Trey Jones
Sales Operations Supervisor
New York
treyjon@cdwg.com
(312) 705-8140

CDW Education

EDU Sales Support



Maxine Shipe
Manager, Sales Operations– HiEd
Email: maxine.shipe@cdw.com
Phone: (312)-547-2753
Home Office: Chicago, IL

HiEd Sales Operations Team



Eloy Noble
Sales Ops Supervisor
For Profit, Pacific & Northwest
eloy.noble@cdwg.com
(847) 465-6000



LySandra DeGraffenreid
Sales Ops Supervisor
HBCU & Southeast
lysadeg@cdw.com
(847) 465-6913



Matt Spiegel
Sales Ops Supervisor
Atlantic, Keystone & Northeast
matspie@cdw.com
(856) 330-3212



Peter Lamberti
Sales Ops Supervisor
Dairyland & Ohio Valley
petlamb@cdw.com
847-465-6000



Spencer Ivy
Sales Ops Supervisor
Midwest & Gulf Coast
spenivy@cdw.com
(847) 371-5581

Education

Education

Higher Education Leadership & Inside Account Managers

Regional Leaders

HiEd Regional Leaders West



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



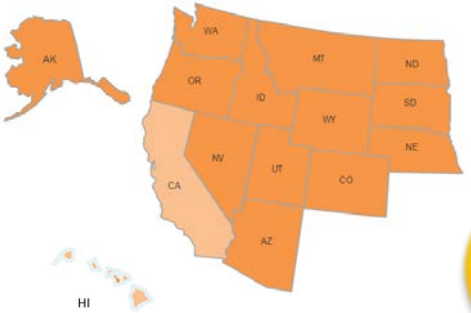
Tony DiGrazia
Director, HiEd West
Email: anthdig@cdw.com Phone: (312) 547-2726
Home Office: Chicago, IL



Brittany Atchison
Sales Manager – GS
HiEd Pacific
Email: britatc@cdw.com Phone: (312) 705-0147
Home Office: Chicago



Andrew Frenz
Sales Manager – NW
HiEd Northwest
Email: andrfre@cdw.com Phone: (312) 705-9559
Home Office: Chicago





Matt Varin
Field Sales Manager – West
Email: mattvar@cdw.com Phone: (262) 521-5679



TBH
Sales Manager – For Profit
Email: Phone:
Home Office:

 © CDW LLC 2017

HiEd Pacific Region



Eloy Noble
Sales Ops Supervisor
eloy.noble@cdwg.com
(847) 465-6000



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Brittany Atchison
Sales Manager – GS
HiEd West
Email: britatc@cdw.com
Phone: (312) 705-0147
Home Office: Chicago

Account Managers





Peter Turelli
Account Representative
peter.turelli@cdwg.com
(847) 371-5516



Gianna Panozzo
Account Representative
Gianna.Panozzo@cdwg.com
(312) 705-9063



Richard Sakofsky
Account Representative
rich.sakofsky@cdwg.com
(480) 270-7006



Allison Winans
Account Representative
allison.winans@cdwg.com
(312) 705-0269



Katie Loehr
Account Representative
katie.loehr@cdwg.com
(312) 547-2279



Sarah Park
Account Manager
sarah.park@cdwg.com
(312) 705-0287



Brett Bradford
Sr. Account Manager
bretbra@cdwg.com
(312) 705-3294



Michael Smaniotto
Account Manager
michsma@cdwg.com
(312) 705-0985



Scott Mueller
Account Manager
Scott.Mueller@cdwg.com
(847) 419-7201



Fabian Espinoza
Account Representative
Fabian.Espinoza@cdwg.com
(312) 705-4510



Paul Cardamone
Executive Account Manager
Paul.cardamone@cdwg.com
(312) 547-2736



Tyler Warren
Sr. Account Manager
tylewar@cdwg.com
(312) 705-8913

CDW Education

HiEd Northwest Region



Eloy Noble
Sales Ops Supervisor
eloy.noble@cdwg.com
(847) 465-6000



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Andrew Frenz
Sales Manager – NW
Hi Ed West
Email: andrfre@cdw.com
Phone: (312) 705-9559
Home Office: Chicago



Account Managers



Bobby Lopez
Account Representative
bobby.lopez@cdwg.com
(312) 547-4803



Felicia Moncada
Account Representative
felicia.moncada@cdwg.com
(312) 705-1886



Joe Devine
Account Representative
joe.devine@cdwg.com
(312) 547-2225



Brett Johnson
Executive Account Manager
brejohn@cdwg.com
(312) 705-6256



Jacob Parker
Account Representative
jake.parker@cdwg.com
(312) 547-2612



Lance McMillan
Executive Account Manager
lancem@cdw.com
(248) 233-4516



Eduardo Leonides
Account Representative
eduardo.leonides@cdwg.com
(312) 547-2650



JB Washburn
Account Representative
jb.washburn@cdwg.com
(312) 547-2732



Melissa Neuman
Executive Account Manager
melineu@cdw.com
(312) 547-2810

CDW Education

HiEd For Profit



Eloy Noble
Sales Ops Supervisor
eloy.noble@cdwg.com
(847) 465-6000



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Andrew Frenz
Sales Manager – FP
Hi Ed West
Email: andrfre@cdw.com
Phone: (312) 705-9559
Home Office: Chicago

Account Managers





Chris Pollack
Executive Account Manager
chripol@cdwg.com
(312) 547-2697



Lauren Lindgren
Account Representative
Lauren.Lindgren@cdwg.com
(312) 705-1867



Katie Bodnar
Account Manager
katibod@cdwg.com
(312) 705-0508



Libby McGuire
Executive Account Manager
emcguire@cdwg.com
(312) 705-6286

Education

HiEd West Field Team



Matt Varin
Field Sales Manager – West
Email: mattvar@cdw.com
Phone: (262) 521-5679





Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Asheley Bailey
ATAE - CA
ashebai@cdw.com
(312) 547-2253



Dustin Harris
ATAE – OR & WA
dustin.harris@cdwg.com
(847) 465-6000



Erin Walther
ATAE - CA
erinwal@cdwg.com
(312) 705-3291



John Menning
ATAE – MT & NE
trevhea@cdw.com
(720)-626-6786



Kyle Cavolo
ATAE – NW
kyle.cavolo@cdwg.com
(847) 465-6000



Larry Rascoe
ATAE – CA
Larry.Rascoe@cdw.com
(310)-968-1802



Trevor Heath
ATAE - CO
trevhea@cdw.com
(720)-626-6786



Tyler Quaranta
ATAE - CA
tylequa@cdw.com
(714)-325-5713

CDW Education

HiEd Regional Leaders Central



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Amanda Mellens Director, HiEd Central
Email: amanneu@cdw.com Phone: (312) 705 -0942
Home Office: Chicago



TBH
Sales Manager – GC
HiEd Gulf Coast
Email: Phone:
Home Office:



Garrett Gottfried
Sales Manager – IL IN
HiEd Midwest
Email: garrgot@cdw.com Phone: (312) 705-8916
Home Office: Chicago, IL





Marvin Gentry
Sales Manager – OV
HiEd Ohio Valley
Email: marvgen@cdw.com Phone: (513)-706-9661
Home Office: Chicago, IL



Kendall Blanzy
Sales Manager – DL
HiEd Dairyland
Email: kendbla@cdwg.com Phone: (312) 705-6206
Home Office: Chicago, IL

 | © CDW LLC 2017

HiEd Gulf Coast Region



Spencer Ivy
Sales Ops Supervisor
spenivy@cdw.com
(847) 371-5581



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



TBH
Sales Manager – GC
HiEd Central
Email:
Phone:
Home Office:

Account Managers





Austin Atkins
Account Representative
austin.atkins@cdwg.com
(312) 05-0177



Jackson Mihevc
Account Manager
jackmih@cdwg.com
(312) 547-2167



Juan Villa
Sr. Account Manager
juanvil@cdwg.com
(312) 705-4525



Brian Floyd
ATAE – TX & OK
brian.floyd@cdwg.com
(312) 705-3277



Jake Legasse
Account Manager
jakelag@cdw.com
(312) 705-9166



Riley Riddle
Account Representative
riley.riddle@cdwg.com
(312) 705-0256



Carianne Asberry
Account Representative
carianne.asberry@cdwg.com
(818) 254-1746



Jeffrey Baumann
Account Representative
jeff.baumann@cdwg.com
(312) 705-4564



Robert Jakubczak
Account Manager
robjaku@cdwg.com
(312) 705-3351



David Garratt
Sr. Account Manager
davgarr@cdwg.com
(312) 705-0937



Joe Freedlund
Account Representative
oseph.freedlund@cdw.com
(312) 705-0204



Terry Tisdale
ATAE - TX
Terry.Tisdale@cdw.com
(281)382-3631

Education

HiEd Dairyland Region



Peter Lamberti
Sales Ops Supervisor
petlamb@cdw.com
847-465-6000



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Kendall Blanzy
Sales Manager – ML
HiEd Central
Email: kendbla@cdwg.com
Phone: (312) 705-6206
Home Office: Chicago, IL

Account Managers





Lucas Murray
ATAE - WI
lucamur@cdwg.com
(608)-235-7689



Alex Gee
Account Representative
alex.gee@cdwg.com
(312) 705-4058



Anthony Walker
Account Representative
Anthony.Walker@cdwg.com
(312) 705-0313



Matt Lubawski
Sr. Account Manager
mattlub@cdwg.com
(312) 547-2289



Alexa Morrow
Account Representative
alexa.morrow@cdwg.com
(312) 547-2634



Dave Walczak
Executive Account Manager
davewal@cdw.com
(312) 547-2260



Melissa Braza
Account Manager
melibra@cdwg.com
(312) 705-5596



Andrew Beninati
Sr. Account Manager
andbeni@cdwg.com
(312) 547-2085



Devyn McDaniels
Account Representative
devyn.mcdaniels@cdwg.com
(312) 705-8969



Rachel Boldt
Account Representative
rachel.boldt@cdwg.com
(312) 547-2243



Andrew Paras
Account Manager
andrpar@cdwg.com
(312) 705-3269



Jim Allen
Sr. Account Manager
jiallen@cdwg.com
(312) 705-2130



Sonjay Punwani
Executive Account Manager
sonjay@cdwg.com
(312) 705-3276

CDW Education

HiEd Midwest Region



Spencer Ivy
Sales Ops Supervisor
spenivy@cdw.com
(847) 371-5581



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Garrett Gottfried
Sales Manager – IL IN
HiEd Central
Email: garrgot@cdw.com
Phone: (312) 705-8916
Home Office: Chicago, IL

Account Managers





Eric Cheng
Executive Account Manager
ericche@cdwg.com
(847) 968-9332



Kelsey Baker
Account Representative
kelsey.baker@cdwg.com
(312) 547-2628



Angie Bania
Executive Account Manager
angieandbrian@cdwg.com
(847) 419-8214



Greg Franklin
ATAE - IN
gregfra@cdw.com
(847) 371-7118



Mike Benkoski
Account Manager
mikbenn@cdwg.com
(312) 705-0327



Anthony D'Anca
ATAE - IL
tdanca@cdwg.com
(630)-698-1227



Jack Fitzgerald
Account Representative
jack.fitzgerald@cdwg.com
(312) 547-2267



Stephen Elijio
Account Manager
stepeli@cdwg.com
(312) 705-0714



Brian O'Callaghan
Executive Account Manager
angieandbrian@cdwg.com
(847) 968-9508



Josh McCray
Account Representative
josh.mccray@cdwg.com
(312) 705-4507



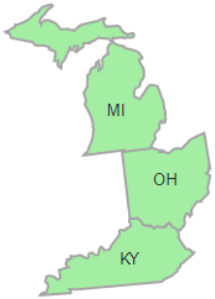
Virgil Cannon Jr
ATAE - IL
virgcan@cdw.com
(847) 968-9998

CDW Education

HiEd Ohio Valley Region



Marvin Gentry
Sales Manager – OV
HiEd Central
Email: marvgen@cdw.com
Phone: (513)-706-9661
Home Office: Chicago, IL





Peter Lamberti
Sales Ops Supervisor
petlamb@cdw.com
847-465-6000



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722

Account Managers



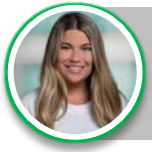
Maxwell Smith
Account Representative
maxwell.smith@cdwg.com
(312) 547-2239



Crystal Price
Account Representative
crystal.price@cdwg.com
(312) 547-2645



Rob Feinholz
Executive Account Manager
robf@cdwg.com
(312) 705-9022



Alexa Pretto
Account Manager
alexa.pretto@cdwg.com
(312) 547-4819



Ethan DeRubbo
ATAE - OH
ethader@cdw.com
(312) 705-3388



Samuel Humanchuk
Account Representative
sam.humanchuk@cdwg.com
(312) 547-2826



Anna Ennesser
Account Manager
annaenn@cdw.com
(312) 705-4086



Hansen Chennikkara
Executive Account Manager
hansenc@cdwg.com
(312) 705-8945



Sean McKnabb
ATAE - MI
SeanMc@cdw.com
(312)705-8573



Connor Dunn
Account Manager
conndun@cdwg.com
(312) 705-8139



Justin O'Brien
Account Representative
justin.obrien@cdwg.com
(312) 547-2816



Susan Pichotta
Executive Account Manager
suep@cdwg.com
(312) 705-9028

CDW Education

HiEd Regional Leaders East



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Matt Somers
Sales Manager – SE
HiEd Southeast
Email: mattsom@cdw.com Phone: (847) 968-9749
Home Office: Chicago, IL



Greg Henderson
Sales Manager – AT
HiEd Atlantic
Email: greghen@cdw.com Phone: (540)-494-2151
Home Office: Reston, VA



Michael Durand Director, HiEd East
Email: michdur@cdw.com Phone: (203) 851-7041
Home Office: Shelton, CT





Tramaine Martin
Sales Manager – HBCU
Email: trammar@cdw.com Phone: (312) 547-2685
Home Office: Chicago, IL



Mike Grey
Sales Manager – NE
HiEd Northeast
Email: mikeg@cdwg.com Phone: (203)581-7197
Home Office: Shelton, CT



Mike Long
Field Sales Manager – Mid Atlantic
Email: mikelon@cdw.com Phone: (312) 705-2060

 | © CDW LLC 2017

HiEd South East Region



LySandra DeGraffenreid
Sales Ops Supervisor
lysadeg@cdw.com
(847) 465-6913



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Matt Somers
Sales Manager – SE HiEd East
Email: mattsom@cdw.com
Phone: (312) 705-2060
Home Office: Chicago, IL



Account Managers



Amanda Swartz
Executive Account Manager
amanswa@cdwg.com
(312) 705-8957



Anne Tracy
Account Representative
anne.tracy@cdwg.com
(312) 547-2827



Bina Patel
Account Representative
bina.patel@cdwg.com
(312) 705-0982



Carson Kirchner - SE
Account Representative
carson.kirchner@cdwg.com
(312) 547-2262



Danny Kee
Account Representative
danny.kee@cdwg.com
(312) 705-1898



James Hillebrand
Executive Account Manager
jamehil@cdwg.com
(312) 705-9535



Jared Benson
Account Manager Associate
jareben@cdwg.com
(312) 547-2633



Joe Buffo
Account Manager
joe.buffo@cdwg.com
(312) 705-0396



Kayla Oharriz
Account Manager
kayloha@cdw.com
(312) 547-2640



Michal Pirga
Account Representative
Michal.Pirga@cdwg.com
(312) 705-9086



Patrick Lendabarker
Sr. Account Manager
patrlen@cdwg.com
(312) 547-2154



Paul Vivirto
Account Manager
paulviv@cdwg.com
(312) 547-2293



Rigo Alvarez
Account Representative
rigo.alvarez@cdwg.com
(312) 705-0249



Sean Queeney
Executive Account Manager
seanque@cdwg.com
(312) 705-0185

© CDW LLC 2017

CDW Education

HiEd Atlantic Region



Matt Spiegel
Sales Ops Supervisor
matspie@cdw.com
(856) 330-3212



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Greg Henderson
Sales Manager – AT
HiEd East
Email: greghen@cdw.com
Phone: (540)-494-2151
Home Office: Reston, VA

Account Managers





Antonio Pinelli
Account Representative
Antonio.Pinelli@cdwg.com
(203) 851-7211



Jordon Biondi
Account Representative
jordon.biondi@cdwg.com
(203) 851-7205



Robert Chlupsa
Executive Account Manager
robert.chlupsa@cdwg.com
(203) 851-7275



Bill Lobdell
Account Representative
bill.lobdell@cdwg.com
(203) 851-7126



Marc Liquindoli
Account Representative
marc.liquindoli@cdwg.com
(203) 899-7651



Sarah Maulucci
Account Representative
sarah.maulucci@cdwg.com
(203) 899-2160



Brian Quinn
Account Manager
brian.quinn@cdwg.com
(203) 851-7019



Mike Millea
Sr. Account Manager
mikemil@cdwg.com
(203) 851-7168



Troy Hart
Account Representative
troy.hart@cdwg.com
(203) 851-7131

CDW Education

HiEd Northeast Region



Matt Spiegel
Sales Ops Supervisor
matspie@cdw.com
(856) 330-3212



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Mike Grey
Sales Manager – NE HiEd East
Email: mikeg@cdwg.com
Phone: (203)581-7197
Home Office: Shelton, CT





Adam Jaloudi
Account Representative
adam.jaloudi@cdwg.com
(203) 899-2158



Charles Rhodes
Account Representative
charlie.rhodes@cdwg.com
(203) 899-2154



Edwin Guerrero
Account Representative
edwin.guerrero@cdwg.com
(203) 851-7011



Fred Riccio
Sr. Account Manager
fred.riccio@cdwg.com
(203) 851-7116



Geoffrey McKay
Account Representative
geoffrey.mckay@cdwg.com
(203) 851-7208

Account Managers



Giovanni Trocchia
Account Representative
gio.trocchia@cdwg.com
(203) 851-7293



Joe Masulli
Sr. Account Manager
joemasu@cdwg.com
(203) 851-7057



John Prestiano
Sr. Account Manager
johnpre@cdw.com
(203) 851-7048



Jonathan Williams
Executive Account Manager
jonawil@cdwg.com
(203) 851-7121



Mitch Amelio
Account Manager
mitcame@cdwg.com
(203) 851-7270



Robert Natalino
Sr. Account Manager
robenat@cdwg.com
(203) 851-7247



Vinny Nariyani
Account Manager
vinnnar@cdwg.com
(203) 851-7169

CDW Education

HiEd HBCU



LySandra DeGraffenreid
Sales Ops Supervisor
lysadeg@cdw.com
(847) 465-6913



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Tramaine Martin
Sales Manager – HBCU
HiEd East
Email: trammar@cdw.com
Phone: (312) 547-2685
Home Office: Chicago, IL

Account Managers





Charlie Prangl
Account Representative
charlie.prangl@cdwg.com
(312) 547-2310



Kimberly Brown
Account Manager
kimbebr@cdw.com
(703)262-8144



Ebony Thomas
Account Representative
ebontho@cdwg.com
(203) 851-7067



Mitch Huffington
Executive Account Manager
mitchh@cdwg.com
(847) 968-9362

CDW Education

HiEd East Field Team



Mike Long
Field Sales Manager – East
Email: mikelon@cdw.com
Phone: (312) 705-2060





Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722



Erica Kordes
ATAE – VA, DC, MD
erica.kordes@cdw.com
(703)-262-8044



Bryan Nasznic
ATAE - MA
bryanas@cdw.com
(617) 297-6973



Steve Bevilacqua
ATAE - GA
steve.bevilacqua@cdwg.com
(404)-245-4289



Dave Hensley
ATAE - GA
steve.bevilacqua@cdwg.com
(904) 599-4059



Suzanne Keith
ATAE – NJ/PA/DE
suzanne.keith@cdwg.com
(862)-217-8038

Education



K12 Leadership & Inside Account Managers

Regional Leaders

K12 Regional Leaders West



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



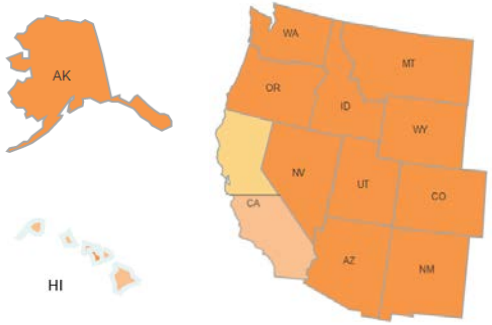
TBH
Sales Manager – CN
K12 California North
Email: Phone:
Home Office



Valerie Hanrahan
Sales Manager – CS
K12 California South
Email: valeban@cdw.com Phone: (312) 547-2711
Home Office: Chicago, IL



Alex Miles Director, K12 West
Email: alemile@cdw.com Phone: (312) 705-4052
Home Office: Chicago





Scott Swanson
Sales Manager – WS
K12 Western States
Email: scott.swanson@cdw.com Phone: (312) 705-9525
Home Office: Chicago, IL



TBH
Field Sales Manager – California
Email: Phone:

 © CDW LLC 2017

K12 Western States Region



Liz Krause
Sales Operations Supervisor
lizkrau@cdwg.com
(312) 705-8146



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Scott Swanson
Sales Manager – WS
K12 West
Email: scott.swanson@cdw.com
Phone: (312) 705-9525
Home Office: Chicago, IL



Account Managers



Ashley Bruser
Executive Account Manager
ashlbru@cdwg.com
(312) 547-2813



Blake Muno
Account Manager
blakmun@cdwg.com
(312) 705-4546



Chris Carpen
Executive Account Manager
chrcarp@cdwg.com
(312) 705-3242



Elizabeth Wink
Account Manager
Liz.Wink@cdw.com
(480) 270-7572



Ellie Easton
Sr. Account Manager
elleeas@cdwg.com
(312) 705-3246



Emily Vlahos
Account Manager
emilvla@cdwg.com
(312) 705-5626



Heather Rose
Account Manager
heather.rose@cdwg.com
(847) 465-6000



Hunter Kingwill
Account Representative
hunter.kingwill@cdwg.com
(312) 547-2367



James Huff
Account Representative
james.huff@cdwg.com
(312) 547-2274



Justin Green
Executive Account Manager
dreamteam@cdwg.com
(312) 705-3348



Marissa O'Malley
Account Manager
dreamteam@cdwg.com
(312) 705-3378



Keith Gavin
Account Manager
keigavi@cdwg.com
(312) 705-3262



Kelvin Johnson
Executive Account Manager
kelvjoh@cdw.com
(312) 705-9540



Kevin O'Connor
Account Manager
kevocon@cdwg.com
(312) 547-2656



Manuel Martinez
ATAE – Western States
mj.martinez@cdwg.com
(847) 465-6000



Nick Kelliher
Executive Account Manager
nickkel@cdw.com
(312) 547-2707



Timothy Park
Account Representative
Tim.Park@cdwg.com
(312) 705-0951

© CDW LLC 2017

Education

K12 California North



Mike Lanfear
Sales Operations Supervisor
miklanf@cdwg.com
(312)547-2844



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435

Account Managers



TBH
Sales Manager – CN
K12 West
Email:
Phone:
Home Office:





Austin Romero
Account Manager
austrom@cdwg.com
(312) 547-2890



Caitlin Kristensen
Account Manager Associate
caithir@cdw.com
(312) 547-2086



Chris Atraje
Executive Account Manager
chriatr@cdwg.com
(312) 705-0376



Ian Rodnick
Executive Account Manager
ianrodn@cdw.com
(312) 547-2701



Justin Davenport
Executive Account Manager
justdav@cdwg.com
(248) 223-4533



Patrick Hein
Executive Account Manager
pathei@cdwg.com
(312) 705-0206



Tyler Emde
Account Manager Associate
tyleemd@cdw.com
(312) 547-2173



Izzy Hallberg
Account Representative
izzy.hallberg@cdwg.com
(312) 547-2784



John Hart
Executive Account Manager
johnhar@cdwg.com
(312) 705-8935



Mary Kate Fee
Account Manager
maryfee@cdw.com
(312) 705-8184



Peter Taylor
Account Representative
peter.taylor@cdwg.com
(312) 547-2259



Ryan Miller
Executive Account Manager
ryanmil@cdwg.com
(312) 705-6288

CDW Education

K12 California South



Valerie Hanrahan
Sales Manager – CS
K12 West
Email: valeban@cdw.com
Phone: (312) 547-2711
Home Office: Chicago, IL



Mary Boland
Sales Operations Supervisor
maritor@cdw.com
(312) 705-0626



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435

Account Managers





Adam Slater
Executive Account Manager
adamsla@cdw.com
(480) 270-7108



Anthony Dierickx
Account Manager
anthdie@cdw.com
(312) 705-4061



Astrid Saed
Account Manager
astrsae@cdw.com
(312)-547-4899



Charleen Chu
Executive Account Manager
charchu@cdw.com
(312) 705-9033



Christopher Zingler
Executive Account Manager
chrizin@cdw.com
(312) 705-9573



Elizabeth Girardini
Executive Account Manager
bethgir@cdwg.com
(480) 270-7282



Jay Montblanc
Executive Account Manager
jaymont@cdwg.com
(312) 705-9557



Jeff Bauman
Executive Account Manager
jbauman@cdw.com
(312) 705-8912



Jeff Polk
Executive Account Manager
jeffpol@cdwg.com
(312) 705-4094



Jonathan Olsen
Account Representative
jonaols@cdw.com
(312) 705-9348



Justin Lindberg
Executive Account Manager
justlin@cdwg.com
(312) 705-0245



Kaitlin Frazier
Account Manager
katefra@cdwg.com
(312) 705-8133



Laure Kovacs
Account Manager Associate
laure.kovacs@cdw.com
(203) 899-4214



Mike Regan
Account Manager
mikereg@cdwg.com
(312) 547-2880



Tyson Lagoni
Executive Account Manager
tylag@cdwg.com
(312) 705-3336

CDW Education

K12 California Field Team



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



TBH
Field Sales Manager – California
Email:
Phone:





Dan Shamburek
ATAE - CA
daniesh@cdw.com
(847)-465-6000



Jeffrey Mitchell
ATAE - CA
jeffmit@cdw.com
(916)-337-4717



Jonathan Gentile
ATAE - CA
jonagen@cdwg.com
(661)-233-5049



Rich Olsen
ATAE - CA
richols@cdw.com
(818) 254-1778



Stacy Goodman
ATAE - CA
sgoodman@cdw.com
(916)-216-5196

Education

K12 Regional Leaders Central



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



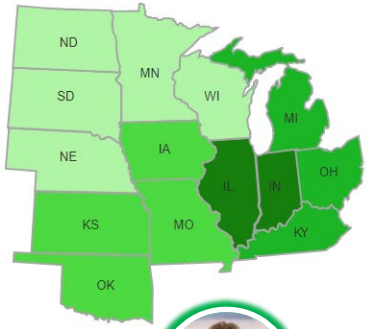
Adam Greene
Sales Manager – HL
K12 Heartland
Email: adagree@cdwg.com Phone: (847) 419-8297
Home Office: Chicago, IL



Brandon Ginter
Sales Manager – NC
K12 North Central
Email: brangin@cdw.com Phone: (847) 371-5547
Home Office: Lincolnshire, IL



Toni Hargis Director, K12 Central
Email: toni.hargis@cdw.com Phone: (312) 705-1891
Home Office: Chicago, IL





Gabriela Rubeck
Field Sales Manager - Midwest
Email: gabiper@cdwg.com Phone: (847)-749-5219



Michael Whartnaby
Sales Manager – OV
K12 Ohio Valley
Email: michwha@cdwg.com Phone: (847) 371-7050
Home Office: Chicago, IL



John Buttita
Sales Manager – MW
K12 Midwest
Email: johnbut@cdw.com Phone: (847) 371-7126
Home Office: Lincolnshire, IL

 | © CDW LLC 2017

K12 Heartland Region



Courtney Irizarry
Sales Operations Supervisor
couriri@cdw.com
(312) 705-5217



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Adam Greene
Sales Manager – HL
K12 Central
Email: adagree@cdwg.com
Phone: (847)419-8297
Home Office:



Account Managers



Daisy Arroyo
Account Manager
daisarr@cdwg.com
(312) 705-3231



Danny Heyman
Account Manager
dannhey@cdwg.com
(312) 547-2282



Lindsey Takaoka
Account Representative
Lindsey.Takaoka@cdwg.com
(312) 705-0977



Matt Albrecht
Account Representative
matt.albrecht@cdwg.com
(847) 968-0693



Nic Snedden
Account Representative
nic.snedden@cdwg.com
(312) 705-1894



Nathan Reynolds
Executive Account Manager
nathrey@cdw.com
(312) 705-6253



Rob Culicchia
Account Manager
robcul@cdw.com
(312) 705-2997



Steve Grempka Jr
Executive Account Manager
stevgre@cdwg.com
(312) 705-9588



Taylor Piazza
Account Representative
taylor.piazza@cdwg.com
(312) 547-2283



Zac Lawhorn
Account Representative
Zac.Lawhorn@cdwg.com
(312) 705-4540



Amanda Marks
Account Representative
amanda.marks@cdwg.com
(312) 547-2280



Arielle Matus
Account Manager
ariemat@cdwg.com
(312) 705-3246



Brendan Devlieger
Executive Account Manager
NateandBrendan@cdwg.com
(312) 705-8778

Education

K12 North Central Region



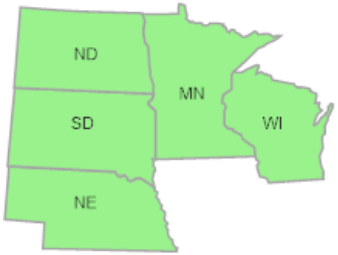
Courtney Irizarry
Sales Operations Supervisor
couriri@cdw.com
(312) 705-5217



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Brandon Ginter
Sales Manager – NC K12 Central
Email: brangin@cdw.com
Phone: (847) 371-5547
Home Office: Lincolnshire



Account Managers



Mayank Srivastava
Executive Account Manager
joelhot@cdwg.com
(312) 547-2953



Dan Behnke
Account Manager
danbehn@cdwg.com
(312) 705-0397



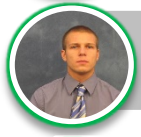
Mike Meier
Executive Account Manager
michmei@cdw.com
(312) 705-0746



Ashok Natraj
Account Manager
ashonat@cdwg.com
(312) 705-4541



Jake Huisman
Account Representative
jake.huisman@cdwg.com
(847) 968-0690



Oleg Krylov
Executive Account Manager
olegkry@cdwg.com
(312) 705-2068



Mohamed Awad
Account Representative
mohawad@cdwg.com
(312) 547-2625



Luke Mahar
Account Representative
luke.mahar@cdwg.com
(312) 547-2361



Ryan Sherman
Account Representative
ryan.sherman@cdwg.com
(312) 547-2284



Dani Stecyna
Account Representative
danielle.stecyna@cdwg.com
(312) 705-4059



Marshall Francis
Account Representative
marshall.francis@cdwg.com
(312) 705-0211



Tanner Frahm
Account Manager
tannfra@cdw.com
(312) 705-8192

CDW Education

K12 Ohio Valley Region



Liz Krause
Sales Operations Supervisor
lizkrau@cdwg.com
(312) 705-8146



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Michael Whartnaby
Sales Manager – OV
K12 Central
Email: michwha@cdwg.com
Phone: (847) 371-7050
Home Office: Chicago, IL



Account Managers



Abby Kuchler
Account Representative
abbkuch@cdwg.com
(312) 547-2630



Bradley Huffman
Executive Account Manager
bradhuf@cdwg.com
(847) 371-8184



Danielle Metzler
Account Manager
danimet@cdwg.com
(312) 547-2422



Elizabeth Glans
Account Manager
elizgla@cdw.com
(312) 547-2802



Hannah Baker
Account Representative
hannah.baker@cdwg.com
(312) 705-5257



Jennifer Hawley
Account Representative
jennifer.hawley@cdw.com
(312) 705-0734



Jonathan Lesher
Executive Account Manager
jonales@cdwg.com
(312) 705-9010



Joseph Stickelmaier
Executive Account Manager
josesti@cdwg.com
(312) 705-9590



Katelin Rembert
Account Representative
katelin.rembert@cdwg.com
(312) 705-8258



KiAundre Garland
Account Manager
kiaugar@cdwg.com
(312) 705-8930



Maggie Bellucci
Account Representative
Maggie.Bellucci@cdwg.com
(312) 705-9073



Mike Goldberg
Executive Account Manager
mikegol@cdw.com
(312) 705-5636



Nikki Serra
Account Representative
nikki.serra@cdwg.com
(312) 705-0371



Patrick Kane
Account Representative
patrick.kane@cdwg.com
(312) 705-8849



Rich Mclean
Executive Account Manager
richmcl@cdw.com
(312) 705-5599



Wes Farrell
Sr. Account Manager
wesfar@cdw.com
(847) 419-8255

Education

K12 Midwest Region



Jeremy Allen
Sales Ops Supervisor
jeralle@cdwg.com
(312) 705-8592



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



John Buttita

Sales Manager – MW
K12 Central
Email: johnbut@cdw.com
Phone: (847) 371-7126
Home Office: Lincolnshire, IL

Account Managers





Abby Moriarty
Account Representative
abby.moriarty@cdwg.com
(312) 547-2639



Angela Collins
Executive Account Manager
angecol@cdwg.com
(847) 371-5501



Anne Getty
Account Manager
anneget@cdwg.com
(847) 371-7130



Brian Lewin
Executive Account Manager
brialew@cdw.com
(847) 371-5533



David Friedman
Executive Account Manager
davifri@cdwg.com
(847) 371-7097



Ivan Ramirez
Account Representative
Ivan.Ramirez@cdwg.com
(847) 371-7167



Kevin Noreikis
Account Manager
kevin.noreikis@cdwg.com
(847) 968-9047



Leigh Ann Wines
Account Manager
LeighAnn@cdwg.com
(847) 968-9766



Luke Starasinich
Account Representative
luke.starasinich@cdwg.com
(312) 547-2252



Marc Arias
Account Representative
marc.arias@cdwg.com
(847)-968-0685



Matt Eisfelder
Executive Account Manager
matteis@cdwg.com
(847) 968-9550



Matt Tallungan
Account Manager
Matt.Tallungan@cdwg.com
(312) 705-4050



Meg Heaphy
Account Representative
meg.heaphy@cdwg.com
(847) 371-5540



Sean Dillon
Executive Account Manager
seandil@cdw.com
(847) 968-9304



Seyed Khalili
Executive Account Manager
seyed.khalili@cdwg.com
(847) 968-9708



Thomas Chung
Account Manager
Tom.Chung@cdwg.com
(847) 968-9046



Todd Tysick
Account Manager Associate
toddtys@cdw.com
(312) 705-3363

Education

K12 Central Field Team



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Gabi Rubeck
Field Sales Manager - Midwest
Email: gabiper@cdwg.com
Phone: (847)-749-5219





Christopher Schwerin
ATAE - IL
chris.schwerin@cdwg.com
(312) 560-9013



Dave Donarski
ATAE - MN
davedon@cdwg.com
(612)-704-6000



Mark Silversten
ATAE– N & Central OH
marksil@cdwg.com
(440)-591-7718



TBH
ATAE– WI



Megan Peterson
ATAE – KS/MO
chris.schwerin@cdwg.com
(312) 547-2817



Rafal Libelt
ATAE - IL
rafalib@cdwg.com
(312)-451 4108



Ryan Parvis
ATAE - IL
ryanpar@cdwg.com
(847)-371-5514



Steve Morrissey
ATAE - IN
steve.morrissey@cdwg.com
(847)-465-6000

CDW Education

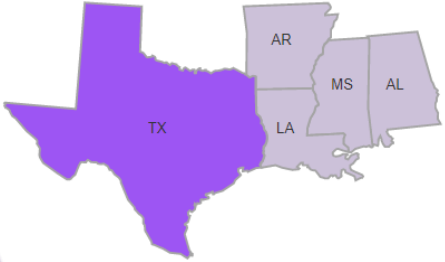
K12 Regional Leaders South



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Ashley DiCiurcio Director, K12 South
Email: ashleyd@cdw.com Phone: (877) 765-2940
Home Office: Chicago, IL





Sia Pettaras
Sales Manager–GU
K12 Gulf Coast
Email: siapett@cdw.com Phone: (312) 705-9388
Home Office: Chicago, IL



Michael Swartz
Sales Manager – TX Majors
K12 Texas
Email: michswa@cdwg.com Phone: (312) 705-9596
Home Office: Chicago, IL



Kelly Mulhollan
Field Sales Manager –South
Email: kelly.mulhollan@cdwg.com Phone: (847) 465-6000



TBH
Sales Manager – TX
K12 Texas
Email: Phone:
Home Office:

 | © CDW LLC 2017

K12 Gulf Coast Region



Sia Pettaras
Sales Manager–GU K12 South
Email: siapett@cdw.com
Phone: (312) 705-9388
Home Office: Chicago, IL



Julie Johnston
Sales Operations Supervisor
julie.johnston@cdwg.com
(847)465-6000



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435





Caleb Chambers
Executive Account Manager
calecha@cdwg.com
(312) 547-2383



Nicole Lieberman
Account Representative
nikki.lieberman@cdwg.com
(312) 705-8785



Alexa Cohen
Account Representative
alecohe@cdwg.com
(312) 547-2632



Daniel Schulman
Executive Account Manager
danschu@cdwg.com
(312) 547-2659



Noah Bergman
Account Manager
noahber@cdwg.com
(312) 705-0963



Angelica Pacleb
Account Manager
angpacl@cdwg.com
(312) 705-6227



Marie Soupart
Account Representative
marie.soupart@cdwg.com
(312) 547-2376



Steven Magid
Executive Account Manager
stevmag@cdwg.com
(312) 547-2142



Anuj Kalra
Executive Account Manager
anujkal@cdwg.com
(312) 705-8946



Mike Bolotnikov
Sr. Account Manager
mikebol@cdwg.com
(312) 547-2964



Walter Lobas
Executive. Account Manager
waltlobas@cdw.com
(312) 705-4805

CDW Education

K12 Texas Majors



Reina Marcos
Sales Operations Supervisor
reinmar@cdw.com
(847) 968-9938



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Michael Swartz
Sales Manager – TX
K12 South
Email: michswa@cdwg.com
Phone: (312) 705-9596
Home Office: Chicago, IL

Account Managers





Matthew Shortell
Executive Account Manager
mattsho@cdwg.com
(469) 587-0476



Mike Smith
Executive Account Manager
miksmit@cdwg.com
(312) 705-8788



Andy Arroyo
Account Manager Associate
andyarr@cdw.com
(847) 371-3970



Mike Chiesa
Executive Account Manager



Mike LaRocco
Executive Account Manager
miclaro@cdwg.com
(312) 705-8715



Gustavo Diaz
Account Representative
gustavo.diaz@cdwg.com
(312) 547-2611



Eric Althoff
Executive Account Manager
k12northtexas@cdwg.com
Mike: (248) 223-4533
Eric: (312) 705-0206



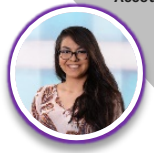
Matt Albertson
Executive Account Manager
mattalb@cdwg.com
(312) 705-9531



Laura Voigt
Executive Account Manager
laurcla@cdwg.com
(312) 705-0328



Catherine Ocampo
Associate AM
(312) 705-0702



Cristina Perez
Account Manager Associate
crisper@cdw.com
(312) 705-9529

Education

K12 Texas Territory



Reina Marcos
Sales Operations Supervisor
reinmar@cdw.com
(847) 968-9938



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Michael Swartz
Sales Manager – TE
K12 South
Email: michswa@cdwg.com
Phone: (312) 705-9596
Home Office: Chicago, IL

Account Managers





Alec Campbell
Account Manager
aleccam@cdwg.com
(312) 705-6942



Alyssa Teague
Account Manager
alystea@cdw.com
(312)-705-9574



Ashley Zimdars
Account Manager
ashlzim@cdwg.com
(312) 705-0996



Corey Grempka
Executive Account Manager

Becky Bradley
Sr. Account Manager

CoreyandBecky@cdw.com
Corey: (312) 705-9518
Becky: (312) 705-9070





Jake Miles – TE
Account Representative
jake.miles@cdwg.com
(847) 968-0702



Jim Donato
Account Manager
jimmdon@cdwg.com
(312) 547-2798



Kevin Tamras
Account Manager
kevitam@cdwg.com
(312) 705-0209



Melissa Zamin
Account Manager
melizam@cdw.com
(312) 705-8947



Swetal Thakkar
Account Representative
Swetal.Thakkar@cdwg.com
(312) 705-0193

Education

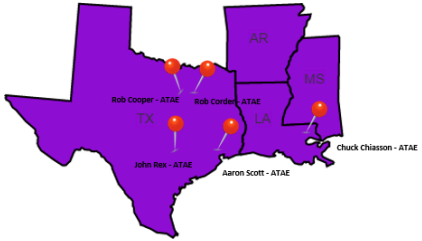
K12 South Field Team



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435



Kelly Mulhollan
Field Sales Manager – Texas
Email: kelly.mulhollan@cdwg.com
Phone: (847) 465-6000





Aaron Scott
ATAE - TX
aarscot@cdw.com
(281)-832-9251



Chuck Chiasson
ATAE - LA
charles.chiasson@cdw.com
(847) 465-6000



Robert Cooper
ATAE - TX
robecoo@cdwg.com
(469) 587-0447



John Rex
ATAE - TX
johnrex@cdw.com
(847) 465-6000



Robert Corder
ATAE - TX
robcor@cdwg.com
(815)-566-0150

Education

K12 Regional Leaders Northeast



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071



Eric Goff Director, K12 Northeast
Email: ericgof@cdw.com Phone: (312) 705-9101
Home Office: Chicago, IL



Derek DellaMonica
Sales Manager – KY
K12 Keystone
Email: deredel@cdw.com Phone: (203) 851-7160
Home Office: Shelton, CT



Milton Saltos
Sales Manager – NY
K12 New York
Email: miltsal@cdw.com Phone: (732) 982-0466
Home Office: Holmdel, NJ





Jorge Esteves
Sales Manager – NE
K12 New England
Email: jorgest@cdwg.com Phone: (203) 851-7217
Home Office: Shelton, CT



Scott Elder
Field Sales Manager – Northeast
Email: scott.elder@cdwg.com Phone: (703)-621-8285

 | © CDW LLC 2017

K12 Keystone Region



Danielle Lodovico
Sales Operations Supervisor
danilod@cdw.com
(203) 851-7196



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071



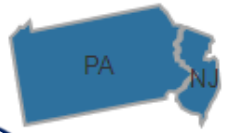
Jill Griffin
Office Admin
jill@cdw.com
(203) 851-7025



Derek DellaMonica

Sales Manager – KY
K12 East
Email: deredel@cdw.com
Phone: (203) 851-7160
Home Office: Shelton, CT

Account Managers





Becky Monteiro
Account Manager
rebemon@cdw.com
(203) 851-7024



Bobby Leonzo
Executive Account Manager
bobbleo@cdw.com
(203) 851-7061



Cassidy Chapman
Account Representative
cassidy.chapman@cdw.com
(203) 851-7050



Christopher Kanios
Account Representative
Chris.Kanios@cdw.com
(203) 851-7229



Christopher Perone
Account Representative
chris.perone@cdw.com
(203) 851-7170



Corey Regalado
Account Representative
Corey.Regalado@cdw.com
(203) 851-7274



Jason Martins
Account Representative
Jason.martins@cdw.com
(203) 851-7166



Joe Reynolds
Executive Account Manager
joereyn@cdw.com
(203) 851-7018



Josh Duancik
Sr. Account Manager
joshduh@cdw.com
(203) 851-7266



Kristin Welch
Sr. Account Manager
kricarm@cdw.com
(203) 851-7257



Luca Durante
Account Manager
luca.durante@cdw.com
(203) 851-7224



Matt Cleveland
Executive Account Manager
mattcle@cdw.com
(203) 851-7075



Megan Olbrys
Executive Account Manager
megaolb@cdw.com
(203) 851-7178



Michael Creegan
Executive Account Manager
michael.creegan@cdw.com
(203) 851-7207



Michael Talbot
Executive Account Manager
michtal@cdw.com
(203) 851-7077



Michael Taraian
Executive Account Manager
miketar@cdw.com
(203) 851-7037



Raj Jhala
Sr. Account Manager
raj.jhala@cdw.com
(203) 851-7054



Thomas Figueiredo
Sr. Account Manager
thomfig@cdw.com
(203) 851-7220

CDW Education

K12 New England Region



Danielle Lodovico
Sales Operations Supervisor
danilod@cdw.com
(203) 851-7196



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071



Jill Griffin
Office Admin
jill@cdw.com
(203) 851-7025



Jorge Esteves
Sales Manager – NE K12 East
Email: jorgest@cdwg.com
Phone: (203) 851-7217
Home Office: Shelton, CT

Account Managers





Steven Evangelista
Sr. Account Manager
steven.evangelista@cdwg.com
(203) 851-7094



Anthony Brown
Account Representative
tony.brown@cdwg.com
(203) 851-7032



Michael Nolan
Account Manager
Mike.nolan@cdwg.com
(203) 851-7158



Tim Smith
Account Manager
timsmit@cdwg.com
(203) 851-7156



Chris Lipford
Executive Account Manager
chrilip@cdwg.com
(203) 851-7163



Rosario Cappetta
Account Representative
ario.cappetta@cdwg.com
(203) 851-7277



Valis Topalis
Account Manager
vasilis.topalis@cdwg.com
(203) 851-7299



Jim Pinto
Account Manager
jimpin@cdwg.com
(203) 851-7119



Steve Fiore
Sr. Account Manager
stepfio@cdw.com
(203) 851-7010



Vincent Mulvihill
Executive Account Manager
vinny@cdwg.com
(203) 851-7154

CDW Education

K12 New York Region



Trey Jones
Sales Operations Supervisor
treyjon@cdwg.com
(312) 705-8140



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071



Jill Griffin
Office Admin
jill@cdw.com
(203) 851-7025



Milton Saltos

Sales Manager – NY
K12 East
Email: miltsal@cdw.com
Phone: (732) 982-0466
Home Office:



Account Managers



Andrew Magliola
Executive Account Manager
andrmag@cdw.com
(203) 851-7195



Aubrey Cameron
Executive Account Manager
aubrcla@cdw.com
(203) 851-7103



Brian Corasaniti
Executive Account Manager
brian.corasaniti@cdw.com
(203) 851-7268



Cait Hitchcock
Account Manager
Cait.hitchcock@cdwg.com
(203) 851-7193



Dana Gambardella
Executive Account Manager
danagam@cdwg.com
(203) 851-7286



EJ Henderson Jr.
Executive Account Manager
ejhende@cdw.com
(203) 851-7013



Grace Doubek
Account Manager Associate
gracdou@cdwg.com
(312) 547-2801



Jen Jadach
Executive Account Manager
jen.jadach@cdwg.com
(203) 851-7219



John Margiotta
Executive Account Manager
john.margiotta@cdwg.com
(203) 851-7262



Katie McGarity
Executive Account Manager
kathmc@cdw.com
(203) 851-7245



Le'Nina Williams
Account Representative
lenina.williams@cdwg.com
(203) 851-7162



Matt Edsall
Executive Account Manager
matteds@cdw.com
(203) 851-7143



Matt Zrallack
Sr. Account Manager
mattzra@cdwg.com
(203) 851-7159



Peter Cotto
Account Manager
petecot@cdwg.com
(203) 851-7185



Ralph Sharkis
Executive Account Manager
ralph.sharkis@cdwg.com
(203) 851-7014



Scott Sember
Sr. Account Manager
scotsem@cdwg.com
(203) 851-7190



Sean Roche
Executive Account Manager
seanroc@cdw.com
(203) 851-7052



Tyler Payne
Account Representative
tyler.payne@cdwg.com
(203) 851-7204

CDW Education

K12 Northeast Field Team



Scott Elder
Field Sales Manager – Northeast
Email: scott.elder@cdwg.com
Phone: (703)-621-8285





Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071



Andrea Cellura
Sr. Client Executive - NY
andrea.cellura@cdw.com
(585)-364-7007



Christopher Andreu
ATAE – Upstate / Central NY
candreu@cdwg.com
(315)-329-9430



Jeremy Servian
ATAE - NYCPS
jeremy.servian@cdwg.com
(847)-465-6000



Natalie Bradley
ATAE – CT / Hudson NY
natalie.bradley@cdwg.com
(203) 899-4206



Steven Marotti
ATAE – Long Island
steve.marotti@cdwg.com
(847) 465-6000



Tim Barron
ATAE - PA
jonaker@cdw.com
(201)-264-6390



Wes Waninger
ATAE - NJ
kyle.shearman@cdwg.com
(203)-400-1339

Education

K12 Regional Leaders Southeast



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071



Jeff Grey Director, K12 Southeast
Email: jeffgre@cdwg.com Phone: (203) 851-7111
Home Office: Shelton, CT



Mike Markasovic
Sales Manager – NC/SC/TN
K12 Southeast NC/SC/TN
Email: MichaelM@cdwg.com Phone: (847) 968-9026
Home Office: Chicago



Matt Robertson
Sales Manager – FL/GA
K12 Southeast FL/GA
Email: mattrob@cdw.com Phone: (703) 262-8060
Home Office: Reston





Josh Savage
Field Sales Manager
K12 Southeast
Email: joshsav@cdw.com Phone: (615)-310-9009



Mike Pinto
Sales Manager – AT
K12 Southeast Atlantic
Email: mikepin@cdw.com Phone: (203) 851-7150
Home Office: Shelton

 | © CDW LLC 2017

K12 Atlantic Region



Adam Finch
Sales Operations Supervisor
adamfin@cdwg.com
203-851-7028



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071



Jill Griffin
Office Admin
jill@cdw.com
(203) 851-7025



Mike Pinto

Sales Manager – AT K12 East
Email: mikepin@cdw.com
Phone: (203)-851-7150
Home Office: Shelton

Account Managers





Anthony Defala Jr
Executive Account Manager
anthdef@cdw.com
(203) 851-7134



Emmery Duprey
Executive Account Manager
emmery.duprey@cdwg.com
(203) 851-7038



Mark Stout
Executive Account Manager
mstout@cdw.com
(203) 851-7129



Bill Rose
Executive Account Manager
billros@cdw.com
(203) 851-7093



Jake Maier
Account Representative
Jake.Maier@cdwg.com
(203) 851-7062



Matt Swinkin
Executive Account Manager
mstout@cdw.com
(203) 851-7129



Chris Hegan
Executive Account Manager
chriheg@cdw.com
(203) 851-7078



Jeff Rossi
Account Manager
jeffros@cdw.com
(203) 851-7074



Matt Todd
Executive Account Manager
matttod@cdwg.com
(203) 851-7184



Danny Ajro
Executive Account Manager
dritajr@cdw.com
(203) 851-7029



Jon Buzelle
Account Representative
jon.buzelle@cdwg.com
(312) 705-1892



Tigo Schauffler
Executive Account Manager
tigosch@cdwg.com
(203) 851-7246

CDW Education

K12 Southeast Region



Adam Finch
Sales Operations Supervisor
adamfin@cdwg.com
203-851-7028



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071



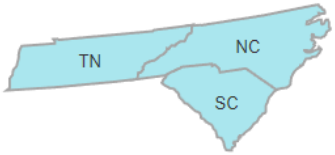
Jill Griffin
Office Admin
jill@cdw.com
(203) 851-7025



Mike Markasovic

Sales Manager – NC/SC/TN/WV
K12 East
Email: MichaelM@cdwg.com
Phone: (847) 968-9026
Home Office: Chicago

Account Managers





Phil Oberholtzer
Executive Account Manager
philobe@cdwg.com
(312) 705-3259



Ashley Pratt
Executive Account Manager
ashlpra@cdwg.com
(203) 851-7086



Darrick Tonini
Account Representative
Darrick.Tonini@cdwg.com
(203) 851-7216



Ray Sorrentino
Account Manager
raysor@cdwg.com
(203) 851-7096



Charlie Celotto
Executive Account Manager
charlie.celotto@cdwg.com
(203) 851-7153



Julie Larsen
Account Manager
jullars@cdwg.com
(203) 851-7242



Rebekah Marco
Sr. Account Manager
rebmarc@cdwg.com
(312) 547-2962



Clint Munoz
Executive Account Manager
clinmun@cdw.com
(312) 705-3398



Michael Pelaccia
Account Manager
micpela@cdwg.com
(203)-851-7006



Sophia Gurera
Account Representative
sophia.gurera@cdwg.com
(847) 371-5552

CDW Education

K12 Southeast FL/GA Region



Julie Johnston
Sales Operations Supervisor
julie.johnston@cdwg.com
(847)465-6000



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071

Account Managers



Matt Robertson
Sales Manager – FL/GA
K12 East
Email: mattrob@cdw.com
Phone: (703) 262-8060
Home Office: Reston





Evan Bleeker
Account Manager
evanble@cdw.com
(847) 465-6000



Jose Pereyda
Account Representative
jose.pereyda@cdwg.com
(312) 547-2339



Galiya Uralova
Account Representative
galiya.uralova@cdwg.com
(312) 705-0314



Matt Antonucci
Sr. Account Manager
mattant@cdwg.com
(813) 804-5381



Andrew Sio
Account Representative
Andrew.Sio@cdwg.com
(312) 705-0971



Isabela Rosales
Account Representative
isabela.rosales@cdwg.com
(312) 547-2346



Stephen Nakonechny
Executive Account Manager
stevnak@cdwg.com
(312) 705-9580



Brennan Geis
Sr. Account Manager
bregeis@cdw.com
(312) 705-3382



Jess Sutton
Executive Account Manager
jesssut@cdwg.com
(312) 705-9075



Ted Kus
Account Manager
tedkus@cdw.com
(813) 574-5545



Dominick Cozzi
Account Manager
domcozz@cdwg.com
(312) 705-4521



Jordan Stevens
Account Manager
jordste@cdwg.com
(312) 705-4533



Todd Short
Executive Account Manager
toddsho@cdw.com
(312) 705-9047

| © CDW LLC 2017

CDW Education

K12 Southeast Field Team



Josh Savage
Field Sales Manager – Southeast
Email: joshsav@cdw.com
Phone: (615)-310-9009

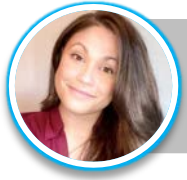




Billy Vanmeter
ATAE – DC Area
billy.vanmeter@cdwg.com
(240) 278-5842



Chris True
ATAE - NC
chris.true@cdwg.com
(803)-554-0355



Cory Minor
ATAE –Richmond, VA
cory.minor@cdwg.com
(804) 238-6923



EJ Owens
ATAE – GA
ej.owens@cdwg.com
(847) 465-6000



German Godoy
ATAE – South FL
germgod@cdw.com
(786) 575-6505



Rick Allain
ATAE – North FL
rickall@cdwg.com
(727) 204-3466



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071

CDW Education

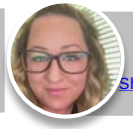
CDW Education

Education Academy / Residency Leaders & Inside Account Managers

Regional Leaders



Kristen Hengl
Executive Assistant
krishen@cdw.com
(847) 419-7539



Shannon Edmundson
SMA –Academy
Shannon.Edmundson@cdwg.com
(847)465-6000

EDU Regional Leaders Academy / Residency



Kristen Peon
SMA - HiEd
krispeo@cdw.com
(312) 705-8722



David Anderson
SMA - K12
david.anderson@cdw.com
(617) 804-4435



Kathryn Haran
Director, Public Residency
Email: kathryn.haran@cdw.com Phone: 312-705-9030
Home Office: Chicago, IL



Bryce Martin
Sales Manager – Residency
HiEd Chicago
Email: brycmar@cdw.com Phone: (866) 902-9452
Home Office: Chicago, IL



Robert DeBartolo
Sales Manager – Residency
K12 Chicago
Email: robedeb@cdw.com Phone: (847) 968-9388
Home Office: Chicago, IL



Jairo Ortiz
Sales Manager – Academy
HiEd Chicago
Email: jairort@cdw.com Phone: (312) 547-8190
Home Office: Chicago, IL



Sarah Stacey
Sales Manager – Residency
EDU Shelton
Email: sarah.rosenfeld@cdwg.com Phone: (203)851-7128
Home Office: Shelton, CT



Meghan Ruscheinski
Sales Manager – Academy
Public Lincolnshire
Email: meghrus@cdwg.com Phone: (847) 371-7662
Home Office: Chicago, IL

K12 Residency



Robert DeBartolo
Sales Manager – Residency
K12 Chicago
Email: robedeb@cdw.com
Phone: (847) 968-9388
Home Office:



Mark Mahler
Sales Ops Supervisor
markmah@cdw.com
(847) 968-0451



David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435

Account Representatives



Dani Stecyna - NC
Account Representative
danielle.stecyna@cdwg.com
(312) 705-4059



Galiya Uralova–FL/GA
Account Representative
galiya.uralova@cdwg.com
(312) 705-0314



Hannah Baker - OV
Account Representative
hannah.baker@cdwg.com
(312) 705-5257



Jake Huisman - NC
Account Representative
jake.huisman@cdwg.com
(847) 968-0690



Jake Miles – TE
Account Representative
jake.miles@cdwg.com
(847) 968-0702



Marc Arias - MW
Account Representative
marc.arias@cdwg.com
(847)-968-0685



Marshall Francis – NC
Account Representative
marshall.francis@cdwg.com
(312) 705-0211



Matt Albrecht - HL
Account Representative
matt.albrecht@cdwg.com
(847) 968-0693



Meg Heaphy - MW
Account Representative
meg.heaphy@cdwg.com
(847) 371-5540



Nic Snedden - HL
Account Representative
nic.snedden@cdwg.com
(312) 705-1894



Nikki Serra - OV
Account Representative
nikki.serra@cdwg.com
(312) 705-0371



Peter Taylor - CN
Account Representative
peter.taylor@cdwg.com
(312) 547-2259



Sophia Gurera - SE
Account Representative
sophia.gurera@cdwg.com
(847) 371-5552

Education

HiEd Residency



Bryce Martin
Sales Manager – Residency HiEd Chicago
Email: brycmar@cdw.com
Phone: (866) 902-9452
Home Office: Chicago, IL



Maureen Kaluzny
Sales Ops Supervisor
maurkal@cdw.com
(312) 547-2585



Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722

Account Representatives



Alex Gee-ML
Account Representative
alex.gee@cdwg.com
(312) 705-4058



Allison Winans-PAC
Account Representative
allison.winans@cdwg.com
(312) 705-0269



Anne Tracy-SE
Account Representative
anne.tracy@cdwg.com
(312) 547-2827



Austin Atkins-GC
Account Representative
austin.atkins@cdwg.com
(312) 507-0177



Carson Kirchner - SE
Account Representative
carson.kirchner@cdwg.com
(312) 547-2262



Charlie Prangl - HBCU
Account Representative
charlie.prangl@cdwg.com
(312) 547-2310



Danny Kee - SE
Account Representative
danny.kee@cdwg.com
(312) 705-1898



Felicia Moncada - NW
Account Representative
felicia.moncada@cdwg.com
(312) 705-1886



Jeffrey Baumann-GC
Account Representative
jeff.baumann@cdwg.com
(312) 705-4564



Joe Freedlund-GC
Account Representative
joseph.freedlund@cdw.com
(312) 705-0204



Jack Fitzgerald – IL IN
Account Representative
jack.fitzgerald@cdwg.com
(312) 547-2267



Joe Buffo - SE
Account Representative
joe.buffo@cdwg.com
(312) 705-0396



Joe Devine - NW
Account Representative
joe.devine@cdwg.com
(312) 547-2225



Josh McCray-MT
Account Representative
josh.mccray@cdwg.com
(312) 705-4507



Katie Loehr - PAC
Account Representative
katie.loehr@cdwg.com
(312) 547-2279



Maxwell Smith - OV
Account Representative
maxwell.smith@cdwg.com
(312) 547-2239



Rachel Boldt - DL
Account Representative
rachel.boldt@cdwg.com
(312) 547-2243



Rigo Alvarez-SE
Account Representative
rigo.alvarez@cdwg.com
(312) 705-0249



Samuel Humanchuk-OV
Account Representative
sam.humanchuk@cdwg.com
(312) 547-2826

CDW Education

Shelton Residency



Sarah Stacey
Sales Manager – Residency
Public - Shelton
Email: sarah.rosenfeld@cdwg.com
Phone: 203-851-7128
Home Office: Shelton, CT



Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071

K12



Anthony Brown - NE
Account Representative
tony.brown@cdwg.com
(203) 851-7032



Cassidy Chapman -KY
Account Representative
cassidy.chapman@cdwg.com
(203) 851-7050



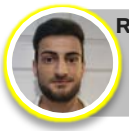
Christopher Perone-KY
Account Representative
chris.perone@cdwg.com
(203) 851-7170



Jonathan Buzelle – AT
Account Representative
jon.buzelle@cdwg.com
(203) 513-3526



Le'Nina Williams - NY
Account Representative
lenina.williams@cdwg.com
(203) 851-7162



Rosario Cappetta - NE
Account Representative
rosario.cappetta@cdwg.com
(203) 851-7277



Tyler Payne - NY
Account Representative
tyler.payne@cdwg.com
(203) 851-7204

HiEd



Bill Lobdell-AT
Account Representative
bill.lobdell@cdwg.com
(203) 851-7126



Edwin Guerrero-KY
Account Representative
edwin.guerrero@cdwg.com
(203) 851-7011



Giovanni Trocchia-KY
Account Representative
gio.trocchia@cdwg.com
(203) 851-7293



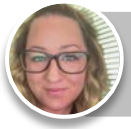
Jordon Biondi-AT
Account Representative
jordon.biondi@cdwg.com
(203) 851-7205



Troy Hart-AT
Account Representative
troy.hart@cdwg.com
(203) 851-7131

CDW Education

HiEd Academy



Shannon Edmundson
SMA –Academy
Shannon.Edmundson@cdwg.com
(847)465-6000



Jairo Ortiz
Sales Manager – Academy
HiEd Chicago
Email: jairort@cdw.com
Phone: (312) 547-8190
Home Office: Chicago, IL

Account Representatives



Adam Jaloudi - NE
Account Representative
adam.jaloudi@cdwg.com
(203) 899-2158



Alexa Morrow - DL
Account Representative
alexa.morrow@cdwg.com(312) 547-2634



Bina Patel - SE
Account Representative
bina.patel@cdwg.com
(312) 705-0982



Carianne Asberry - GC
Account Representative
carianne.asberry@cdwg.com
(818) 254-1746



Charles Rhodes - NE
Account Representative
charlie.rhodes@cdwg.com
(203) 899-2154



Crystal Price - OV
Account Representative
crystal.price@cdwg.com
(312) 547-2645



Eduardo Leonides - NW
Account Representative
eduardo.leonides@cdwg.com
(312) 547-2650



Kelsey Baker – IL IN
Account Representative
kelsey.baker@cdwg.com
(312) 547-2628



Marc Liquindoli - AT
Account Representative
marc.liquindoli@cdwg.com
(203) 899-7651



Peter Turelli - PAC
Account Representative
peter.turelli@cdwg.com
(847) 371-5516



Richard Sakofsky - PAC
Account Representative
rich.sakofsky@cdwg.com
(480) 270-7006



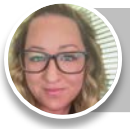
Sarah Maulucci - AT
Account Representative
sarah.maulucci@cdwg.com
(203) 899-2160

CDW Education

K12 Academy



Meghan Ruscheinski
Sales Manager – Academy
EDU Lincolnshire
Email: meghruc@cdwg.com
Phone: (847) 371-7662
Home Office: Chicago, IL



Shannon Edmundson
SMA –Academy
Shannon.Edmundson@cdwg.com
(847)465-6000

Account Representatives



Abby Kuchler - OV
Account Representative
abbkuch@cdwg.com
(312) 547-2630



Abby Moriarty - MW
Account Representative
abby.moriarty@cdwg.com
(312) 547-2639



Alexa Cohen - GU
Account Representative
alecohe@cdwg.com
(312) 547-2632



Gustavo Diaz -- TX
Account Representative
gustavo.diaz@cdwg.com
(312) 547-2611



Hunter Kingwill - WS
Account Representative
hunter.kingwill@cdwg.com
(312) 547-2367



Isabela Rosales–FL/GA
Account Representative
isabela.rosales@cdwg.com
(312) 547-2346



Jose Pereyda-FL/GA
Account Representative
jose.pereyda@cdwg.com
(312) 547-2339



Katelin Rembert - OV
Account Representative
katelin.rembert@cdwg.com
(312) 705-8258



Luke Mahar-NC
Account Representative
luke.mahar@cdwg.com
(312) 547-2361



Marie Soupart - GU
Account Representative
marie.soupart@cdwg.com
(312) 547-2376



Mohamed Awad - NC
Account Representative
mohawad@cdwg.com
(312) 547-2625

Education



Education Customer Enablement Team

Regional Leaders

EDU Customer Enablement Team



Sean Galligan
Senior Manager –
K12 Customer Enablement Team
Email: seangal@cdw.com Phone: (203) 851-7042
Home Office: Shelton, CT



Tony Vitale
Director, Customer Enablement Team
Email: tonyvit@cdw.com Phone: (312)705-3253
Home Office: Chicago, IL



Mike Peters
Senior Manager –
Customer Enablement Education Solutions
Email: mikpet@cdw.com Phone: (312) 705-8940
Home Office: Chicago, IL



Jessica Bright
Senior Manager –
HiEd Customer Enablement Team
Email: Jessica.Bright@amplifiedit.cdw.com Phone: (203) 851-7042
Home Office:



Michael Waters
Senior Manager – Sales Enablement
Email: michael.walters@amplifiedit.cdw.com Phone: (757) 276-7268
Home Office:



Michael Beeson
Dir EDU Impact and Initiatives
Email: mike.beeson@amplifiedit.cdw.com Phone: (847) 465-6000
Home Office: Chicago, IL

CDW AMPLIFIED™ for Education

EDU Customer Enablement Team



Jessica Bright
Senior Manager –
HiEd Customer Enablement Team
Email: Jessica.Bright@amplifiedit.cdw.com
Phone: (719)-359-3326
Home Office: Chicago, IL

Customer Success - Hi Ed



Mark Rosenblum
Sr. Cloud Strategist - HiEd
marrose@cdw.com
(847) 465-6000



Paris Clark
Customer Success Strategist
paris.clark@amplifiedit.cdw.com
(312) 210-3613



Jennifer Clark
Customer Success Strategist
jennifer.clark@amplifiedit.cdw.com
(206) 743-1974



Shannon Forte
Customer Success Strategist
shannon.forte@amplifiedit.cdw.com
(754) 200-1464

CDW AMPLIFIED for Education

CDW Amplified for Education



Michael Beeson
Director – EDU Impact and Initiatives
Email: mike.beeson@amplifiedit.cdw.com
Phone: (203) 851-7179



Amy Passow
Senior Manager – EDU Funding Solutions
Email: amypass@cdw.com
Phone: (719)-359-3326



Doug Konopelko
Sr. Manager Education Impact
Email: dougkon@cdw.com Phone: (847) 465-6000



Gabe Arias
Senior Manager – Education Digital Scale
Email: gabe.arias@cdw.com
Phone: (312) 447-1988

EDU Customer Enablement Team



Amy Passow
Sr Manager
Education Funding Solutions
Email: amypass@cdw.com
Phone: (719)-359-3326
Home Office: Chicago, IL

Education Funding Solutions Team



Alex Kalayil
Business Development Strategist
alex.kalayil@cdwg.com
(630) 263-0520



Dave LeNard
E-Rate Manager
dave.lenard@cdwg.com
(202) 941-9378



Shaun Albrechtson
Customer Enablement Specialist: Extreme
shaun.albrechtson@cdwg.com
(763) 592-5838



Heather Frazer
Customer Enablement Specialist: Cisco
heatfra@cdwg.com
(734) 635-7341



Shannon Brown
Customer Enablement Specialist: Aruba
shabrow@cdw.com
(312) 796-4392

CDW AMPLIFIED for Education

EDU Customer Enablement Team



Gabe Arias
Senior Sales Manager
Email: gabe.arias@cdw.com
Phone: (312) 705-5686
Home Office: Chicago



Jon Grey
Supervisor – Digital EdTech
Email: jongray@cdw.com
Phone: (203) 851-7133
Home Office: Shelton

Education Marketing Team



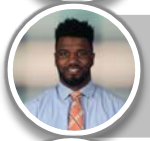
Alex Wojciechowski
Ed Tech Advisor
Alex.Wojciechowski@cdwg.com
(312) 547-2613



Brion Jacobs
Residency Ed Tech Advisor
brion.jacobs@cdwg.com
(312) 547-2384



Carey Abrams
Ed Tech Advisor
careabr@cdwg.com
(312) 705-6915



Damien Smith
Ed Tech Advisor
damiesm@cdw.com
(480) 270-7392



Hannah Like
Residency Ed Tech Advisor
hannah.like@cdwg.com
(312) 547-2359



Jonny Santana
Residency Ed Tech Advisor
jonny.santana@cdwg.com
(312) 547-2393



Matt Smith
Residency Ed Tech Advisor
matt.smith@cdwg.com
(312) 547-2385



Max Jones
Ed Tech Advisor
maxjone@cdwg.com
(312) 705-4538



Nick Schultz
Ed Tech Advisor
nischul@cdwg.com
(312) 547-5027



Nick Strauss
Ed Tech Advisor
nicstrau@cdwg.com
(312) 705-8936



Tristen Slater
Confidential Residency Ed Tech Advisor
tristen.slater@cdwg.com
(312) 547-2363

CDW AMPLIFIED™ for Education

Amplified for Education



Doug Konopelko
Sr. Manager Education Impact
Email: dougkon@cdw.com Phone: (847) 465-6000



Danielle Rourke
Education Business Development Manager
Email: danielle.rourke@cdwg.com
Phone: (847) 465-6000



Wendy Jones
Education Business Development Manager
Email: wendy.jones@cdwg.com
Phone: (737) 267-5563



Cari Warnock
Education Ambassador
Email: cari.warnock@cdw.com
Phone: (847) 465-6000



Janice Mertes
Education Ambassador
Email: janice.mertes@cdw.com
Phone: (847) 465-6000



Natalia LeMoyne Hernandez
Manager, Education Community
Email: natalia.lemoyne@amplifiedit.cdw.com
Phone: (847) 465-6000



Nori Barajas-Murphy
Education Ambassador
Email: nori.barajas@cdw.com
Phone: (847) 465-6000

 © CDW LLC 2017

Amplified IT for Education



Danielle Rourke

Manager – Business Development

Email: dougkon@cdw.com Phone: (847) 465-6000

K12 & HiEd

Esports Team



Jen Dawson

AIT Education Esports

ariafle@cdw.com

(909) 253-5959



Josh Whetherholt

AIT Education Esports

joshwhe@cdwg.com

(929) 286-1075

CDW AMPLIFIED for Education

Amplified IT for Education



Wendy Jones

K12 Education Strategist Manager
Email: wendy.jones@cdwg.com
Phone: (737) 267-5563
K12

Education Strategy Team



Akilah Willery
K12 Education Strategist - South
akilah.willery@cdwg.com
(281) 889-8560



Jennette Vanderpool
K12 Education Strategist – West-Cal
j.diamond-vanderpool@cdwg.com
(847) 465-5600



Bryan Krause
K12 Education Strategist - West
bryan.krause@cdwg.com
(720) 703-8935



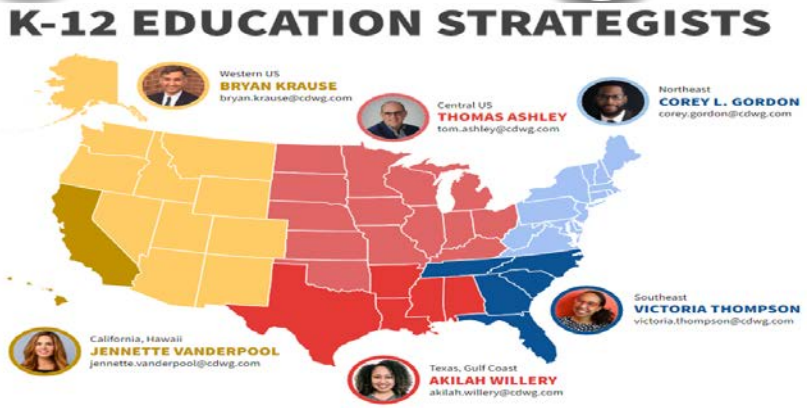
Tom Ashley
K12 Education Strategist - Central
tom.ashley@cdwg.com
(260) 519-8045



Corey Gordon
K12 Education Strategist - Northeast
corey.gordon@cdwg.com
(646) 509-9935



Victoria Thompson
K12 Education Strategist
victoria.thompson@cdwg.com
(847) 465-5600



CDW AMPLIFIED for Education

AIT Sales Enablement Team



Michael Walters
Senior Manager – Sales Enablement
Email: michael.walters@amplifiedit.cdw.com
Phone: (757) 276-7268
Home Office: Chicago, IL



Catherine Gold
Senior Manager – Education Marketing
Email: Catherine.Gold@cdw.com
Phone: (347) 224-0235
Home Office: New York



Kristin Wisniewski
Sr Program and Enablement Spec
Email: krishof@cdw.com
Phone: (847) 419-6144



Keegan Morrison
Manager – Systems
Email: keegan.morrison@amplifiedit.cdw.com
Phone: (847) 465-6000

CDW AMPLIFIED™ for Education

EDU Customer Enablement Team



Catherine Gold
Senior Manager
Education Marketing
Email: Catherine.Gold@cdw.com
Phone: (347) 224-0235
Home Office: New York

Education Marketing Team



Aleksandra (Ola) Ziemacka
Education Marketing Program Manager
ola.ziemacka@amplifiedit.cdw.com
(847) 465-6000



Ashley Ion
Lead Marketing Delivery Specialist
ashley.ion@cdwg.com
(847) 465-6000



Brady Heinrich
Lead Digital Marketing Specialist
brady.heinrich@amplifiedit.cdw.com
(847) 465-6000



Jada Dawson
Lead Content Delivery Specialist
jada.dawson@amplifiedit.cdw.com
(847) 465-6000



Scott Melville
Digital EdTech Marketing Manager
scott.melville@cdwg.com
(847) 465-6000

CDW AMPLIFIED for Education

AIT Sales Enablement Team



Keegan Morrison
Manager – Systems
Email: keegan.morrison@amplifiedit.cdw.com
Phone: (847) 465-6000

Infrastructure Modernization Team



Adam Van Doren
Data Consultant
adam.vandoren@amplifiedit.cdw.com
(847) 465-6000



Jarrett Hatchett
Systems Engineer
j.hatchett@amplifiedit.cdw.com
(847) 465-6000

CDW AMPLIFIED for Education

Customer Enablement, Education Solutions Team



Mike Peters
Senior Manager – Customer Enablement
Education Solutions
Email: mikpet@cdw.com
Phone: (312) 705-8940



Wayne Lawson
Education Ambassador
Email: wayne.lawson@cdw.com
Phone: (847) 465-6000



Maggie Gang
Bus Dev Strategist
Microsoft Device Specialist
Email: maggie.gang@cdwg.com
Phone: (847) 465-6000



Ari Flewelling
Sr Bus Dev Strategist
Professional Development Manager
Email: ariafle@cdw.com
Phone: (909) 253-5959



Caitlin Witry
Sr Mgr Business Development
Email: caitw@cdw.com
Phone: (312) 547-2358



Heather Rose
Education Ambassador
Education Partner Program
Email: heather.rose@cdwg.com
Phone: (847) 465-6000



Derek Carnwath
Program Manager
Email: derecar@cdw.com
Phone: (813) 547-5534



Maureen Corlett
Manager
Classroom Modernization Customer Success
Email: Maursmi@cdw.com
Phone: (203) 851-7179

K-12 Education Partner Program



Caitlin Witry
Sr. Manager Business Development
Email: caitw@cdw.com
Phone: (312) 547-2358
Home Office: FIELD

TBH
Education Partners Specialist
email@cdw.com
(847) 465-6000



Ana Luong
Bus Dev Strategist
ana.luong@cdw.com
(425) 943-2008



Dan Hogan
Go Guardian Specialist
danhog@cdw.com
(312) 705-6228



Brian Putka
Education Partners Specialist
brian.putka@amplifiedit.cdw.com
(330) 687-1950



Kevin McMahon
Bus Dev Manager
kevimcm@cdwg.com
(847) 371-7113

CDW AMPLIFIED for Education

Customer Enablement, CDW Local Education Solutions



Derek Carnwath
Manager – Device Lifecycle
Email: derecar@cdw.com
Phone: (813) 547-5534
Home Office:

Christian Anderson
Program Manager
christian.anderson@cdw.com
(469) 249-6585

CDW AMPLIFIED for Education

EDU Customer Enablement Team



Maureen Corlett
Manager
Classroom Modernization
Customer Success
Email: Maursmi@cdw.com
Phone: (203) 851-7179
Home Office: Shelton, CT

Classroom Modernization Team



TBH
Business Development



Eden Howe
Business Development
eden.howe@cdwg.com
(847) 465-6000



TBH
BDM - Samsung



Ivan Ours
FSA
ivan.ours@cdwg.com
(847) 465-6000



Santino Martinez
Sr. Classroom Modernization Strategist
santino.martinez@cdwg.com
(312) 914-9787



Jim Spencer
FSA
jim.spencer@cdwg.com
(847) 465-6000



Ted Bartnik
Classroom Modernization Strategist
theodore.bartnik@cdw.com
(708) 227-8120

CDW AMPLIFIED for Education

K12 Google Customer Success Team



Sean Galligan
Senior Sales Manager
Email: seangal@cdw.com Phone: (203) 851-7042



Chris Hanson
Manager
Chrome Customer Enablement Customer Success
Email: chrishan@cdwg.com Phone: (847) 465-6000



Mike Reorowicz
Sales Manager – West/Central
Email: mikereo@cdwg.com Phone: (312) 547-2196



Erika Renfrew
Sales Manager – East
Email: erika.renfrew@amplifiedit.cdw.com Phone: (602) 598-1584



Peter Henrie
Business Development Manager
Email: peter.henrie@amplifiedit.cdw.com
Phone: (847) 465-6000



Tanya Holloran
Manager
Google Workspace & Education Partners Customer Success
Email: tanya.holloran@amplifiedit.cdw.com Phone: (847) 465-6000

CDW AMPLIFIED™ for Education

K-12 Google Customer Success - West



Jordan Harrison
Sr. Sales Operations Supervisor
jordhar@cdw.com
(847) 968-9937



Mike Reorowicz
Sales Manager – Central
Email: mikereo@cdwg.com
Phone: (312) 547-2196
Home Office: Chicago, IL



Adam Kofod
K-12 Google Customer Success Specialist
AK, ID, NM, WA, AZ, MT, OR, WY:
ALL ENROLLMENTS
adam.kofod@amplifiedit.cdw.com
(650) 204-0006



Darian Venerable
K-12 Google Customer Success Specialist
CA, CO, NV, UT: BELOW 5K
darian.venerable@amplifiedit.cdw.com
(909) 206-2533



Rosario Pascasio
K-12 Google Customer Success Specialist
CA, NV, CO, UT: ABOKE 5K
HI: ALL ENROLLMENTS
rosario.pascasio@amplifiedit.cdw.com
(757) 828-3843

CDW AMPLIFIED for Education

EDU Customer Enablement Team

David Andrade
Business Development Manager, Google Services
Email: davandr@cdw.com Phone: (203) 851-7290
Home Office: Shelton, CT



Chris Hanson
Manager
Chrome Customer Enablement
Customer Success
Email: chrishan@cdwg.com
Phone: : (262) 496-1440
Home Office: Chicago, IL

K12 Google Chrome Sales Specialist Team



David Andrade
Business Development Manager
davandr@cdw.com
(203) 851-7290



Michael Collins
Business Development Manager
michcol@cdwg.com
(847) 465-6000



Todd Miletti
Chrome Device Specialist -Google
todd.miletti@cdwg.com
(248) 877-7380

CDW AMPLIFIED for Education

K-12 Google Customer Success - East



Jordan Harrison
Sr. Sales Operations Supervisor
jordhar@cdw.com
(847) 968-9937



Erika Renfrew
Sales Manager – East
Email: erika.renfrew@amplifiedit.cdw.com
Phone: (602) 598-1584
Home Office: FIELD



Dana Jackson
Google Customer Success Specialist
CANADA
dana.jackson@amplifiedit.cdw.com
(703) 262-8132



Lauren Piroscafo
Google Customer Success Specialist
New England - CT, MA, ME, NH, RI, VT
laurpir@cdwg.com
(203) 851-7145



Ryan Pronk
Google Customer Success Specialist
NY
ryan.pronk@amplifiedit.cdw.com
(757) 354-4396



Robert Tiffey
Google Customer Success Specialist
Keystone - NJ, PA Southeast (Sub5K) -
TN, NC, SC, GA, FL, WV, VA, MD, DE
derecar@cdw.com
(202) 735-1412



Shannon Jesequel
Google Customer Success Specialist
Southeast –
TN, NC, SC, GA, FL, WV, VA, MD, DE
s.jesequel@amplifiedit.cdw.com
(703)262-8009

CDW AMPLIFIED for Education

K-12 Google Customer Success - Central



Jordan Harrison
Sr. Sales Operations Supervisor
jordhar@cdw.com
(847) 968-9937



Mike Reorowicz
Sales Manager – West
Email: mikereo@cdwg.com
Phone: (312) 547-2196
Home Office: Chicago, IL



Amaury McCormack
Google Customer Success Specialist
IA, MN, NE, KS, MO, ND, OK, SD, WI
ENROLLMENT BELOW 5K
amaurymccormack@amplifiedit.com
(512) 238-7549



Alex Kwiatkowski
K-12 Google Customer Success Specialist
AL, LA, TX, AR, MS
ENROLLMENT BELOW 5K
a.kwiatkowski@amplifiedit.cdw.com
(216) 200-8917



Bridget Porro
K-12 Google Customer Success Specialist
AL, KS, MS, OK, AR, LA, MO, TX
ENROLLMENT ABOVE 5K
bridget.porro@amplifiedit.cdw.com
(757) 255-8530



Dana Jackson
K-12 Google Customer Success Specialist
IL, IA, MI, NE, OH, IN, KY, MN, ND, SD, WI:
ENROLLMENT ABOVE 5K
dana.jackson@amplifiedit.cdw.com
(757) 255-8895



Kim Mauney
K-12 Google Customer Success Specialist
IL, KY, OH, IN, MI
ENROLLMENT BELOW 5K
kim.mauney@amplifiedit.cdw.com
(704) 251-0736

CDW AMPLIFIED for Education

EDU Customer Enablement Team

GOOGLE WORKSPACE & EDUCATION PARTNERS



Tanya Holloran
Manager
Google Workspace & Education Partners Customer Success
Email: tanya.holloran@amplifiedit.cdw.com
Phone: (847) 465-6000
Home Office:

Google Workspace & Education Partners

Emily Frankoff
Google Workspace For Education Specialist
emily.frankoff@amplifiedit.cdw.com
(847) 465-6000



Michelle Tindle
Google Workspace For Education Specialist
michelle.tindle@amplifiedit.cdw.com
(847) 419-7560



Gil Anspacher
Google Workspace For Education Specialist
edwin.anspacher@cdwg.com
(847) 465-6000



Ryan Eick
Sr Bus Dev Strategist
ryaneic@cdwg.com
(847) 419-7560

CDW AMPLIFIED for Education



Education
Business Development

K-12 / HIGHER EDUCATION BUSINESS DEVELOPMENT



Chris Webb
Director, Capture & Business Development



Lisa Missana
Assistant

Large Account BD & Contract Capture



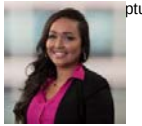
Melissa Deets



Debb Atnip
Manager, pture



Nicole Tuzzolino
Contract Success BD



Amanda Coleman
Edu BD, West



Leah Guerrero
Edu BD, Central



Stephanie Christensen
Edu BD, East

Partner Growth BD - Solutions



Jennifer Roth



Lindsay Drake
VMware BD



Damir Karahodzich
Aruba/HPE BD



Mary Cesaretti
Dell/EMC BD



Mark Santaromita
APC BD

OPEN
Palo Alto BD

Partner Growth BD - Core



Eric Schmitt



Brooke Langley



Collin Young
Apple BD



Anthony Orticelli
Campus Interns - West



Anthony Fiore
Campus Interns - East

Education Additional Resources

EDU Project Management Team



Kim Ciaccio
Supervisor- Project Manager, EDU
Email: kimbhay@cdw.com Phone: (312) 705-5268
Home Office: Chicago, IL



Cassie Floersch
Associate Manager – HiEd
Email: cassflo@cdw.com Phone: (312) 705-8836
Home Office: Chicago, IL



Danielle Ryan
Project Manager
Email: danielle.ryan@amplifiedit.cdw.com Phone: (847) 465-6000
Home Office:

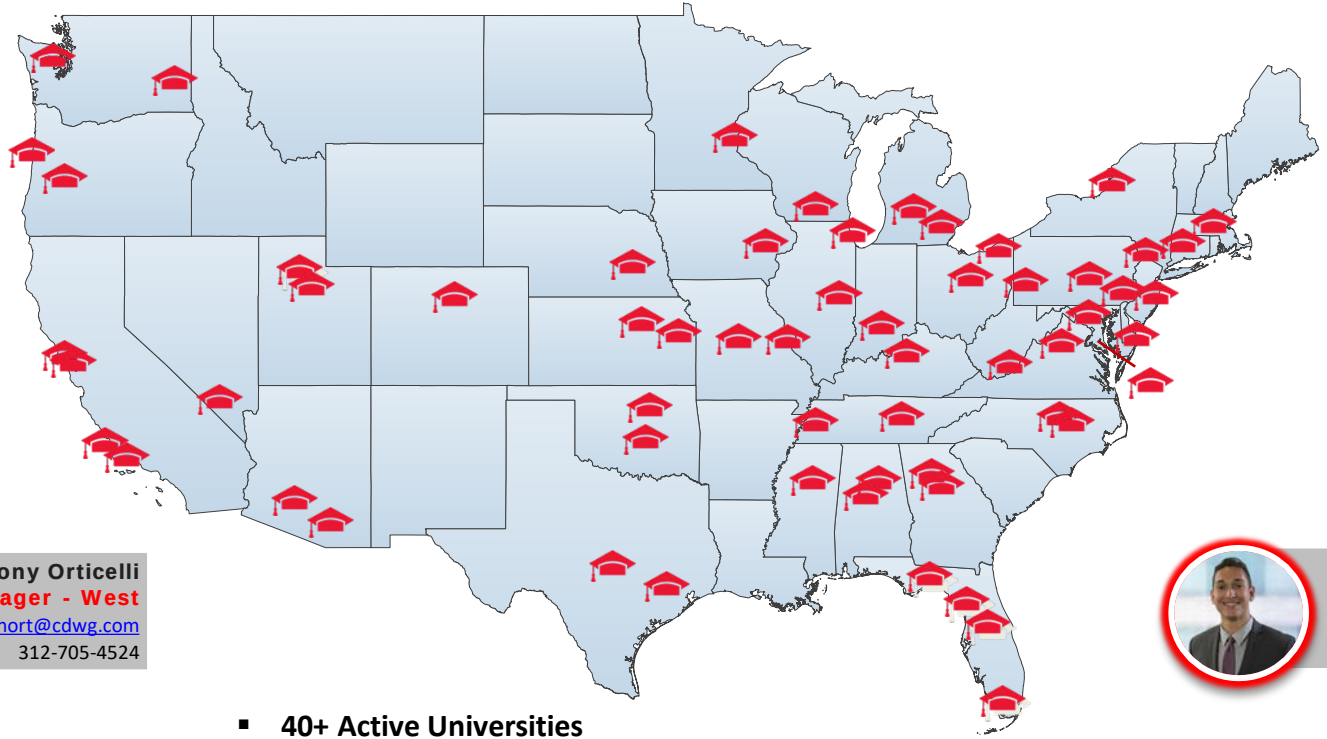


Julie D'Angelico
Associate Manager – K12
Email: julituz@cdwg.com Phone: (203) 851-7291
Home Office:



Education Maps

Campus Intern Coverage Map





Anthony Orticelli
Manager - West
anthort@cdwg.com
312-705-4524

Anthony Fiore
Manager – East
anthfio@cdwg.com
312-705-5598

- **40+ Active Universities**
- **Nationwide Footprint**
- **1:1 Campus Coverage**

CDW·G Campus Intern Program

THANK YOU!



CDW Education

CDW AMPLIFIED™ for Education

CDW·G PEOPLE WHO GET IT™

AEPA RFP #025

Cyber Security & Training and Security Solutions

Digital Response | 9/17/2024 1:30 PM ET



CDW Education

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW·G").

9/17/2024

Association of Educational Purchasing Agencies

CDW Education

One CDW Way
230 N. Milwaukee Avenue
Vernon Hills, IL 60061
Toll-free: 800.808.4239
F: 847.465.6800
cdwg.com/PeopleWhoGetIT

RE: CDW Education Response to Association of Educational Purchasing Agencies' AEPA RFP #025

To the AEPA Evaluating Committee,

Association of Educational Purchasing Agencies (AEPA) is seeking a reliable and experienced supplier partner capable of providing Cybersecurity & Training services and Security Solutions in the eight AEPA Member Regions. CDW Education's response demonstrates our ability to contribute to the overall success of this initiative.

CDW Education is a specialized segment of CDW Government LLC (CDW·G), the wholly owned subsidiary of CDW LLC. CDW is now the largest security integrator in North America. Specific advantages of partnering with us include:

- **An experienced account team** that will support AEPA members' day-to-day IT needs, connect them with resources, and ensure satisfaction with our services. Your account team's expertise developing solutions that provide robust functionality, efficiencies, and cost savings directly benefits AEPA members throughout the lifecycle of the contract.
- **Comprehensive security practice** that has the depth and breadth to support the entire cybersecurity journey of AEPA members, helping them to mature and scale security programs that drive toward business objectives without slowing down innovation. Our security team includes 500+ professionals focused on cybersecurity, 350+ delivery engineers, architects, and consultants, and 150+ presales architects and advisors focusing on delivering full lifecycle cyber solutions.
- **Hands-on experience deploying successful complex projects**, including in adverse conditions. We have delivered 40,000+ cybersecurity solutions, have trained 17K+ cybersecurity professionals, and delivered $3.9B in security solutions and services. We continually evaluate and adapt our approach, ever mindful of logistics and possibilities to proactively identify and mitigate challenges in physical and virtual environments.

As always, we consistently strive to exceed your expectations. Should you have any questions regarding our response, please contact Jeff Hagen, Manager Program Management at 813.462.4055 or jeff.hagen@cdwg.com or Stephanie Kessler, Deputy Program Manager at 920.996.3100 or kessler@cdw.com. We thank you for the opportunity to participate in this RFP process and are confident you will find our response advantageous from both a strategic and budgetary standpoint.

Sincerely,



Dario Bertocchi
VP Contracting Operations
CDW Education

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW·G").

Table of Contents

CDW Government Overview **4**

Large Onsite Inventories 5

CDW Cybersecurity Risk Management Services **6**

Breadth of Capabilities 6

Security Solutions **10**

Our Knowledge Goes Deep 10
Meet Our Security Experts 11
Certifications 12

Our World-Class Technology Partnerships **15**

Attachments **16**

Attachment A: CDW Security Capabilities (11 pages) 17
Attachment B: CDW_WFD Catalog (93 pages) 18

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW·G").

CDW Government Overview

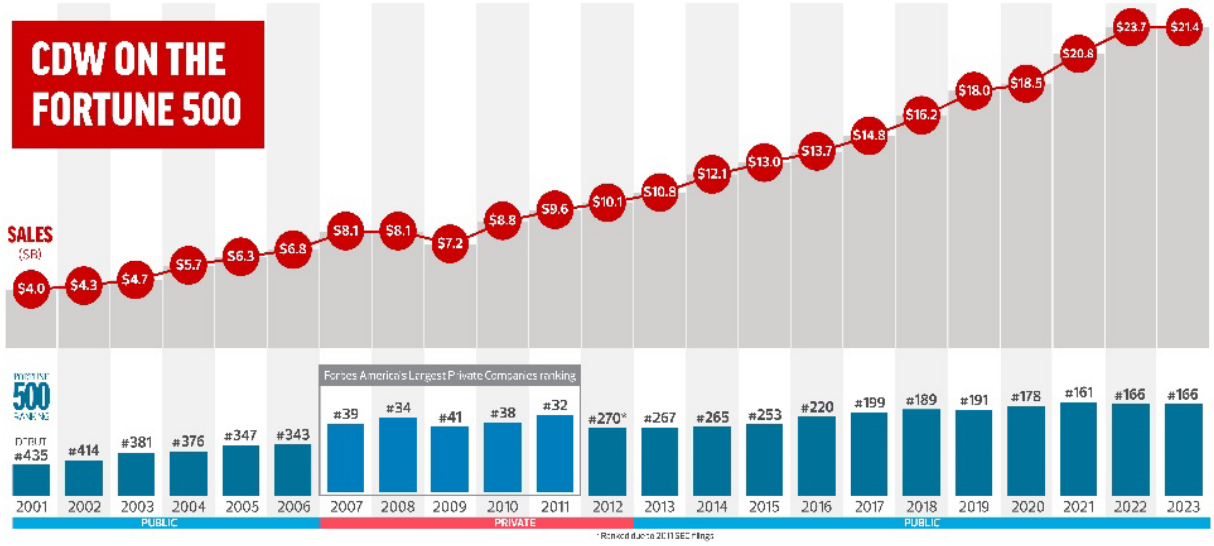
CDW is a leading multi-brand technology solutions provider to business, government, education and healthcare organizations in the United States, the United Kingdom and Canada. A Fortune 500 company with multi-national capabilities, CDW was founded in 1984 and employs approximately 15,100 coworkers. We have an expansive network of offices near major cities and a large team of field coworkers across the United States. CDW Government LLC is the wholly owned subsidiary of CDW LLC. Our customer base is quite diverse, ranging from state and local government, federal, healthcare, K-12, and higher education.

- **Headquarters:** Vernon Hills, IL
- **2023 Annual Net Sales:** $21B
- **# of Coworkers:** 15,100
- **# of U.S. Offices:** 53
- **# of Customers:** 250,000+
- **Fortune 500 Rank (2023):** 166

Our broad array of offerings range from discrete hardware and software products to integrated IT solutions such as mobility, security, data center optimization, cloud computing, virtualization and collaboration. We are technology "agnostic," with a product portfolio that includes more than 100,000 products from more than 1,000 brands. We provide our products and solutions through our sales and service delivery teams, consisting of nearly 6,000 customer-facing coworkers, including more than 2,000 field sellers, highly skilled technology specialists and advanced service delivery engineers.



CDW debuted on the Fortune 500 in 2001, at No. 435. CDW's rise in the rankings highlights its sustainable, profitable growth over the years, from $4 billion in sales in 2001 to $24 billion in 2022. CDW now ranks at number 166 on the FORTUNE 500 list for 2023. CDW ranks at No. 5 on CRN's Solution Provider 500 list for 2024.



© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW·G").

Large Onsite Inventories

CDW has two large, strategically located distribution centers controlled by a state-of-the-art Warehouse Management System (WMS) that ensures speed and accuracy throughout the order fulfillment and distribution processes. CDW has a 450,000-square-foot distribution center located at our headquarters in Vernon Hills, IL and a 513,000-square-foot distribution center located in North Las Vegas, NV. These locations facilitate quick distribution of products to our growing customer base throughout the country. The Vernon Hills (VH) distribution center focuses on distributing products to customers east of the Mississippi River while the Las Vegas (LV) distribution center primarily serves the western part of the United States.



450,000-square-foot distribution center in IL



513,000-square-foot distribution center in NV

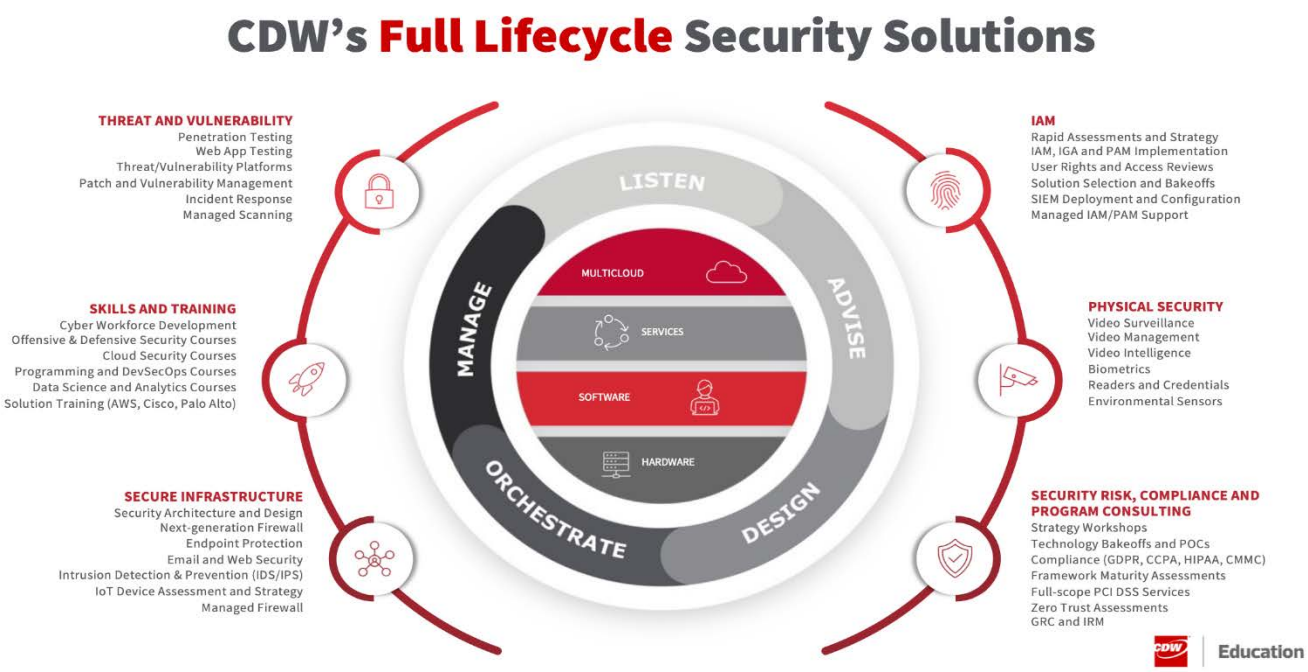
CDW holds more than $300M of available inventory in our two CDW-owned distribution centers that total almost 1M square feet. Our ISO 9001, 14001 and 28000 certified strategically located distribution centers provide speed, accuracy, and excellent geographic coverage across the United States. We have access to more than 100,000 top brand-name products from more than 1,000 leading manufacturers.

Due to the size of our facilities that span four levels of storage and three level picking modules, forklifts are required to stock and pick products as needed. Our product lineup includes desktops, notebooks, servers, peripherals, networking and communications equipment, software, accessories, plotters, network printers, desktop printers, and print supplies. CDW offers everything your IT operation could possibly need – from enterprise solutions to mouse pads.

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW·G").

CDW Cybersecurity Risk Management Services



Breadth of Capabilities

CDW has one of the most complete portfolios of security services in the market today. Our delivery teams are organized along seven core disciplines, though many customer risk management initiatives bridge multiple domains. The breadth of our capabilities allows us to help customers identify and solve all of their problems – not just one. These delivery teams include:

- **Program Strategy and Operations** – Security and risk management program design, with a focus on framework alignment, program maturity, and risk consulting.
- **Data and Application** – Protect your information assets against mistakes that lead to data leaks and intentional misuse by insiders, as well as external attacks on your information infrastructure. Our data-centric security program includes application security, security intelligence and analytics, DLP strategy and roadmaps, data protection programs, data discovery, handling, and classification, web app firewalls (WAF), and more.
- **Cloud Security** – Security assessment and services designed to measure data flows through cloud and hybrid environments.
- **Identity and Access Management (IAM)**– Solution assessment, design, implementation, and management for workforce and customer use cases across AM, IGA, PAM, and SIEM.

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW·G").

- **Secure Infrastructure** – Network security, physical security, and incident response services designed to strengthen defenses and improve incident containment and response.
- **Skills and Training** – Train security professionals in critical capability areas (Secure Coding, DevSecOps, Cloud Security, Offensive and Defensive Security) and technology stacks (Palo Alto Networks, Cisco, AWS, etc.).
- **Threat and Vulnerability** – Penetration testing, threat management, and vulnerability management services designed to find and remediate critical gaps in a customer's security defenses.

With $3.9B in security solutions annually, CDW is the largest security integrator in the United States.

CDW is the largest cybersecurity integrator in North America, with an expanding footprint across the globe of multinational and in-market customers. We leverage this capability set – supported by enabling technologies from our partners - to design cybersecurity risk management programs that address our customers' specific risk management goals.

Over recent years, CDW has executed its vision for creating a competitive cybersecurity practice, particularly as it relates to cybersecurity risk services. To that end, CDW made the acquisitions of Focal Point Data Risk and Sirius Computer Solutions in 2021. These acquisitions expanded the breadth and depth of services that CDW could offer its customers, creating new opportunities for CDW to introduce risk-based security services into markets and verticals where CDW has historically had a strong presence. In addition, these acquisitions became the building blocks for further innovation, driven through CDW's Security Research & Development and GSSO Global Security Strategy Office functions. Focal Point brought strong capabilities and coworkers focused on risk management, and Sirius brough a mature managed services capability that are currently being leveraged to drive forward the full-stack approach advocated in our vision.

CDW's scale and ability to support clients across the full range of their cyber needs gives us an advantage that we can bring to AEPA members. Automating elements of assess and delivery more frequently as a service with drive costs into a more affordable range for clients of any size. Importantly, helping clients assess what is reasonable and rationalized to address cyber risk can help break the cycle of event-driven spending and over-consumption of tools, relative to need. By aligning risk and security ops more closely, in conjunction with the push from regulators to place accountability on the board and senior leadership, CDW will help customers quickly assess their current risk posture and technology/process landscape and align a roadmap to that idea of what is reasonable.

CDW engages with clients on risk management programs across not only cybersecurity, but also as part of an organization's enterprise risk management process. Cybersecurity is deemed as mission critical for all types of organizations, and accordingly our service capabilities are designed to address risk management from both a top-down level, starting with those charged with governance (i.e., Board of Directors) and from a bottom-up approach where we may be engaged to assist with an acute issue

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW·G").

that is part of an overall risk management program (e.g., vulnerability scanning and patching). Our offerings are designed to be flexible to accommodate our client needs, recognizing factors such as industry, jurisdiction, and size will impact an organization's risk management needs.

Please see Attachment A: CDW Security Capabilities Brochure and uploaded collateral for more information.

Cyber Security and Training Solutions

CDW·G offers a comprehensive set of services designed to take a technical deep dive into an organization's security, with assessments that measure the strength of networks, applications, and endpoints. With our detailed deliverables, we can lead or assist organizations remediate high-priority gaps, and design stronger detection and incident response programs to mitigate the risk of compromise or data loss. Our services include:

- Assessments
- Network Security
- Endpoint Security
- Data Security
- Identify and Access Management
- Cloud Security
- Incident Response
- Training
- Compliance

Technology Training with CDW

CDW·G's IT and cybersecurity training aligns the needs of our customers' workforces with the goals of their technology projects, ensuring teams have the skills to support and optimize tech stacks long-term. We have the capability to provide high-value courses and programs relevant to the following requirements of the RFP:

- Technical Training
- Compliance Training
- Certification and Professional Development
- Simulation and Hands on Training

Please see Attachment B: CDW_WFD Catalog for more information.

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW·G").

CYBER SECURITY & TRAINING REQUREMENTS

CDW·G Response

In addition to providing world-class products and services with our partner vendors and OEMs, CDW·G also offers its own professional and managed services in many cyber and physical security areas, ensuring our customers are set up for success, no matter the project they are undertaking.

Referenced below are a few of CDW·G's core professional and managed services offerings; this is not an inclusive list, and many more are available to AEPA. We are proud to offer our expertise for these engagements while utilizing the discount rate/fee structure provided in our pricing documentation.

*The level of effort varies by engagement.

Item	Description	Comply
6.1.1	**Network Security** (e.g., Firewall Management, Intrusion Detection and Prevention, Virtual Private Network)	**Y**
6.1.2	**Endpoint Security** (e.g., Antivirus, Antimalware, Endpoint Detection and response, Mobile Device Management, Patch Management)	**Y**
6.1.3	**Application Security** (e.g., Web Application Firewall, Secure Coding Practices, Application Vulnerability Scanning, Software Composition Analysis)	**Y**
6.1.4	**Data Security** (e.g., Data Encryption, Data Loss Prevention, Backup and Recovery Solutions, Database Security)	**Y**
6.1.5	**Identity and Access Management** (e.g., Single Sign-On, Multi-Factor Authentication, Privileged Access Management, Identity Governance and Administration)	**Y**
6.1.6	**Threat Intelligence** (e.g., Threat Intelligence Platforms, Cyber Threat Analysis, Incident Response, Threat Hunting)	**Y**
6.1.7	**Penetration Testing**	**Y**
6.1.8	**Security Audits**	**Y**
6.1.9	**Security Operations Center** (e.g., SOC as a Service (SOCaaS), Security Information and Event Management (SIEM), Managed Detection and Response (MDR), Incident	**Y**
6.1.10	**Cloud Security** (e.g., Cloud Access Security Broker (CASB), loud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPP), Secure Cloud	**Y**
6.1.11	**Compliance and Risk Management** (e.g., Compliance Frameworks (e.g., GDPR, HIPAA, PCI-DSS), Risk Assessment and Management, Security Audits and Assessments, Policy Development and Management)	**Y**
6.1.12	**Physical Security** (e.g., Security of Physical Assets, Access Control Systems, Surveillance Systems, Environmental Controls)	**Y**
6.1.13	**Cyber Security Insurance**	**N**
6.1.14	**User Awareness** (e.g., Phishing Simulation and Training, General Cyber Security Awareness Programs, Role-Based Training (e.g., executives, developers), Social	**Y**
6.1.15	**Technical Training** (e.g. Advanced Persistent Threat (APT) Detection, Malware Analysis and Reverse Engineering, Network Security Monitoring, Incident Response	**Y**
6.1.16	**Compliance and Regulatory Training** (e.g. Data Protection Regulations, Industry-Specific Compliance Training, Legal and Ethical Aspects of Cyber Security, Governance, Risk, and Compliance (GRC) Training)	**Y**
6.1.17	**Certification and Professional Development** (e.g. Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA))	**Y**
6.1.18	**Simulation and Hands on Training** (e.g. Cyber Range Exercises, Red Team vs. Blue Team Exercises, Capture the Flag (CTF) Challenges, Real-World Scenario	**Y**

© CDW Government LLC 2024 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Association of Educational Purchasing Agencies are the Proprietary and Confidential property of CDW Government LLC ("CDW·G").

Security Solutions

We know that security goes deeper than software and applications. It touches every layer of AEPA member's network infrastructure and requires a holistic defense strategy that aligns people, processes and policies. Far from a single firewall or IPsec VPN that you can build and forget, true cybersecurity needs to be fortified with continuous testing, monitoring and review. With more than 20 years of experience, our experts can objectively assess your organization's cybersecurity practices and develop a plan and policies that both proactively mitigate risk and react to events such as data breaches and disasters.

Cybersecurity Is more than an IT concern, it's a business concern. Cybersecurity is a persistent effort and culture that needs to align people, processes and technology. It also needs to include regular cybersecurity assessments, testing, monitoring and a strategy for risk containment, remediation and response using the latest antivirus and firewall solutions.

CDW·G has more than 20 years of experience designing and implementing security solutions and in-depth defense strategies for a range of organizations spanning commercial, government, education and healthcare industries. Our security solutions services, which can be tailored to specific technical environments, include:

- Crisis Alert/Management
- Access Control
- Surveillance Equipment
- Perimeter Security/Protective Barriers

Our Knowledge Goes Deep



CDW is the #1 partner for many of the industry's top security vendors.

We hold elite and master certifications from such vendors as Cisco, Palo Alto, Fortinet, Crowdstrike, SentinelOne, Arctic Wolf, OKTA, Verkada, Genetec, Sailpoint, and Proofpoint, among others.



Our outstanding team works with businesses across the country.



We approach data security, mobile security and cloud security with unmatched depth.

Meet Our Security Experts

Our highly specialized teams can consult with you about weak spots in your network and will work with you to design a custom security solution to fit the needs of your organization.

Security Assessment Team

Dedicated solely to security engineering, this elite team of white-hat hackers performs assessments and penetration tests for vulnerabilities within your network. They use their findings to give vendor- and product-neutral advice to help you make informed decisions on risk management.

Security Delivery Engineers

These top-talent specialists will come and implement the right security strategy for your organization. They're equipped with the specific technical knowledge to make sure everything works together and will help you understand the full functionality of a security solution through training. This team performs complimentary malware assessments, providing you with the insights you need today to face tomorrow's security threats with confidence.

Data Loss Prevention Solution Architects

Our consultants work with you to understand the flow of your organization's sensitive data through your network infrastructure before helping you build a long-term data loss prevention security strategy.

Security Solution Architects

Our highly trained and technical solution architects will work with you to identify your unique challenges with network and data security, mobile security and cloud security. Then they'll recommend the right strategy that fits your organization's needs.

Certifications

We hold an array of industry- and partner-specific certifications that ensure the highest level of expertise.



Certified Information Systems Security Professional (CISSP)



GIAC Certified Incident Handler (GCIH)



GIAC Security Essentials (GSEC)



Expert Partner – Symantec Data Security Competency



Certified in Risk and Information Systems Control (CRISC)



Certified Ethical Hacker (CEH)



Cisco Certified Internetworking Expert – Security (CCIE Security)



Cisco Security Master

SECURITY SOLUTIONS REQUIREMENTS

CDW·G Response

In addition to providing world-class products and services with our partner vendors and OEMs, CDW·G also offers its own professional and managed services in many cyber and physical security areas, ensuring our customers are set up for success, no matter the project they are undertaking.

Referenced below are a few of CDW·G's core professional and managed services offerings; this is not an inclusive list, and many more are available to AEPA. We're proud to offer our expertise for these engagements while utilizing the discount rate/fee structure provided in our pricing documentation.

*The level of effort varies by engagement.

Item	Description	Comply
6.1.1	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. · Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. · Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. · Analysis is conducted to ensure effective response and support recovery activities. · Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies)	**Y**
6.1.2	Crisis Alert/Management For IP/networked based systems or solutions, the following features are desired: ● Multi-Channel Alert Delivery: The system should support multiple communication channels such as text messages, emails, voice calls, mobile app notifications, social media, and desktop alerts. ● Customizable Alert Templates ● Ability to integrate with previously purchased security system products or solutions ● Off site viewing capabilities (i.e., mobile device) ● Mobile or wireless panic button ● Door locking system controlled by the agency ● Mechanical, electronic wireless door locking ● Automated activation devices ● Analysis and management software solutions: Self-hosted and Software as a Service (Saas) based systems ● Mass Notifications/Emergency Communication Systems: to include intercoms, public address (PA) systems, mass notification software and emergency alert apps ● Integration with emergency services	**Y**

Item	Description	Comply
6.1.3	Access Control The following features are desired: ● Scalable ● Multi-factor authentication ● Centralized management ● Customizable access levels ● Audit trails and reporting ● Electronic locks and keyless entry systems ● Access control credentials (keycards or fobs) ● Role-based access control ● Eye lock iris biometrics ● Remote access control management ● Interoperability with security systems ● Intruder lock & exit devices for classrooms ● Master keying systems ● Panic & fire exit hardware ● Compliance with standards and regulations (FERPA, HIPAA)	**Y**
6.1.4	Surveillance Equipment For IP/networked systems or solutions, the following features are desired: ● On/off recording capabilities ● Sound integration and sound recording capabilities ● Ability to integrate with previously purchased security system products or solutions ● Offsite viewing capabilities (i.e., mobile device) ● Software solutions self-hosted and Software as a Service (SaaS) based systems ● Video service & monitoring/security camera system ● Compliance with Standards and Regulations (FERPA, HIPAA)	**Y**
6.1.5	Perimeter Security/Protective Barriers The following features are desired: • Ballistic & blast resistant doors & glass • Perimeter security • Protective barriers • Telemetry controls	**N**
6.1.6	All equipment, supplies, products, and all related accessories that can be purchased must be new and actively marketed products by the manufacturers and/or their authorized dealers.	**Y**
6.1.7	For time and materials-based services, a “not to exceed” project quote must be provided to the purchasing Member Agency for work approval before work begins.	**Y**

Our World-Class Technology Partnerships



Attachments

Attachment A: CDW Security Capabilities

Attachment B: CDW_WFD Catalog

Attachment A: CDW Security Capabilities

The security landscape is changing. Are you prepared?

Today's security professionals are caught in a balancing act between risk and reward. Each new technology has the potential for greater agility, scalability, and efficiency — but they also introduce risk into the IT environment. Organizations that learn to adopt and integrate these technologies without slowing innovation will be best positioned for success.

At CDW, we help you embrace and utilize these solutions. Our experienced teams listen to your needs, and design end-to-end solutions to help you deter, detect and manage the latest threats. Whether you need the latest technology, expert advice, or a strategic partner, CDW has the solution for you.

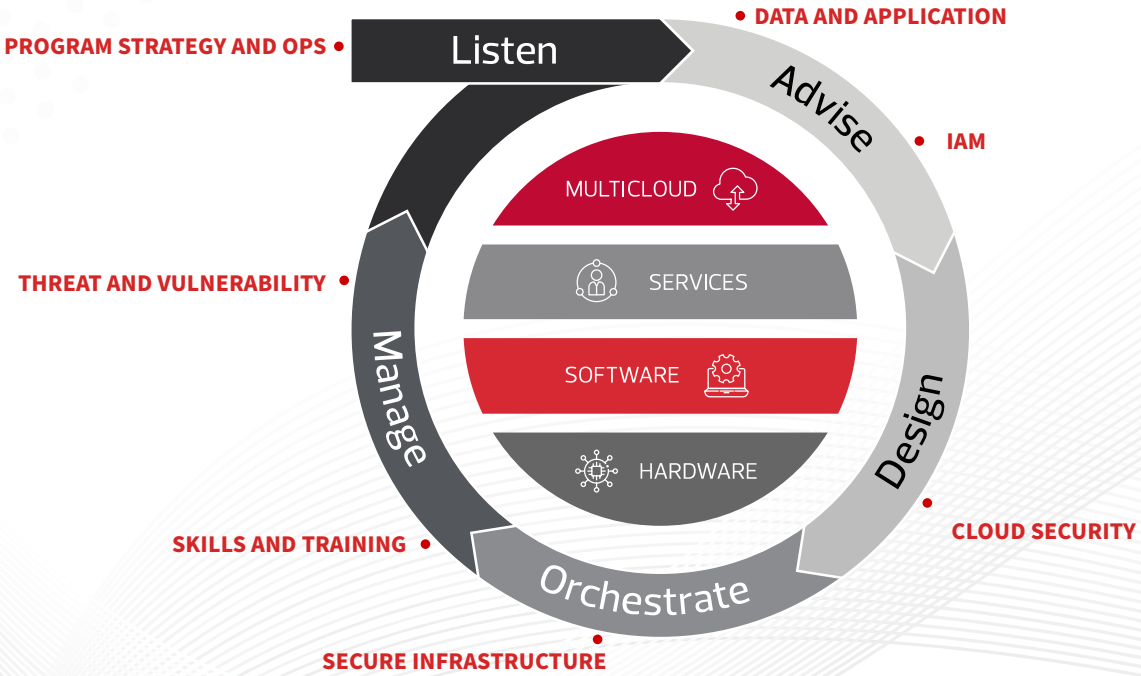


The CDW Approach

CDW has the expertise to help you manage security-related risk.

CDW makes security an enabler, not an obstacle. Our full-stack, full lifecycle approach allows us to leverage our breadth of services and solutions to identify the best solution for your needs.

CDW helps you mature and scale a security program that drives toward your business objectives without slowing down innovation.





Proven Service-Level Agreements (SLAs)
Industry-leading performance against SLAs means predictability, continuity, and agility.

End-to-End Service
Everything you need, from one vendor. Less risk, less paperwork, less hassle.

Unmatched Expertise
The broadest and deepest security skill sets in the market.

500+ security professionals

300+ managed services professionals

100+ IAM specialists

150+ vendor partnerships

40K+ security solutions delivered

15K+ industry-trained security professionals

Outcomes we are driving

CDW security solutions are aligned to your business outcomes, with products and services designed to drive innovation, increase value from your technology investments, improve agility, manage risk, and optimize the customer and employee experience.



Defending critical assets from ransomware and other threats: Securing customer data against ransomware.

Challenge: A ransomware attack locked out nearly 100% of the customer's systems

Solution: CDW teams contained the breach, rebuilt the data environment in the cloud, and got their sales team up and running

Outcome: Response and remediation complete in less than 36 hours



Growing through M&A without increasing cyber risk: Securing Active Directory after a merger.

Challenge: M&A activity created a host of security, risk, and operational issues stemming from disconnected Active Directory environments.

Solution: CDW performed an assessment to provide a clear picture of architecture, governance, and management processes for the directory, and evaluated the security posture against best practices. CDW then built out a full Active Directory integration plan.

Outcome: CDW delivered a migration and integration that solved several challenges, reduced security/access risk, and resulted in cost savings for the customer.



Enabling innovation with secure cloud and hybrid infrastructures: Securing the cloud in AWS, Azure, and Alibaba.

Challenge: A global manufacturer needed to secure their Alibaba QA and production environments in advance of a major IoT release. They needed to align standards across continents and cloud platforms without delaying the launch.

Solution: CDW led a rapid mobilization effort, utilizing security best practices the company was using in Azure and AWS and translated it into the Alibaba cloud environment.

Outcome: CDW delivered on a tight timeline, providing the customer with an environment they were comfortable with while also training their internal resources on how to secure an Alibaba cloud.



Designing and delivering full-stack Zero Trust solutions: Achieving Identity and Access Management (IAM) at scale in a distributed medical environment.

Challenge: The customer was concerned about its ability to manage, secure, and scale its large endpoint user community in a cost-effective manner.

Solution: CDW conducted an initial assessment, provided enterprise security guidance, and implemented IAM systems and integrated with over 2,600 endpoints.

Outcome: The customer was able to establish and implement an identity platform with proper governance that gave seamless and secure access to its thousands of end users.

The business strategy is the security strategy

Achieving your business goals requires a robust security strategy. being a cost center to an innovation engine.

CDW offers advisory services that help assess your security environment, determine the best strategy for moving forward and improve your organization's governance and compliance posture.

Solutions and Services:

- Strategy workshops
- SAP consulting
- Technology bake-offs
- Compliance consulting
- Governance, risk and compliance (GRC) technology
- Data governance planning
- Data protection planning
- Risk consulting
- Internal audit and IT audit services
- Technology proofs of concept (POCs)

Managed Services

- Solution optimization/tuning
- vCISO
- Audit/risk outsourcing

CDW's vCISO service helps you rapidly mature your security practices with embedded support from a seasoned security expert. Our vendor-neutral vCISOs are available for project- or time-based engagements to help you assess, define, and execute new security strategies.





Ensure your cyberdefenses can combat evolving threats

Are you prepared to protect your data in a changing security landscape? With cyberattacks growing in volume and complexity, and data and apps residing everywhere and being accessed from anywhere, it's time to adopt a zero-trust philosophy.

CDW provides a wide range of solutions to handle your data protection needs:

Solutions and Services:

- Application security
- Security intelligence and analytics
- DLP strategy and roadmaps
- Data protection programs
- Data discovery, handling, and classification
- Web app firewalls (WAF)

Managed Services

- Solution optimization/tuning
- Managed proxy

Key Considerations for Strengthening Cybersecurity Effectiveness

Do I have the visibility I need across my network? Can I identify what data I need to protect? Can I identify which people and devices are connecting to my network? Do I have insight into which devices they're using and which applications they're accessing? How regularly do I conduct threat assessments and red and blue team exercises?

How quickly can I detect, mitigate and recover from a cyberattack, if one occurs? For cyber-risk insurance purposes, have I evaluated the value of my data and what the impact would be if exfiltration occurred? How resilient is my environment? Do I have the proper tools in place to detect breaches and reduce time-to-response? How often do I test my backup/recovery systems? Do I have procedures in place to comply with SEC cybersecurity disclosure rules?

Overcome the authentication challenge

Cyberthreats related to identity and credential exploits are on the rise, with new challenges from AI-powered attackers, complex multicloud environments and increasing regulatory scrutiny. Many organizations lack proper credential and account access protections, leaving the door open for breaches.

Robust identity management involves a multilayered security strategy and approach, which CDW can provide through:

Solutions and Services:

- Rapid assessments and strategy
- IAM, IGA, and PAM implementation
- User rights and access reviews
- Solution selection and bake-offs
- SIEM deployment and configuration

Managed Services

- SIEM deployment and configuration
- Solution optimization/tuning
- IAM and PAM support services
- Managed authentication
- Managed identity programs
- Managed SIEM



Cyberthreats related to identity and credential exploits are on the rise, especially with the prevalence of remote and hybrid work. especially with the prevalence of remote and hybrid work. cybersecurity disclosure rules?

84% **of respondents experienced an identity-related breach in the past year.**

Source: Identity Defined Security Alliance. “2022 Trends in Securing Digital Identities.” www.idsalliance.org.

Adhere to best practices with Cloud Security Posture Management (CSPM) solutions

CDW's Cloud Security Posture Management (CSPM) solutions help organizations solve potential liabilities related to visibility, configuration, compliance and ongoing management of the cloud environment. This technology supports adherence to security best practices and regulatory requirements, facilitates inventory management, and provides log and alert capabilities. It essentially provides governance, risk management and compliance capabilities for cloud environments, and has four primary elements:

1 Configuration Management:
CSPM tools assess environments against target compliance or security rules and alert IT staff or automatically make the necessary fixes. Proactive identification and elimination of improper configuration is essential because it reduces cloud risks.

2 Threat Intelligence:
Threat intelligence encompasses data related to threats and vulnerabilities, as well as bad actors, exploits, malware and indicators of suspicious activity or compromised systems (making it a critical capability for the cloud).

3 Multicloud Support:
When multiple cloud services communicate with each other, the landscape becomes even more difficult to parse. CSPM restores control and oversight to cloud ecosystems that can quickly feel unmanageable if they are not subject to proper controls.

4 Continuous Compliance:
CSPM tools assess compliance against specific sets of rules and best practices. Equally important, organizations can choose to have CSPM tools automatically make corrections to maintain compliance, evenas circumstances shift either within the requirements or the cloud environment.

Manage your cloud security effectively

Today, cloud is about how software works together across boundaries to enable not only agility, but also choice of the best cloud for each workload. Regardless of whether you are operating a hybrid or multicloud environment, security should be the cornerstone of any cloud strategy.

CDW has the tools to help you assess vulnerabilities and ensure the right protocols are in place across your cloud platform.

Solutions and Services:

- Cloud security posture management
- Cloud security architecture
- Cloud access security broker
- Secure access service edge
- DevSecOps

Managed Services

- Solution optimization/tuning
- Managed cloud security



Secure your entire infrastructure – both on-prem and in the cloud

Both on-premises security and cloud-based security have their advantages. On-premises security options allow for greater control and uptime, while cloud-based security options allow for remote management, greater ROI, and enhanced scalability.

Regardless of whether your organization relies on cloud-based security, on-premises security, or a hybrid model, you need to make sure your entire infrastructure is secure. CDW can ensure you're covered:

Solutions and Services:

- Next-generation firewall
- Security architecture and design
- Endpoint protection
- Intrusion detection and prevention (IDS/IPS)
- Email and web security
- Network segmentation workshops
- IoT device assessment and strategy
- Physical security solutions

Managed Services

- Solution optimization/tuning
- Managed firewall
- Managed IDS/IPS



Driving continuity and reliability with managed security

With managed security services from CDW, our customers have dramatically reduced the impact of workforce, political, and supply chain disruptions on their businesses. Always-on support from CDW ensures that you can focus on running critical operations, growing your business, and achieving business outcomes without fear of system downtime, ticket surges, or other disruptions



Strengthen your security team with the latest skills and technologies

In today's evolving security landscape, it's imperative that your team has the skills and training to manage threats and leverage the latest technologies.

CDW provides training development and expertise to help your team meet today's challenges, while improving employee retention and job satisfaction.

Solutions and Services:

- Cyber Workforce Development
- Offensive & Defensive Security Courses
- Cloud Security Courses
- Programming and DevSecOps Courses
- Data Science & Analytics Courses
- Solution Training (AWS, Cisco, Palo Alto)

Managed Services

- Managed workforce development
- vCISO

Secure your organization

Improve employee retention

Reduce costs

Validate your team

CDW believes strongly in the concept of workforce development:
the process of defining, measuring, training, and validating your teams. From this process emerges a long-term strategy to ensure your team has the skills to protect and enable your business-critical functions. We take a programmatic approach to workforce development, providing practitioners with training programs designed to help them reach their career goals.

Strengthen defenses with technical assessments, remediation and response services

CDW offers a comprehensive set of services designed to take a technical deep dive into your security, with assessments that measure the strength of your networks, applications and endpoints. With our detailed deliverables, we can lead or assist as you remediate high-priority gaps, and design stronger detection and incident response programs to mitigate the risk of compromise or data loss.

Our services, which can be tailored to your technical environment, include:

Solutions and Services:

- Penetration testing
- Red and purple teaming
- Web app VA/testing
- Patch management
- Vulnerability management
- Endpoint detection and response (EDR)
- Incident response

Managed Services

- Managed vulnerability scanning
- Managed IR
- Managed SIEM
- Managed scanning
- Managed EDR



Considerations for Implementing Effective Incident Response Capabilities

Do I understand my business risk? Have I identified the types of assets and information that need to beprotected?
Have I secured an executive sponsor?
Has my organization developed a security strategy and communicated it effectively?
Do I have the right team assembled? Do they understand their responsibilities during an incident?
Do I have the right tools in place to ensure timely incident detection and response?
Have I developed a formal incident response plan?
Have I tested the efficacy of my current incident response plan and processes?

Credentials

CDW's Security teams blend training and certifications from industry organizations, vendors, and CDW proprietary methodologies. Sample certs:

Industry	Vendor
CISSP	**Cisco** CCNPs and CCIEs
CISA	**Splunk** Certified Consultants and Enterprise Architects
CIPP	**AWS** Cloud Security Architects
PCI QSA	**Microsoft** Certified Systems Engineers
CEH	**Palo Alto** Certified Network Security Professionals
PMP	**SailPoint** Certified Engineers and Architects
CSM	**Okta** Certified Professionals, Administrators, Architects
Juris Doctor	**CyberArk** Certified Delivery Engineers

Standards Bodies

CDW sponsors, supports, or aligns methodologies with the training and resources of the following standard-setting bodies:

NIST, PCI Security Standards Council, Identity Defined Security Alliance, iapp, NACD, ISACA, (ISC)², CSA cloud security alliance, The Institute of Internal Auditors



World-Class Technology Partnerships

With one of the largest technology partnership portfolios in the industry, CDW can support a full stack of security solutions.

Barracuda	Delinea	KnowBe4	Proofpoint	Tanium
Check Point	ExtraHop	Microsoft	SailPoint	Tenable
Cisco	F5	Mimecast	SentinelOne	Trellix
Cofense	Forcepoint	Netskope	SonicWall	Trend Micro
CrowdStrike	Fortinet	Okta	Sophos	VMware
CyberArk	IBM	Palo Alto Networks	Splunk	Zscaler

Discover how CDW's security capabilities can help your organization achieve its goals. Contact your account team, or give us a call at **800.800.4239**

Attachment B: CDW_WFD Catalog

Technology Skills and Training

2024 Course Catalog

Cyber Security and IT and Security Frameworks

cdw.com

Table of Contents

Category: Cyber Security 4

Administering Information Protection and Compliance in Microsoft 365 (SC-400T00) 5
Advanced Linux Kernel Internals 7
Android Attack and Defend 8
Assembly for Reverse Engineers 9
Attacking and Securing Java / JEE Web Applications 10
Automated Network Defense 12
Behavioral Malware Analysis 13
CAP: Certified Authorization Professional 14
CBROPS - Understanding Cisco Cybersecurity Operations Fundamentals 15
CCSP: Certified Cloud Security Professional 17
Certified CMMC Professional (CCP) 18
CISSP: Certified Information Systems Security Professional 19
CompTIA Advanced Security Practitioner (CASP+) 21
CompTIA Cyber Security Analyst (CySA+) 22
CompTIA PenTest+ 23
CompTIA Security+ 24
CSSLP: Certified Secure Software Lifecycle 25
Cyber Risk Management Overview 27
DevSecOps for Security Practitioners 28
EC Council Certified Ethical Hacker (CEH) 30
EC Council Certified Hacking Forensic Investigator (CHFI) 32
EC Council Certified Network Defender (CND) 34
EC-Council ICS SCADA Cybersecurity 35
Endpoint Live Forensics 36
Evasive Techniques and Breaching Defenses 37
Event Monitoring and Incident Detection 38
Exploring the OWASP Top 10 40
Hacker Methodologies for Security Professionals 42
HCISPP: HealthCare Information Security and Privacy Practitioner 43
Incident Analysis 44
Introduction to Security Analysis 46
iOS Attack and Defend 47

ISACA Certified Information Security Manager (CISM) 48
Linux Kernel Internals 49
Machine Learning Operations (MLOps) and AI Security 50
Malware Reverse Engineering 52
Microsoft Azure Security Technologies (AZ-500T00) 53
Microsoft Cybersecurity Architect (SC-100T00) 55
Microsoft Identity and Access Administrator (SC-300T00) 57
Microsoft Security Operations Analyst (SC-200T00) 59
Microsoft Security, Compliance, and Identity Fundamentals (SC-900T00) 61
Network Forensics and Investigation I 62
Network Forensics and Investigation II 64
OffSec PEN-200 - Penetration Testing with Kali Linux (OSCP) 65
Python for Reverse Engineers 66
SCOR - Implementing and Operating Cisco Security Core Technologies 67
Secure Web App Development Overview - Java / JEE 69
Securing Web Applications Overview 71
Security Engineering on AWS 73
SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention 74
SISE - Implementing and Configuring Cisco Identity Services Engine 76
SSCP: Systems Security Certified Practitioner 78
Threat Hunting with Python 79
Understanding Operating Systems 80

Category: IT and Security Frameworks 81

Application Security and Development (STIG) 82
Certified CMMC Professional (CCP) 84
CompTIA A+ 85
Database Security (STIG) 87
HCISPP: HealthCare Information Security and Privacy Practitioner 89
Information Assurance (STIG) Overview 90
ISACA Certified Information Security Manager (CISM) 92
ITIL Foundation 93

Category: Cyber Security

Administering Information Protection and Compliance in Microsoft 365 (SC-400T00)

MS-SC-400

View schedule and pricing on cdw.com

Summary

Learn how to protect information in your Microsoft 365 deployment. This course focuses on data lifecycle management and information protection and compliance within your organization.

WHO SHOULD ATTEND:

- Information Protections Administrators
- Roles responsible for implementing and managing solutions for content classification, data loss prevention (DLP), information protection, data lifecycle management, records management, privacy, risk, and compliance.

LENGTH: 4 Days

Description

Learn how to protect information in your Microsoft 365 deployment. This course focuses on data lifecycle management and information protection and compliance within your organization. The course covers implementation of data loss prevention policies, sensitive information types, sensitivity labels, data retention policies, Microsoft Purview Message Encryption, audit, eDiscovery, and insider risk among other related topics. The course helps learners prepare for the Microsoft Information Protection Administrator exam (SC-400).

Learning Objectives

- Introduction to information protection and data lifecycle management in Microsoft Purview
- Classify data for protection and governance
- Create and manage sensitive information types
- Understand Microsoft 365 encryption
- Deploy Microsoft Purview Message Encryption
- Protect information in Microsoft Purview
- Apply and manage sensitivity labels
- Prevent data loss in Microsoft Purview
- Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform
- Manage data loss prevention policies and reports in Microsoft 365
- Manage the data lifecycle in Microsoft Purview
- Manage data retention in Microsoft 365 workloads
- Manage records in Microsoft Purview
- Explore compliance in Microsoft 365
- Search for content in the Microsoft Purview compliance portal
- Manage Microsoft Purview eDiscovery (Standard)
- Manage Microsoft Purview eDiscovery (Premium)
- Manage Microsoft Purview Audit (Standard)
- Prepare Microsoft Purview Communication Compliance
- Manage insider risk in Microsoft Purview
- Implement Microsoft Purview Information Barriers
- Manage regulatory and privacy requirements with Microsoft Priva
- Implement privileged access management
- Manage Customer Lockbox

Prerequisites

- Foundational knowledge of Microsoft security and compliance technologies.
- Basic knowledge of information protection concepts.
- Understanding of cloud computing concepts.
- Understanding of Microsoft 365 products and services.

Advanced Linux Kernel Internals

OS-600

View schedule and pricing on cdw.com

Summary

Advanced Linux Kernel Internels focuses on the skills of developing and detecting techniques used by Linux kernel mode rootkits at every stage of their execution.

WHO SHOULD ATTEND:

- Offensive and defensive security professionals including security researchers, digital forensic analysts, red-teamers and blue-teamers and anyone who wants to learn about the modern Linux kernel.

LENGTH: 5 Days

Description

Advanced Linux Kernel Internals provides comprehensive coverage of the key functional areas of Linux kernel rootkits through a practical hands-on approach. Dive into techniques used by malicious kernel mode software to abuse Linux kernel subsystems and their programming interfaces to achieve their goals. This course also covers the security functionality and mitigations in the latest Linux kernel.

Learning Objectives

- Identify kernel components and programming interfaces used to compromise a system.
- Develop shellcode that executes in the kernel.
- Develop linux kernel modules that provide offensive security functionality.
- Implement key components of a kernel rootkit.
- Recognize security related enhancements in the modern Linux kernel.
- Analyze a Linux system to find and identify malicious activity.
- Configure a Linux system to improve the system's security posture.

Prerequisites

- Proficient in C programming language.
- Comfortable with Linux command line tools.
- Familiar with Linux development tools such as gcc and make.
- Familiar with gdb commands.
- Knowledgeable of data structures such as pointers, structures, arrays and linked lists.
- Knowledgeable of Linux kernel internals, kernel module development and debugging.

Android Attack and Defend

CT-400

View schedule and pricing on cdw.com

Summary

Android™ Attack and Defend provides an instructor-led, hands-on course in the fundamentals of software development for this ubiquitous operating system from Google. This course is a laboratory intensive programming course designed for students looking to gain a working knowledge in Android development. Through a combination of instructor-led examples and a series of programming assignments and challenges, students will build and enhance their practical knowledge of software development in the Android operating system. Additionally, students will also deploy, execute, and test all developed programs on Android emulation software and Android hardware devices provided in the class.

Description

None

Learning Objectives

- Android Architecture and Design
- Android SDK (Software Development Kit) and Android APK development
- The Stack
- Lists and Adapters, Broadcast Receivers, Content Providers and System Services
- Reverse Engineering Android Applications
- Hacking Android Devices

Prerequisites

- Experience with Android products such as Android phones and tablets is recommended
- Programming experience in C, Python, Perl or Java is highly recommended

Assembly for Reverse Engineers

RE-300

View schedule and pricing on cdw.com

Summary

This course will equip you with the know-how to effectively read Assembly, review statements, and reverse machine code back to its higher-level equivalent.

LENGTH: 5 Days

Description

Many analysts and programmers have not yet learned assembly language - a skill that will save them precious time when effective analysis is needed most. Designed for malware analysts and code developers alike, Assembly for Reverse Engineers will equip you with the know-how to effectively read Assembly, review statements, and reverse machine code back to its higher-level equivalent. Learn and practice development techniques to improve the speed and quality of static analysis during this week-long, lab-intensive course.

Learning Objectives

- Describe how code execution works
- Understand the components of the x86 instruction set
- Apply demonstrated analysis techniques to the reverse engineering of Windows executables
- Use IDA Pro's powerful assembly markup features to optimize analysis
- Use static and dynamic analysis to interpret and document program flow

Prerequisites

- Experience with C programming in a Windows environment
- Successful completion of Understanding Operating Systems course (or equivalent knowledge)

Attacking and Securing Java / JEE Web Applications

SC-300

View schedule and pricing on cdw.com

Summary

This is a lab-intensive, intermediate-level, hands-on Java / JEE security training course that provides a unique coverage of Java application security. In this with the course begins with:

WHO SHOULD ATTEND:

- Experienced Java Web Developers
- Software Engineers and Architects
- Security Analysts
- Security Engineers
- DevOps Teams

LENGTH: 4 Days

Description

Discover the cutting-edge of cybersecurity and elevate your skills as a Java Web developer with our comprehensive Bug Hunting and Application Security course. Designed specifically for experienced Java web developers, our Java Secure Coding Camp | Attacking and Securing Java Web Applications is an immersive, hands-on training program that delves deep into the world of bug hunting, ethical hacking, and web application security. Through real-world case studies, engaging labs, and expert instruction, you'll gain the knowledge and skills needed to fortify your applications, stay ahead of emerging threats, and protect your organization from costly security breaches.

Upon completing this course, you will not only acquire a profound understanding of application security concepts and best practices but also enhance your problem-solving, debugging, and overall software development prowess. Empowered with these new skills, you'll be well-prepared to identify, address, and prevent security threats in your Java Web applications, ensuring a robust and secure digital environment for your organization.

Learning Objectives

- Master the fundamentals of secure coding and understand the stages of an exploit, focusing on defensive techniques.
- Establish foundational axioms for analyzing and addressing security in web applications, guiding your approach through this course and future endeavors.
- Learn responsible ethical hacking methods, including defect detection, bug reporting, and ensuring all activities are executed in a safe environment.
- Recognize and sidestep frequent pitfalls in vulnerability testing and bug hunting, leveraging best practices.
- Gain insight into the significance of multilayered defense strategies, evaluating the effectiveness of layered defenses through hands-on testing.
- Identify and handle untrusted data sources, understanding the associated risks like denial of service, cross-site scripting, and injections.
- Dive deep into authentication and authorization, pinpointing vulnerabilities and learning how to fortify these crucial security areas.
- Understand and counteract web-specific threats such as Cross-Site Scripting (XSS) and Injection attacks, mastering both offensive and defensive techniques.
- Examine risk factors in XML processing, file and software uploads, and deserialization, along with strategies for risk mitigation.
- Get acquainted with key security tools, from code scanners to web application firewalls, while also exploring server and infrastructure hardening techniques.

Prerequisites

- Familiarity with Java and JEE is required, and real-world programming experience is highly recommended.
- Ideally, students should have approximately six months to a year of Java and JEE working knowledge.

Automated Network Defense

CT-302

View schedule and pricing on cdw.com

Summary

Taught by experts in network defense, this course equips you with the skills to build and maintain Intrusion Detection/Prevention Systems (IDS/IPS) and utilize advanced signature-writing techniques to defend large-scale network infrastructures.

WHO SHOULD ATTEND:

- Incident Responders who need to understand and react to IDS alerts
- Network Defenders seeking to automate threat detection
- IDS administrators who wish to improve their signature writing skills
- Security Operations Center Staff seeking to automate traffic analysis
- Penetration Testers looking to reduce their network visibility

LENGTH: 5 Days

Description

An Intrusion Detection/Prevention System (IDS/IPS) can automate the process of identifying attacks among the thousands of connections on a network. Taught by leaders in network defense who work in the cybersecurity industry, this course demonstrates how to defend large-scale network infrastructures by building and maintaining IDS/IPS and mastering advanced signature-writing techniques. With IDS and trained network security auditors, organizations have a reliable means to prioritize and isolate the most critical threats in real time.

Learning Objectives

- Recognize the benefits and limitations of different intrusion detection system types (network- and host-based, and distributed systems)
- Identify optimal sensor placement and gaps in coverage
- Write basic IDS signatures to identify traffic of interest and tune them to reduce false positives
- Use reassembly and pre-processing engines to automatically reconstruct streams of network data prior to analysis
- Apply decoding and other techniques to overcome IDS evasion efforts
- Develop complex signatures employing rule chaining, event filtering and post-detection analysis to identify distributed attacks, multi-stage events, and other more complex threats
- Use regular expressions to effectively detect variable or morphing attacks
- Manage rule sets to reduce redundancy and maintain system efficiency

Prerequisites

- A strong understanding of TCP/IP networking
- Network Forensics and Investigation I and II

Related Courses:

- Network Forensics and Investigation I
- Network Forensics and Investigation II

Behavioral Malware Analysis

MA-300

View schedule and pricing on cdw.com

Summary

This course teaches you the fundamental skills necessary to analyze malicious software from a behavioral perspective.

LENGTH: 5 Days

Description

Behavioral Malware Analysis teaches you the fundamental skills necessary to analyze malicious software from a behavioral perspective. From simple key loggers to massive botnets, this class covers a wide variety of current threats. Using system monitoring tools and analytic software, you will analyze real-world malware samples in a training environment, giving you hands-on experience building secure lab environments, classifying malware, analyzing behavioral characteristics and their effects to systems, and documenting your findings. You will leave the course with the skills and abilities required to be an effective malware analyst.

Learning Objectives

- Set up a secure lab environment in which to analyze malicious software
- Build and maintain a tool set of freely available, trusted tools
- Classify different types of malware and describe their capabilities
- Analyze malware samples of varying types to ascertain their specific behavioral characteristics and their impact on a system
- Determine if a given sample is persistent and, if so, identify and remediate the persistence mechanism(s)
- Identify when a sample is aware of its virtual environment and will require more advanced static or dynamic analysis

Prerequisites

This is an introductory course in malware analysis. It is for security practitioners who already have a firm understanding of the internals of desktop operating systems and a general understanding of common threats to computer systems.

Required Knowledge & Experience:

- A firm understanding of the purpose and function of major components in a desktop operating system – processes, services, memory, APIs, file systems, Windows Registry.
- CompTIA Security+ and/or a high-level understanding of the common forms of malware (such as ransomware), and the dangers they each present.

Recommended:

- End-user experience with virtualized operating systems (VMware, VirtualBox, etc.)
- Windows host command-line administration
- Familiarity with the Sysinternals tool suite

Optional:

- Prior incident handling/response experience
- Administrative experience with virtual machines

CAP: Certified Authorization Professional

ISC-202

View schedule and pricing on cdw.com

Summary

This official ISC2 course provides students with in-depth coverage on the skills and concepts in the 7 domains including RMF, Security Categorization, Security Controls implementation, assessment, monitoring, and authorization.

WHO SHOULD ATTEND:

- IT Professionals interested in learning more about lifecycle cybersecurity risk management
- Auditors
- Infosec/Information Assurance Practitioners
- Program Managers.

LENGTH: 5 Days

Description

The Risk Management Framework (RMF) is used by security professionals who are responsible for assessing risk and establishing documentation for their IT systems. The Certified Authorization Professional (CAP) certification covers the RMF in great detail and is the only security certification under the DoD8570 Mandate that aligns to each of the RMF steps. This official ISC2 course provides students with in-depth coverage on the skills and concepts in the 7 domains including RMF, Security Categorization, Security Controls implementation, assessment, monitoring, and authorization. This course is for IT Professionals interested in learning more about lifecycle cybersecurity risk management, as well as auditors, infosec/information assurance practitioners and program managers.

Learning Objectives

- Distinguish the differences between the Risk Management Framework (RMF) steps and how the RMF process relates to the organizational structure.
- Examine the relationship between the RMF and System Development Life Cycle (SDLC).
- Assess legal, regulatory, and other security requirements.
- Utilize the system through categorization, descriptions including security authorization boundaries and registration.
- Create a documented plan for (inheritable) controls and security controls highlighting their effectiveness.
- Develop security control monitoring strategy.
- Develop a security assessment report (SAR) and provide a review interim SAR and initial remediation actions with a final SAR and optional addendum.
- Develop plan of action and milestones (POAM) (e.g., resources, schedule, requirements).
- Assemble security authorization package and obtain security authorization decision.
- Determine risk and acceptability.
- Determine security impact of changes to system and environment.
- Perform ongoing security control assessments (e.g., continuous monitoring, internal and external assessments) and remediation actions (resulting from incidents, vulnerability scans, audits, vendor updates, etc.).
- Perform periodic security status reporting, ongoing risk determination and acceptance.

Prerequisites

- A minimum of 2 years full-time experience in one or more of the 7 domains covered in the CAP exam.

CBROPS - Understanding Cisco Cybersecurity Operations Fundamentals

CBROPS

View schedule and pricing on cdw.com

Summary

Understanding Cisco Cybersecurity Operations Fundamentals teaches security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This course prepares learners for the Cisco Certified CyberOps Associate certification and the role of a Junior or Entry-level cybersecurity operations analyst in a SOC.

WHO SHOULD ATTEND:

- Individuals seeking a role as an associate-level cybersecurity analyst
- IT professionals desiring knowledge in Cybersecurity operations
- Those in pursuit of the Cisco Certified CyberOps Associate certification

LENGTH: 5 Days

Description

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course teaches you security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This course teaches you how to monitor alerts and breaches, and how to understand and follow established procedures for response to alerts converted to incidents. Through a combination of lecture, hands-on labs, and self-study, you will learn the essential skills, concepts, and technologies to be a contributing member of a cybersecurity operations center (SOC) including understanding the IT infrastructure, operations, and vulnerabilities. This course helps you prepare for the Cisco Certified CyberOps Associate certification and the role of a Junior or Entry-level cybersecurity operations analyst in a SOC.

Learning Objectives

- Explain how a Security Operations Center (SOC) operates and describe the different types of services that are performed from a Tier 1 SOC analyst's perspective.
- Explain Network Security Monitoring (NSM) tools that are available to the network security analyst.
- Explain the data that is available to the network security analyst.
- Describe the basic concepts and uses of cryptography.
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.
- Understand common endpoint security technologies.
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors.
- Identify resources for hunting cyber threats.
- Explain the need for event data normalization and event correlation.
- Identify the common attack vectors.
- Identify malicious activities.
- Identify patterns of suspicious behaviors.
- Conduct security incident investigations.
- Explain the use of a typical playbook in the SOC.
- Explain the use of SOC metrics to measure the effectiveness of the SOC.
- Explain the use of a workflow management system and automation to improve the effectiveness of the SOC.
- Describe a typical incident response plan and the functions of a typical Computer Security Incident Response Team (CSIRT).

- Explain the use of Vocabulary for Event Recording and Incident Sharing (VERIS) to document security incidents in a standard format.

Prerequisites

- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with the basics of networking security concepts

The following Cisco course can help you gain the knowledge you need to prepare for this course:

- Implementing and Administering Cisco Solutions (CCNA)

CCSP: Certified Cloud Security Professional

ISC-201

View schedule and pricing on cdw.com

Summary

The Certified Cloud Security Professional (CCSP) Boot Camp is a comprehensive training designed to build your skills around securing cloud-based environments.

Who Should Attend: IT and information security leaders, including those in the following positions:

- Cloud Architect
- Cloud Engineer
- Cloud Consultant
- Cloud Administrator
- Cloud Security Analyst
- Cloud Specialist
- Auditor of Cloud Computing Services
- Professional Cloud Developer

Length: 5 Days

Description

The Certified Cloud Security Professional (CCSP) Boot Camp is a comprehensive training designed to build your skills around securing cloud-based environments. In this course, you will learn about cloud architecture and design requirements, operational and compliance issues, and the security of cloud data, applications, and infrastructure. You will leave the boot camp fully prepared to earn your CCSP certification, one of the most in-demand certifications focused on cloud security.

Learning Objectives

- Identify architectural concepts and design requirements.
- Determine cloud data concepts and data classification.
- Comprehend cloud platform and infrastructure security and cloud application security operations elements
- Describe mitigated risks in cloud computing systems in federated identity and access management solutions.
- Assess the security-related mandates, information security requirements and relevant privacy legislation.
- Use the controls to ensure secure implementation of cloud services.
- Explain the six domains of the Certified Cloud Security Professional (CCSP) life cycle.

Prerequisites

- Minimum of five years cumulative paid work experience in information technology, of which three years must be in information security and one year in one or more of the six domains of the CCSP CBK.
- A candidate who doesn’t have the required experience to become a CCSP may become an Associate of ISC2’s by successfully passing the CCSP examination. The Associate of ISC2 will then have six years to earn the five years required experience.
- Part-time work and internships may also count towards your experience.

Certified CMMC Professional (CCP)

CS-200

View schedule and pricing on cdw.com

Summary

The Cybersecurity Maturity Model Certification (CMMC), managed by The Cyber AB (formerly known as the CMMC Accreditation Body or the CMMC-AB), is a program through which an organization's cybersecurity program maturity is measured by their initial and ongoing compliance with applicable cybersecurity practices, as well as their integration of corresponding policies and plans into their overall business operations.

Who Should Attend:

- This course is a prerequisite for the Certified CMMC Professional program, and it prepares students for the Certified CMMC Professional (CCP) certification exam. Students might consider taking this course to learn how to perform CMMC certification readiness checks within their own organization, or as a consultant to other Organizations Seeking Certification (OSC). The CCP certification is also a required step toward becoming a Certified CMMC Assessor (CCA), so students might take this course to begin down the path toward CCA certification.

Length: 5 Days

Description

This course prepares students for the Certified CMMC Professional (CCP) certification, which authorizes the holder to use The Cyber AB Certified CMMC Professional logo, to participate as an Assessment Team Member under the supervision of a Lead Assessor, and to be listed in the CMMC Marketplace. The CCP certification is also prerequisite for the Certified CMMC Assessor (CCA) certification.

Learning Objectives

- Identify the threats to the Defense Supply Chain and the established regulations and standards for managing the risk.
- Identify the sensitive information that needs to be protected within the Defense Supply Chain and how to manage it.
- Describe how the CMMC Model ensures compliance with federal acquisitions regulations.
- Identify responsibilities of the Certified CMMC Professional, including appropriate ethical behavior.
- Establish the Certification and Assessment scope boundaries for evaluating the systems that protect regulated information.
- Prepare the OSC for an Assessment by evaluating readiness.
- Use the CMMC Assessment Guides to determine and assess the Evidence for practices.
- Implement and evaluate practices required to meet CMMC Level 1.
- Identify the practices required to meet CMMC Level 2.
- As a CCP, work through the CMMC Assessment process.

Prerequisites

- Some foundational education or experience in cybersecurity.
- College degree in a cyber or information technical field with 2+ years of experience; or 2+ years of equivalent experience (including military) in a cyber, information technology, or assessment field.

CISSP: Certified Information Systems Security Professional

ISC-200

View schedule and pricing on cdw.com

Summary

This course covers the eight domains of the official CISSP CBK (Common Body of Knowledge). Students will gain knowledge in information security that will increase their ability to successfully implement and manage security programs in any organization or government entity.

WHO SHOULD ATTEND:

- Anyone whose position requires CISSP certification
- Individuals who want to advance within their current computer security careers or migrate to a related career.

LENGTH: 5 Days

Description

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization. The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of information security.

Learning Objectives

- Apply concepts of confidentiality, integrity, availability, and security governance principles and compliance.
- Align overall organizational operational goals with security functions and implementation.
- Determine how to protect assets of the organization as they go through their lifecycle.
- Leverage the concepts, principles, structures, and standards used to design, implement, monitor and secure operating systems, equipment, networks, applications etc.
- Apply security design principles to select appropriate mitigations for vulnerabilities present in common information system types and architecture.
- Explain the importance of cryptography and the security services it can provide in today's digital and information age.
- Evaluate the physical security elements relative to information system needs.
- Evaluate the elements that comprise communication and network security relative to information security needs.
- Leverage the concepts and architecture that define the associated technology and implementation systems and protocols.
- Determine appropriate access control models to meet business security requirements.
- Apply physical and logical access controls models to meet information security needs.
- Differentiate between primary methods for designing and validating test and audit strategies that support information security requirements.
- Apply appropriate security controls and countermeasures to optimize an organization's operation function and capacity. •Assess information systems risks to an organization's operational endeavors.
- Determine appropriate controls to mitigate specific threats and vulnerabilities.
- Apply information systems security concepts to mitigate the risk of software and systems vulnerabilities through the systems' lifecycles.

Prerequisites

- CISSP candidates must meet specific requirements, as established by (ISC)2 — see: https://www.isc2.org/cissp/default.aspx
- Those without the required experience can take the exam to become an Associate of (ISC)² while working toward the experience needed for full certification.
- CISSPs are required by (ISC)2 to earn 120 Continuing Professional Education (CPE) credits every three years.

CompTIA Advanced Security Practitioner (CASP+)

TIA-300

View schedule and pricing on cdw.com

Summary

CASP+ is an advanced-level cybersecurity certification covering technical skills in security architecture and senior security engineering in traditional, cloud, and hybrid environments, governance, risk, and compliance skills, assessing an enterprise's cybersecurity readiness, and leading technical teams to implement enterprise-wide cybersecurity solutions. An exam voucher is included in this course.

WHO SHOULD ATTEND

- Security architects
- Security engineers
- Advanced cybersecurity practitioners

LENGTH: 5 Days

Description

Information security threats are on the rise globally. Organizations are increasingly concerned over the lack of adequately trained senior IT security staff's ability to effectively lead and manage the overall cybersecurity resiliency against the next attack. The CASP+ certification qualifies advanced skills required of security architects and senior security engineers to effectively design, implement, and manage cybersecurity solutions on complex enterprise networks.

The Official CompTIA CASP+ course teaches the knowledge and skills to understand security architecture, security operations, security engineering and cryptography, governance, risk and compliance, and prepare candidates to take the CompTIA CASP+ certification exam.

Learning Objectives

- Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise
- Use monitoring, detection, incident response, and automation to proactively support ongoing security operations in an enterprise environment
- Apply security practices to cloud, on-premises, endpoint, and mobile infrastructure, while considering cryptographic technologies and techniques
- Consider the impact of governance, risk, and compliance requirements throughout the enterprise

Prerequisites

Foundational knowledge of informaton security, including:

- Knowledge of identity and access management (IAM) concepts and common implementations, such as authentication factors and directory services.
- Knowledge of cryptographic concepts and common implementations, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) and public key infrastructure (PKI).
- Knowledge of computer networking concepts and implementations, such as the TCP/IP model and configuration of routers and switches.
- Knowledge of common security technologies used to safeguard the enterprise, such as anti-malware solutions, firewalls, and VPNs.

CompTIA Cyber Security Analyst (CySA+)

TIA-301

View schedule and pricing on cdw.com

Summary

CompTIA Cybersecurity Analyst (CySA+) is a certification for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring. The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. An exam voucher is included with this course.

WHO SHOULD ATTEND

- Security Analysts
- Security Operations Center (SOC) Analysts
- Vulnerability Management Analysts
- Security Engineers
- Threat Hunters

LENGTH: 5 Days

Description

CompTIA Cybersecurity Analyst (CySA+) is a certification for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring. The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur.

The CompTIA Cybersecurity Analyst (CySA+) certification verifies that successful candidates have the knowledge and skills required to detect and analyze indicators of malicious activity, understand threat intelligence and threat management, respond to attacks and vulnerabilities, perform incident response, and report and communicate related activity.

Learning Objectives

- Improve processes in security operations
- Differentiate between threat intelligence and threat hunting concepts
- Identify and analyze malicious activity using the appropriate tools and techniques
- Implement and analyze vulnerability assessments, prioritize vulnerabilities, and make recommendations
- Apply updated concepts of attack methodology frameworks
- Perform incident response activities
- Understand the incident management lifecycle
- Apply communication best practices in vulnerability management and incident response

Prerequisites

- Minimum of 4 years of hands-on experience as an incident response analyst or security operations center (SOC) analyst, or equivalent experience.

CompTIA PenTest+

TIA-302

View schedule and pricing on cdw.com

Summary

This course introduces general concepts and methodologies related to pen testing. PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks. The CompTIA PenTest+ Certification Study Guide will prepare you to take the CompTIA PenTest+ exam. An exam voucher is included.

WHO SHOULD ATTEND

- Security Analysts
- Penetration Testers
- Vulnerability Testers
- Network Security Operations

LENGTH: 5 Days

Description

Global cybercrime costs are expected to grow 15% over the next five years. Now more than ever, it is imperative that organizations prevent sensitive data from falling into the wrong hands. Updates to PenTest+ reflect newer pen testing techniques for the latest attack surfaces, including the cloud, hybrid environments, and web applications, as well as more ethical hacking concepts, vulnerability scanning and code analysis.

PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks.

Learning Objectives

- Plan and scope penetration tests.
- Conduct passive and active reconnaissance.
- Perform non-technical tests to gather information.
- Analyze vulnerabilities.
- Penetrate networks.
- Exploit host-based vulnerabilities.
- Test applications.
- Complete post-exploit tasks.
- Analyze and report pen test results.

Prerequisites

- Minimum of 3-4 years of hands-on information security or related experience.
- Recommended experience in Network+, Security+ or equivalent knowledge.

CompTIA Security+

TIA-201

View schedule and pricing on cdw.com

Summary

CompTIA Security+ teaches the knowledge and skills to understand and assess the security posture of an enterprise environment and to recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents, and prepare candidates to take the CompTIA Security+ certification exam. An exam voucher is included with this course.

WHO SHOULD ATTEND:

- Security Specialists
- Security Administrators
- Systems Administrator Help Desk Analysts
- Security Analysts
- Security Engineers

LENGTH: 5 Days

Description

The Official CompTIA Security+ Instructor and Student Guides teach the knowledge and skills to understand to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents, and prepare candidates to take the CompTIA Security+ certification exam.

Learning Objectives

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, and Internet of Things (IoT).
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

Prerequisites

- CompTIA Network+
- 2 years of experience working in a security/systems administrator job role.

CSSLP: Certified Secure Software Lifecycle

ISC-203

View schedule and pricing on cdw.com

Summary

Earning the globally recognized CSSLP secure software development certification is a proven way to build your career and better incorporate security practices into each phase of the software development lifecycle (SDLC).

CSSLP certification recognizes leading application security skills. It shows employers and peers you have the advanced technical skills and knowledge necessary for authentication, authorization and auditing throughout the SDLC using best practices, policies and procedures established by the cybersecurity experts at ISC2.

WHO SHOULD ATTEND:

- Software development and security professionals responsible for applying best practices to each phase of the SDLC – from software design and implementation to testing and deployment.

LENGTH: 5 Days

Description

Offered as a private class only.

The (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) training provides a comprehensive review of the knowledge required to incorporate security practices –authentication, authorization, and auditing –into each phase of the Software Development Lifecycle (SDLC), from software design and implementation to testing and deployment. This training course will help students review and refresh their knowledge and identify areas they need to study for the CSSLP exam. Content aligns with and comprehensively covers the eight domains of the (ISC)² CSSLP Common Body of Knowledge (CBK®).

Learning Objectives

- Understand the core concepts of software security and the foundational principles that drive construction of resilient software.
- Recognize the importance of security requirements and understand the techniques for elicitation and specification of software security requirements.
- Recognize privacy requirements and their impact on the selection of safeguards and countermeasures.
- Understand threat modeling, attack surface evaluation, and architectural risk assessment. Recognize secure design principles and patterns.
- Understand secure coding practices, common application vulnerabilities and their mitigation strategies.
- Understand various code analysis techniques using automated and manual techniques.
- Recognize risks of third-party software components and libraries, malicious code and mitigation strategies.
- Describe security testing strategy and techniques and identify functional and non-functional testing methods.
- Describe defect tracking and risk scoring methods. Identify secure software methodologies, standards and frameworks.
- Understand Governance, Risk, and Compliance and recognize regulations and compliance requirements.
- Describe risks during deployment and understand security relevant issues during the operations and maintenance phase of the lifecycle.
- Understand vulnerability management, security monitoring, incident response, and root cause analysis. Recognize software supply chain risks and attacks.

Prerequisites

- At least four years of cumulative, paid work experience as software development lifecycle professional in one or more of the eight domains of the (ISC)2 CSSLP CBK

Cyber Risk Management Overview

CS-100

View schedule and pricing on cdw.com

Summary

This one-day, seminar-style course covers the cyber fundamentals you need to operate your business securely, embrace disruption safely, and effectively communicate cyber risks within your organization.

LENGTH: 1 Day

Description

All organizations face cyber risk in today's world. This seminar-style program covers the fundamentals professionals need to operate their organizations securely, embrace disruption safely, and communicate cyber risks effectively within their organizations. Designed with professionals in mind, this program dissects the most important issues in cyber risk management and arms attendees with the tools needed to engage in strategic cyber risk conversations.

Learning Objectives

- Express the importance of a sound cyber security strategy in attaining the organization's business goals
- Recognize areas of vulnerability within the organization and the threats that seek to exploit them
- Identify the cyber risks to the organization and the practices that will mitigate and eliminate them
- Practice effective personal cyber hygiene

Prerequisites

- This course is intended for executive-level business leaders (e.g., CEO, CFO, VPs).

DevSecOps for Security Practitioners

DO-300

View schedule and pricing on cdw.com

Summary

DevSecOps for Security Practitioners is designed to provide the skills needed to help build security automation framework to scan for vulnerabilities without human intervention, and focuses on how to adopt security automation techniques to continuously improve entire software development and security testing, learning about and working with open-source tools and techniques to integrate security testing tools directly into your CI/CD framework.

WHO SHOULD ATTEND:

- Anyone with intermediate IT skills

LENGTH: 4 Days

Description

Offered as a private class only.

Security automation is the automatic handling of software security assessments tasks. DevSecOps for Security Practitioners is a comprehensive hands-on course designed to provide you with the skills needed to help you build your security automation framework to scan for vulnerabilities without human intervention. This course will teach you to adopt security automation techniques to continuously improve your entire software development and security testing, learning about and working with open source tools and techniques to integrate security testing tools directly into your CI/CD framework.

Throughout this course, you will see how to implement security inspection at every layer, such as secure code inspection, fuzz testing, Rest API, privacy, infrastructure security, and web UI testing. With the help of practical examples, this course will teach you to implement the combination of automation and Security in DevOps. You will learn about the integration of security testing results for an overall security status for projects. By the end of this course, you will be confident implementing automation security in all layers of your software development stages and will be able to build your own in-house security automation platform throughout your mobile and cloud releases.

Learning Objectives

- Secure and automate techniques to protect web, mobile or cloud services
- Automate secure code inspection in C++, Java, Python, and JavaScript
- Automate secure code inspection with open source tools and effective secure code scanning suggestions
- Apply security testing tools and automation frameworks to identify security vulnerabilities in web, mobile and cloud services
- Integrate security testing tools such as OWASP ZAP, NMAP, SSLyze, SQLMap, and OpenSCAP
- Integrate security testing with automation frameworks like fuzz, BDD, Selenium and Robot Framework
- Implement automation testing techniques with Selenium, JMeter, Robot Framework, Gauntlt, BDD, DDT, and Python unittest
- Execute security testing of a Rest API Implement web application security with open source tools and script templates for CI/CD integration
- Integrate various types of security testing tool results from a single project into one dashboard

Prerequisites

- Basic to Intermediate IT Skills.
- Basic Python scripting skills. Attendees without a programming background like Python may view labs as follow along exercises or team with others to complete them.

- Solid foundational mathematics or logic skills
- Basic Linux skills, including familiarity with command-line options such as ls, cd, cp, and su

EC Council Certified Ethical Hacker (CEH)

ECC-201

View schedule and pricing on cdw.com

Summary

This course provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures, focusing on how hackers think and act maliciously. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident and set up a security infrastructure and defend future attacks. CEH is divided into 20 modules with extensive hands-on lab components. And exam voucher is included with this course.

WHO SHOULD ATTEND:

- Information Security Analyst / Administrator
- Information Assurance (IA) Security Officer
- Information Security Manager / Specialist
- Information Systems Security Engineer / Manager
- Information Security Professionals / Officers
- Information Security / IT Auditors
- Risk / Threat / Vulnerability Analyst
- System Administrators
- Network Administrators and Engineers

LENGTH: 5 Days

Description

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers.

CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident. CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure.

Learning Objectives

- Demonstrate the understanding of attack vectors.
- Navigate network scanning to identify live and vulnerable machines in a network.
- Perform OS banner grabbing, service, and user enumeration.
- Conduct system hacking, steganography, steganalysis attacks, and cover tracks.
- Identify and use viruses, computer worms, and malware to exploit systems.
- Employ packet sniffing.
- Conduct a variety of web server and web application attacks including directory traversal, parameter tampering, XSS, etc.
- Perform SQL injection attacks and various types of cryptography attacks.
- Implement a vulnerability analysis to identify security loopholes in the target organization’s network, communication infrastructure, and end systems etc.

Prerequisites

- At least two years of IT security experience
- A strong working knowledge of TCP/IP
- Security+ Prep Course is highly recommended

EC Council Certified Hacking Forensic Investigator (CHFI)

ECC-202

View schedule and pricing on cdw.com

Summary

EC-Council's Certified Hacking Forensic Investigator (CHFI) prepares cybersecurity professionals with the knowledge and skills to perform effective digital forensics investigations and bring their organization into a state of forensic readiness. An exam voucher is included in this course.

WHO SHOULD ATTEND:

- IT professionals involved with information system security, computer forensics, and incident response.

LENGTH: 5 Days

Description

EC-Council's Certified Hacking Forensic Investigator (CHFI) program prepares cybersecurity professionals with the knowledge and skills to perform effective digital forensics investigations and bring their organization into a state of forensic readiness. This includes establishing the forensics process, lab and evidence handling procedures, as well as the investigation procedures required to validate/triage incidents and point the incident response teams in the right direction. Forensic readiness is crucial as it can differentiate between a minor incident and a major cyber-attack that brings a company to its knees.

This intense hands-on digital forensics program immerses students in over 68 forensic labs, enabling them to work on crafted evidence files and utilize the tools employed by the world's top digital forensics professionals. Students will go beyond traditional hardware and memory forensics and learn current topics such as cloud forensics, mobile and IoT, investigating web application attacks, and malware forensics. CHFI presents a methodological approach to computer forensics, including searching and seizing, chain-of-custody, acquisition, preservation, analysis, and reporting of digital evidence.

Learning Objectives

- The computer forensic investigation process and the various legal issues involved
- Evidence searching, seizing and acquisition methodologies in a legal and forensically sound manner
- Types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category
- Roles of the first responder, first responder toolkit, securing and evaluating electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, and reporting the crime scene
- Setting up a computer forensics lab and the tools involved in it
- Various file systems and how to boot a disk
- Gathering volatile and non-volatile information from Windows
- Data acquisition and duplication rules
- Validation methods and tools required
- Recovering deleted files and deleted partitions in Windows, Mac OS X, and Linux
- Forensic investigation using AccessData FTK and EnCase
- Steganography and its techniques
- Steganalysis and image file forensics
- Password cracking concepts, tools, and types of password attacks
- Investigating password protected files
- Types of log capturing, log management, time synchronization, and log capturing tools
- Investigating logs, network traffic, wireless attacks, and web attacks

- Tracking emails and investigate email crimes
- Mobile forensics and mobile forensics software and hardware tools
- Writing investigative reports

Prerequisites

- IT/Forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, incident response, and threat vectors.

EC Council Certified Network Defender (CND)

ECC-200

View schedule and pricing on cdw.com

Summary

Certified Network Defender (CND) is a vendor-neutral, hands-on, instructor-led comprehensive network security certification training program. It is a skills-based, lab intensive network security training program based on a job-task analysis and cybersecurity education framework presented by the National Initiative of Cybersecurity Education (NICE).

WHO SHOULD ATTEND:

- Those who work in the network administration
- Anyone in a cybersecurity operations role
- Anyone looking to build their career in cybersecurity

LENGTH: 5 Days

Description

Certified Network Defender (CND) is designed by industry experts to help IT Professionals play an active role in the protection of digital business assets and detection and Response to Cyber Threats, while leveraging Threat Intelligence to Predict them before they happen. This is network security course designed to help organizations create and deploy the most comprehensive network defense system. The program prepares network administrators how to identify what parts of an organization need to be reviewed and tested for security vulnerabilities and how to reduce, prevent, and mitigate risks in the network. CND covers the protect, detect, respond and predict approach to network security.

Learning Objectives

- Recognize network security management, policies, and procedures.
- Run Windows and Linux security administration.
- Determine mobile and IoT device security.
- Apply data security techniques.
- Embed virtualization technology security and cloud and wireless security.
- Deploy risk assessment tools. · Define the basics of first response and forensics.
- Recognize the indicators of compromise, attack, and exposures (IoC, IoA, IoE).
- Build threat intelligence capabilities.
- Establish and monitor log management.
- Implement endpoint security.
- Configure firewall solutions.
- Identify IDS/IPS technologies.
- Establish network authentication, authorization, and accounting (AAA)

Prerequisites

- Cyber security fundamentals recommended
- Basic network and host operations knowledge.
- Experience commensurate with one to five years of network, host, or application administration.

EC-Council ICS SCADA Cybersecurity

ECC-300

View schedule and pricing on cdw.com

Summary

This hands-on course teaches the foundations of security and defending network architectures from attacks, using powerful methods to analyze risks possessed by network infrastructure in IT and corporate spaces.

WHO SHOULD ATTEND:

- IT professionals who manage or direct their organization's IT infrastructure and are responsible for establishing and maintaining information security policies, practices, and procedures.

LENGTH: 3 Days

Description

Offered as a private class only.

The ICS/SCADA Cybersecurity course is a hands-on training module that teaches the foundations of security and defending network architectures from attacks. Students will learn to think like a malicious hacker to defend their organizations. ICS/SCADA teaches powerful methods to analyze risks possessed by network infrastructure in IT and corporate spaces. Once your foundation or basic concepts are clear, you will learn a systematic process of intrusion and malware analysis. After this, you will learn about digital forensic process and incident response techniques upon detecting a breach. The focus in the course is on the Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Systems.

Learning Objectives

- Demonstrate the foundations of security and how to defend network architectures from attacks
- Analyze risks to network infrastructure in IT and corporate spaces
- Analyze intrusions and malware using a systemic process
- Understand the digital forensic process and respond to incidents after a breach is detected
- Think like a hacker and use techniques to defend against common attacks
- Implement best practices

Prerequisites

- Linux operating system fundamentals, including basic command line usage.
- Conceptual knowledge of programming/scripting.
- Solid grasp of essential networking concepts (OSI model, TCP/IP, networking, devices, and transmission media).
- Understanding of basic security concepts (e.g., malware, intrusion detection, systems, firewalls, and vulnerabilities).
- Familiarity with network traffic inspection tools (Wireshark, TShark, or TCPdump) is highly recommended.

Endpoint Live Forensics

OS-300

View schedule and pricing on cdw.com

Summary

Endpoint Live Forensics teaches students how to identify abnormal activity and investigate a running system that may have been compromised.

WHO SHOULD ATTEND:

- Incident Responders who need to quickly identify a security breach
- Operations Specialists needing to analyze the state of a running system
- Forensic Investigators who need to identify malicious intrusions
- Malware Analysts requiring a thorough understanding of operating system instrusions

LENGTH: 5 Days

Description

While there is undoubtedly a need for deep forensic analysis in the investigation of malware and operating system intrusions, an investigator has to know that there has been an intrusion before that activity can begin. Many organizations rely on technology to perform this task, but there is still no substitute for a well-trained analyst, when it comes to identifying and investigating abnormal behavior on a system.

Endpoint Live Forensics teaches students how to identify abnormal activity and investigate a running system that may have been compromised. In this course, students will learn the most useful commands, tools and techniques that can be employed during investigation to reveal the significant indicators of infiltration, as well as how to create a system baseline to be used for future analysis. This course is focused primarily on the Windows 10 and Linux operating systems.

Learning Objectives

- Identify the core components of the operating system and acertain a current state, using built-in or other trusted tools.
- Analyze a running system and detect abnormal behavior relating to operating system components.
- Use event log analysis to verify and correlate the artifacts of anomalous behavior and determine the scope of an intrusion.
- Build or modify PowerShell scripts to Interrogate an operating system and automate repetitive analytic tasks.
- Create and use a system baseline to identify unexpected items, such as rogue accounts or configuration changes.

Prerequisites

- Familiarity with the general use of Windows systems and at least beginner-level experience with the command line interface
- Basic understanding of TCP/IP networking
- Experience with VMware or other virtualization software is an advantage

---

Related Courses:

- Behavioral Malware Analysis
- Network Forensics and Investigation I
- Network Forensics and Investigation II

Evasive Techniques and Breaching Defenses

PEN-300

View schedule and pricing on cdw.com

Summary

Evasion Techniques and Breaching Defenses (PEN-300) is an advanced penetration testing course that builds on the knowledge and techniques taught in Penetration Testing with Kali Linux. This is an advanced course designed for OSCP-level penetration testers who want to develop their skills against hardened systems.

WHO SHOULD ATTEND:

- Information security professionals who want to take a serious and meaningful step into the world of professional penetration testing.

Description

Evasion Techniques and Breaching Defenses (PEN-300) is an advanced penetration testing course. Learners who complete the course and pass the exam will earn the OffSec Experienced Pentester (OSEP) certification. This course builds on the knowledge and techniques taught in Penetration Testing with Kali Linux, teaching learners to perform advanced penetration tests against mature organizations with an established security function and focuses on bypassing security mechanisms that are designed to block attacks. The OSEP is one of three certifications making up the OSCE³ certification along with the OSWE for advanced web attacks and OSED for exploit development.

Learning Objectives

- Preparation for more advanced field work
- Knowledge of breachingnetwork perimeter defenses through clientside attacks, evading antivirus and allow listing technologies
- How to customize advanced attacks and chain them together web vulnerabilities

Prerequisites

We strongly suggest that students taking PEN-300 have either taken PWK and passed the OSCP certification or have equivalent knowledge and skills in the following areas:

- Working familiarity with Kali Linux command line
- Solid ability run enumerating targets to identify vulnerabilities
- Basic scripting abilities in Bash, Python and PowerShell
- Identifying and exploiting vulnerabilities like SQL injection, file inclusion and local privilege escalation
- Foundational understanding of Active Directory and knowledge of basic AD attacks
- Familiarity with C# programming is a plus

Event Monitoring and Incident Detection

IR-110

View schedule and pricing on cdw.com

Summary

This is the first course in our Incident Response series. This course aims to help students develop the professional competencies to detect intrusions, determine the nature of security events, and initiate critical first response for security incidents.

WHO SHOULD ATTEND:

- Those interested in learning about the initial phases of Cyber Incident Response handling

LENGTH: 3 Days

Description

Event Monitoring and Incident Detection, part of our Incident Response series, will help students develop the professional competencies to detect intrusions, determine the nature of security events, and initiate critical first response for security incidents. It will also help to build important technical skills through several labs, tabletop exercises, and case-study based activities.

The goals of this 3-day course are to examine the Incident Response Life Cycle, determine the existence of security events, and implement the Computer Security Incident Response Team (CSIRT) Services Framework, to contain, eradicate, and remediate threats. This course is for anyone interested in learning about the initial phases of Cyber Incident Response handling. This course will also help the learner understand how to approach security incidents while working in an organization.

Learning Objectives

- Describe the requirements for technical and functional preparation for Incident Response
- Identify attack surfaces to be covered by an Incident Response Plan
- Compare tools and processes used to monitor cyber activities
- Construct a baseline of “normal” cyber traffic
- Interpret data and logs of activity
- Examine network traffic for evidence of anomalies
- Collect evidence of anomalous activity
- Explain the purposes of triage in incident response
- Apply the MITRE ATT&CK matrix to anomalous activity observed
- Construct security event timelines
- Determine if incident escalation is appropriate
- Report actionable data in a timely, clear, concise, and accurate manner
- Apply playbooks in the incident response process

Prerequisites

- Basic understanding of operating system internals
- Familiarity with the general use of Windows systems
- Basic understanding of TCP/IP networking

Related Courses:

- OS-100 Understanding Operating Systems
- IR-120 Incident Analysis
- IR-210 Incident Response Planning and Management (*coming soon*)
- IR-220 Analysis, Containment, and Recovery (*coming soon*)

Exploring the OWASP Top 10

SC-201

View schedule and pricing on cdw.com

Summary

This two day engaging course teaches an understanding of the recently updated OWASP Top 10, and provides you with the skills to protect data and maintain user trust across various digital projects.

WHO SHOULD ATTEND:

- Software Developers
- IT Professionals
- Cybersecurity enthusiasts, Project Managers, and Team Leads overseeing digital projects

LENGTH: 2 Days

Description

Offered as a private class only.

OWASP 2021 refers to the latest edition of the Open Web Application Security Project (OWASP) Top Ten list, which identifies the most critical web application security risks. It is a valuable resource as it provides organizations with insights into prevalent vulnerabilities, helping them prioritize their security efforts and fortify their applications against potential attacks.

Exploring the OWASP Top 10 is a two day engaging course that provides you with the skills to protect data and maintain user trust across various digital projects. From identifying and eliminating bugs to managing unvalidated data, you'll delve into a myriad of vulnerabilities such as Broken Access Control, Cryptographic Failures, and the complexities of Server-Side Request Forgeries (SSRF). Throughout the course you'll explore the realm of software integrity, proper handling of authentication data, and the importance of robust security logging and monitoring systems. You'll also examine the challenges of 'Shifting Left' in software development processes and explore the intricacies of handling software and data integrity failures. These encompass using trusted repositories, protecting software development resources, and issues related to Continuous Integration/Continuous Deployment (CI/CD) pipelines.

This course is led by a seasoned web application security expert who shares practical insights, best practices, and real-life experiences, adding invaluable depth to your learning journey. Through engaging demonstrations and activities, you'll apply your newfound knowledge to real-world scenarios, enhancing your ability to analyze and mitigate security risks while maintaining privacy and ethical standards. You'll also gain practical experience with innovative tools and strategies, working through labs mirroring real-world situations, such as dissecting high-profile case studies like SolarWinds and Capital One.

By the end of this course, you'll have a robust understanding of the OWASP Top Ten, secure software development principles, and a broadened view of web application security. Armed with these skills, you'll be well-prepared to help your organization navigate the challenging landscape of cybersecurity.

Learning Objectives

- Learn to execute bug hunting and hacking activities in a manner that respects privacy and system integrity.
- Develop the ability to recognize and effectively utilize defect/bug reporting systems within your organization.
- Gain insights into common mistakes made during bug hunting and vulnerability testing and learn strategies to avoid them.
- Delve into the principles and terminology of defensive coding, including understanding the phases and objectives of a typical exploit, to build more secure applications.
- Recognize the value of a layered, in-depth defense strategy in cybersecurity, enhancing your capacity to build robust and resilient systems.
- Understand the potential origins of untrusted data and the risks they pose.

- Learn about the vulnerabilities associated with authentication and authorization, and how to detect, attack, and implement defenses.
- Familiarize yourself with the risks involved in XML processing, file uploads, and server-side interpreters, and learn how to mitigate these risks.

Prerequisites

- Real-world programming experience is highly recommended for code reviews, but not required.

Hacker Methodologies for Security Professionals

HK-300

View schedule and pricing on cdw.com

Summary

This course teaches you the processes threat actors use to break into organizations' networks and steal their most sensitive data.

WHO SHOULD ATTEND:

- Threat Hunters who need to understand hacker behavior and methodology
- Security Analysts and Incident Responders who need to indentify signs of compromise
- New members of penetration testing or red teams

LENGTH: 5 Days

Description

Hacker Methodologies for Security Professionals teaches you the processes threat actors use to break into organizations' networks and steal their most sensitive data. Utilizing industry-standard penetration testing and auditing software, you will learn to identify, scan, and enumerate target systems; correlate services to vulnerabilities and exploits; employ exploits to gain access to the target systems; elevate privileges; propagate through the network; and cover their tracks within a target network. This course is focused primarily on Linux and Windows operating systems, so students should be comfortable with both.

Learning Objectives

- Identify the classes of hackers, their motivations, and the methodologies employed by threat actors
- Use publicly available tools and open source intelligence techniques to develop a target footprint
- Scan and enumerate targets to identify underlying operating systems and services
- Research and leverage exploits for vulnerable services to achieve access to target systems
- Identify system configuration weaknesses and viable privilege escalation tactics
- Analyze exploited systems to identify and remove indicators of compromise
- Employ system tools to exploit additional targets within an internal system

Prerequisites

- Familiarity with Windows or Linux command-line interfaces
- Knowledge of TCP/IP networking

HCISPP: HealthCare Information Security and Privacy Practitioner

ISC-204

View schedule and pricing on cdw.com

Summary

The HealthCare Information Security and Privacy Practitioner (HCISPP) educational course are intended to communicate to the audience the basic structure, the essentials of the legal basis, the issues of and the information security and privacy particulars within the described context of the American healthcare delivery system. An integral part of this course is to prepare the attendee (with the required minimum experience) to sit for the (ISC)² HCISPP certification examination.

Description

Offered as a private class only.

Learning Objectives

- Determine the Healthcare environment components, third-party relationships, and foundational health data management concepts.
- Compare information governance frameworks, roles and responsibilities, security, and privacy policies as well as standards and procedures.
- Identify the impact of healthcare information technologies on privacy and security.
- Verify regulatory requirements, regulations and controls and the privacy and security compliance frameworks.
- Define security objectives, attributes, security definitions, concepts and security and privacy governance.
- Verify basic risk management methodologies and the information risk management life cycles.
- Participate in risk assessment consistent with a role in the organization and remediate gaps.
- Identify risk response and control assessment procedures from within organizational risk frameworks as well as continuous monitoring.

Prerequisites

- 5 or more years of professional practice of which 2 should be in a healthcare environment.

Incident Analysis

IR-120

View schedule and pricing on cdw.com

Summary

This is the second course in the Incident Response series, taking students through the critical processes that occur once a security event has been elevated to the status of a confirmed security incident.

WHO SHOULD ATTEND:

- Entry-level incident responders and incident investigators
- Information Technology personnel interested in transitioning to a security role
- Anyone interested in fundamental Blue or Purple Teams operations

LENGTH: 3 Days

Description

This introductory-level course is aimed at a broad audience - anyone who is interested in learning about the Incident Response Life Cycle and how to analyze, contain, and recover from a security incident. This is the second course in the Incident Response series, taking students through the critical processes that occur once a security event has been elevated to the status of a confirmed security incident.

The goals of this 3-day course are to have students analyze log and sensor data, network traffic, host-based artifacts, emails, and contextual data for evidence related to the attack vectors and scope of a breach, using FIRST CVSS 4.0 and other tools. Once this analysis is complete, students will use playbooks and industry-recognized resources, such as the MITRE ATT&CK matrix, to determine the appropriate follow-on actions for containment and recovery.

Learning Objectives

- Identify the types of data relevant to information security events
- Analyze host-based artifacts for the presence of anomalous activity
- Assess log and sensor data for detection of anomalous activity
- Assess contextual data sources for detection of anomalous activity
- Analyze email traffic for the presence of anomalous activity
- Analyze network traffic for the presence of anomalous activity
- Apply playbooks to contain and mitigate threats
- Recommend actions for containment and recovery using the Mitre ATT&CK matrix and detection use cases
- Simulate best practices for containment, analysis, and recovery in an incident response scenario

Prerequisites

- Basic understanding of operating system internals
- Familiarity with the general use of Windows systems
- Basic understanding of how network traffic traverses intranets, extranets, cloud, and the internet.

Related Courses:

- OS-100 Understanding Operating Systems
- IR-110 Event Monitoring and Incident Detection
- IR-210 Incident Response Planning and Management (*coming soon*)
- IR-220 Analysis, Containment, and Recovery (*coming soon*)

Introduction to Security Analysis

CS-101

View schedule and pricing on cdw.com

Summary

This hands-on course gives a jumpstart into the analysis of network intrusions, compromised hosts, and malware.

WHO SHOULD ATTEND:

- IT Administrators
- System analysts and engineers who wish to incorporate security in their design processes
- Interns and newly hire security team members
- Anyone considering a career transition to security analysis

LENGTH: 2 Days

Description

Most IT professionals are aware of the importance their jobs play in securing an organization, but many are not adequately trained in this important function and may not know where to begin. This hands-on course gives a jumpstart into the analysis of network intrusions, compromised hosts, and malware. Students will learn what common attacks look like, how to track and analyze malicious activity, and what mitigation steps should be taken.

Learning Objectives

- Profile/baseline the hosts, services and activity in a computer network
- Perform user-level attribution of unwanted activity in a network
- Compare observed network traffic to expected topology
- Identify and observe the core components of an operating system
- Conduct basic behavioral analysis of malware on a running Windows system

Prerequisites

- A background in information technology
- Basic understanding of networking and security concepts
- Light experiencewith the Windows Sysinternals Suite

iOS Attack and Defend

CT-401

View schedule and pricing on cdw.com

Summary

iOS™ Attack & Defend provides an instructor-led, hands-on course in the fundamentals of software development. This course is a laboratory intensive programming course designed for students looking to gain a working knowledge in iOS development. Through a combination of instructor-led examples and a series of programming assignments and challenges, the students will build and enhance their practical knowledge of software development in the iOS operating system. Additionally, students will also deploy, execute, and test all developed programs on Apple devices, provided in the class.

Description

None

Learning Objectives

- Identify iOS versions, design features, devices, and hardware.
- Navigate the File system
- Explore the iPhone and its capabilities
- Implement various Jailbreaking techniques
- Determine the differences in RE for disassembling and decompiling
- Identify the languages of ARM
- Recall the Components of Computer Architecture
- Distinguish the differences between RISC vs. CISC Design
- Recognize the Design Philosophy and two modes
- Examine the Components of RISC Architecture
- Define ARM Processor Basics
- Navigate ARM Instructions
- Compile and execute the Mach-O File Format
- Hack an iPhone Application
- Summarize iOS Security Features
- Execute Encryption and Code Signing
- Determine how to use Real World Malware
- Manipulate Live View Debugging

Prerequisites

- Experience with Apple® products such as Apple® phones and tablets is recommended.

ISACA Certified Information Security Manager (CISM)

ISACA-250

View schedule and pricing on cdw.com

Summary

Validate your proficiencies for handling the challenges and responsibilities of a modern IT security manager with a CISM, which focuses on information security governance, information security risk management, information security program development, and incident management. This advanced-level course prepares you for the Certified Information Security Manager® exam.

WHO SHOULD ATTEND:

- Information Security Managers
- Information Security Consultants
- CIOs and CISOs

LENGTH: 3 Days

Description

Certified Information Security Manager® (CISM®) affirms your ability to assess risks, implement effective governance, and proactively respond to incidents. With a highlight on emerging technologies such as AI and blockchain, it guarantees your skillset meets evolving security threats and industry requirements. By addressing top-of-mind concerns like data breaches and ransomware attacks, crucial for IT professionals, this certification ensures you are staying ahead of the pace of change.

Learning Objectives

- Ensure that an enterprise's information is protected
- Have the expertise needed to reduce risk and protect the enterpris
- Design, develop, implement and manage an effective security management program
- Establish and maintain an IT governance framework aligned with business objectives
- Identify and manage information security risks
- Have an understanding of the format and structure of the CISM certification exam
- Have knowledge of the various topics and technical areas covered by the exam
- Practice with specific strategies, tips and techniques for taking and passing the exam

Prerequisites

- 5 years of IT and security experience

Linux Kernel Internals

OS-500

View schedule and pricing on cdw.com

Summary

This intermediate level course focuses on the skills of investigating the internals of the Linux kernel and the development and debugging of Linux loadable kernel modules.

WHO SHOULD ATTEND:

- Offensive and defensive security professionals including security researchers, digital forensic analysts, red-teamers and blue-teamers and anyone who wants to learn about the modern Linux kernel.

LENGTH: 5 Days

Description

Linux Kernel Internals covers the internals of the Linux kernel and kernel module development with emphasis on security. The course covers the internal algorithms, data structures, programming interfaces, relevant parts of the latest Linux kernel source code and real world use cases to provide a holistic view of the topics.
Attendees learn about the basics of the Linux kernel, kernel development toolchain, kernel module development, kernel execution contexts, memory management, user-kernel interfaces, device drivers, virtual file system interface, kernel synchronization mechanisms and kernel debugging.

In the hands-on labs attendees use built-in tools to peek into the kernel and use kernel programming interfaces to implement various functionality as loadable kernel modules (LKM). Attendees build, deploy, test and debug these LKMs on the latest 64-bit Linux kernel.

Learning Objectives

- Describe the different components of the Linux kernel.
- Develop, build, test and debug Linux kernel modules.
- Implement security related functionality in kernel modules.
- Identify the kernel programming interfaces to solve a given development task.
- Retrieve information from the kernel using various commands.
- Examine crash dumps and identify the cause of the crash.
- Build the foundation to attend the Linux Kernel Exploitation and Rootkit training (LKXR).

Prerequisites

- Proficient in C programming language.
- Comfortable with Linux command line tools.
- Familiar with Linux development tools such as gcc and make.
- Knowledgeable of data-structures such as pointers, structures, arrays and linked lists.

Machine Learning Operations (MLOps) and AI Security

AI-450

View schedule and pricing on cdw.com

Summary

Dive into the rapidly evolving world of Machine Learning Operations (MLOps) and AI Security with our intensive 3-day boot camp. MLOps bridges the gap between data science and operation teams, delivering continuous collaboration and integration to drive the efficient production of AI models.

WHO SHOULD ATTEND:

- Technical professionals eager to deepen their knowledge in machine learning and AI security.
- Data Scientists, Machine Learning Engineers, IT Security Professionals, and DataOps Engineers.
- Technical leads and managers who oversee machine learning projects and need to understand both the operational and security aspects of AI systems.

LENGTH: 3 Days

Description

Dive into the rapidly evolving world of **Machine Learning Operations (MLOps) and AI Security** with our intensive 3-day boot camp. MLOps bridges the gap between data science and operation teams, delivering continuous collaboration and integration to drive the efficient production of AI models. Similarly, AI Security focuses on protecting AI systems from potential vulnerabilities, a critical skillset given the increasing reliance on AI in modern infrastructures. By mastering these skills, you'll be able to streamline machine learning projects and bolster security within your organization.

Working in a hands-on workshop style environment guided by our AI security expert, you'll explore a wide range of topics and hands-on labs designed to provide a robust understanding of both MLOps and AI Security. Starting from an introduction to MLOps, you'll uncover the importance of this discipline, its distinction from DevOps and DataOps, and its lifecycle. You'll explore MLOps tools and techniques, including MLflow and Kubeflow, along with pipeline components and best practices. You will be able to set up an MLOps environment, automate ML workflows, monitor and manage models, and implement vital security measures in real-world situations. Lastly, you'll dive into the world of AI Security, exploring the AI threat landscape and best practices while applying basic security measures in a lab environment. The boot camp wraps up with advanced topics in AI Security, covering AI privacy, ethical considerations, adversarial attacks, and defenses.

Upon completion, you will have gained practical, hands-on skills in operationalizing and securing machine learning workflows, implementing best practices in model management, and understanding ethical considerations in AI Security. Our boot camp ensures that you will have the necessary knowledge to navigate MLOps and AI Security effectively, making your machine learning projects more efficient and secure.

Learning Objectives

- Gain a solid understanding of the Machine Learning Operations (MLOps) lifecycle, including its purpose, key elements, and how it differs from related fields like DevOps and DataOps.
- Develop practical skills in using key MLOps tools and techniques, such as setting up an MLOps environment using MLflow and Kubeflow, and working through a basic machine learning pipeline.
- Master the art of automating machine learning workflows to streamline and improve the efficiency of your machine learning projects.
- Familiarize yourself with the AI Security landscape, including threat identification and application of best practices for securing machine learning environments.
- Dive deep into advanced AI Security concepts, including understanding and implementing differential privacy in machine learning models and defending against adversarial attacks.

- Learn to balance technical implementation with ethical considerations, developing a well-rounded approach to AI Security that respects privacy concerns and adheres to ethical guidelines.

Prerequisites

- Familiarity with basic machine learning concepts such as supervised and unsupervised learning, regression, classification, and neural networks will be beneficial.
- Experience with data preprocessing, feature engineering, and understanding of algorithms and data structures would be advantageous.
- Ideally, attendees should have practical experience with a programming language, preferably Python, given its prominence in machine learning and AI development. Those without programming background can follow along with the labs.
- Basic knowledge of cloud platforms like AWS, GCP, or Azure will be useful, especially regarding how they support machine learning operations and AI security.
- A general understanding of the software development process or lifecycle (SDLC), including stages like design, development, testing, and deployment, will be helpful as MLOps is a similar, but more specific, lifecycle.

Malware Reverse Engineering

RE-400

View schedule and pricing on cdw.com

Summary

This course teaches students how to perform more advanced analysis of real-world malware samples.

WHO SHOULD ATTEND:

- Malware analysts who want to develop more advanced skills in reverse engineering
- Forensic investigators who need to analyze malicious software
- Threat intelligence analysts developing code-based and behavioral signatures

LENGTH: 5 Days

Description

Malware Reverse Engineering teaches students how to perform more advanced analysis of real-world malware samples. The primary techniques taught are disassembly and debugging. The course also covers topics such as data decoding and binary obfuscation in order to bypass protections and perform effective analysis on hardened samples, how to deal with destructive malware, and how to defeat anti-debugging and other anti-analysis techniques.

Learning Objectives

- Use IDA Pro, OllyDbg, x64dbg, and other tools to analyze and debug malware, and report on its capabilities
- Describe in detail the structure and functions of the Portable Executable (PE) header, and analyze PE headers to aid in malware characterization
- Apply techniques for identifying, analyzing, and bypassing data obfuscation
- Understanding the structure and use of Dynamic Linked Libraries (DLLs) and apply reverse engineering skills to DLL analysis
- Identify and overcome a range of anti-debugging and anti-analysis techniques used in modern malware
- Identify developer code in a compiled binary

Prerequisites

- Successful completion of Assembly for Reverse Engineers course
- Strong understanding of operating system internals
- Experience in C programming and Python is recommended

Microsoft Azure Security Technologies (AZ-500T00)

MS-AZ-500

View schedule and pricing on cdw.com

Summary

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization’s security posture, and identify and remediate security vulnerabilities.

WHO SHOULD ATTEND:

- Azure Security Engineers who are planning to take the associated certification exam, or who are performing security tasks in their day-to-day job.
- Engineers that wants to specialize in providing security for Azure-based digital platforms and play an integral role in protecting an organization's data.

LENGTH: 4 Days

Description

Microsoft Azure Security Technologiesprovides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization’s security posture, and identify and remediate security vulnerabilities. This course includes security for identity and access, platform protection, data and applications, and security operations.

Learning Objectives

- Implement enterprise governance strategies including role-based access control, Azure policies, and resource locks.
- Implement an Azure AD infrastructure including users, groups, and multi-factor authentication.
- Implement Azure AD Identity Protection including risk policies, conditional access, and access reviews.
- Implement Azure AD Privileged Identity Management including Azure AD roles and Azure resources.
- Implement Azure AD Connect including authentication methods and on-premises directory synchronization.
- Implement perimeter security strategies including Azure Firewall.
- Implement network security strategies including Network Security Groups and Application Security Groups.
- Implement host security strategies including endpoint protection, remote access management, update management, and disk encryption.
- Implement container security strategies including Azure Container Instances, Azure Container Registry, and Azure Kubernetes.
- Implement Azure Key Vault including certificates, keys, and secretes.
- Implement application security strategies including app registration, managed identities, and service endpoints.
- Implement storage security strategies including shared access signatures, blob retention policies, and Azure Files authentication.
- Implement database security strategies including authentication, data classification, dynamic data masking, and always encrypted.
- Implement Azure Monitor including connected sources, log analytics, and alerts.
- Implement Azure Security Center including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.

Prerequisites

- Security best practices and industry security requirements such as defense in depth, least privileged access, role-based access control, multi-factor authentication, shared responsibility, and zero trust model.
- Be familiar with security protocols such as Virtual Private Networks (VPN), Internet Security Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.

- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security-specific information.
- Have experience with Windows and Linux operating systems and scripting languages. Course labs may use PowerShell and the CLI.
- Prior attendance of the course Microsoft Azure Administrator (AZ-104T00) is recommended.

Microsoft Cybersecurity Architect (SC-100T00)

MS-SC-100

View schedule and pricing on cdw.com

Summary

This is an advanced, expert-level course that prepares students with the expertise to design and evaluate cybersecurity strategies in the following areas: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps), and data and applications.

WHO SHOULD ATTEND:

- Experienced Cloud Security Engineers who have taken a previous certification in the security, compliance, and identity portfolio.

LENGTH: 4 Days

Description

This is an advanced, expert-level course. Although not required to attend, students are strongly encouraged to have taken and passed another associate level certification in the security, compliance and identity portfolio (such as AZ-500, SC-200 or SC-300) before attending this class. This course prepares students with the expertise to design and evaluate cybersecurity strategies in the following areas: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps), and data and applications. Students will also learn how to design and architect solutions using zero trust principles and specify security requirements for cloud infrastructure in different service models (SaaS, PaaS, IaaS).

Learning Objectives

- Introduction to Zero Trust and best practice frameworks
- Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
- Design solutions that align with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB)
- Design a resiliency strategy for common cyberthreats like ransomware
- Case study: Design solutions that align with security best practices and priorities
- Design solutions for regulatory compliance
- Design solutions for identity and access management
- Design solutions for securing privileged access
- Design solutions for security operations
- Case study: Design security operations, identity, and compliance capabilities
- Design solutions for securing Microsoft 365
- Design solutions for securing applications
- Design solutions for securing an organization's data
- Case study: Design security solutions for applications and data
- Specify requirements for securing SaaS, PaaS, and IaaS services
- Design solutions for security posture management in hybrid and multicloud environments
- Design solutions for securing server and client endpoints
- Design solutions for network security
- Case study: Design security solutions for infrastructure

Prerequisites

- Highly recommended to have attended and passed one of the associate-level certifications in the security, compliance, and identity portfolio (such as AZ-500, SC-200, or SC-300)

- Advanced experience and knowledge in identity and access, platform protection, security operations, securing data, and securing applications.
- Experience with hybrid and cloud implementations.

Microsoft Identity and Access Administrator (SC-300T00)

MS-SC-300

View schedule and pricing on cdw.com

Summary

Explore how to design, implement, and operate an organization's identity and access management systems by using Azure AD.

WHO SHOULD ATTEND:

- Identity and Access Administrators who are planning to take the associated certification exam, or who are performing identity and access administration tasks in their day-to-day job.
- Administrators or engineers who want to specialize in providing identity solutions and access management systems for Azure-based solutions.

LENGTH: 4 Days

Description

Learn to manage tasks such as providing secure authentication and authorization access to enterprise applications. You will also learn to provide seamless experiences and self-service management capabilities for all users. Finally, learn to create adaptive access and governance of your identity and access management solutions ensuring you can troubleshoot, monitor, and report on your environment. The Identity and Access Administrator may be a single individual or a member of a larger team. Learn how this role collaborates with many other roles in the organization to drive strategic identity projects. The end goal is to provide you the knowledge to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

Learning Objectives

- Explore identity in Microsoft Entra ID
- Implement initial configuration of Microsoft Entra ID
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity
- Secure Microsoft Entra users with multifactor authentication
- Manage user authentication
- Plan, implement, and administer Conditional Access
- Manage Microsoft Entra Identity Protection
- Implement access management for Azure resources
- Plan and design the integration of enterprise apps for SSO
- Implement and monitor the integration of enterprise apps for SSO
- Implement app registration
- Plan and implement entitlement management
- Plan, implement, and manage access review
- Plan and implement privileged access
- Monitor and maintain Microsoft Entra ID

Prerequisites

- Security best practices and industry security requirements such as defense in depth, least privileged access, shared responsibility, and zero trust model.
- Be familiar with identity concepts such as authentication, authorization, and active directory.

- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security-specific information.
- Some experience with Windows and Linux operating systems and scripting languages is helpful but not required. Course labs may use PowerShell and the CLI.

Microsoft Security Operations Analyst (SC-200T00)

MS-SC-200

View schedule and pricing on cdw.com

Summary

Learn how to mitigate cyberthreats using by configuring and using Microsoft Sentinel as well as utilizing Kusto Query Language (KQL) to perform detection, analysis, and reporting.

WHO SHOULD ATTEND:

- Anyone in a Security Operations role who wants to prepare for the SC-200: Microsoft Security Operations Analyst exam.

LENGTH: 4 Days

Description

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment.

The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies. In this role, you collaborate with business stakeholders, architects, identity administrators, Azure administrators, and endpoint administrators to secure IT systems for the organization.

Learn to reduce organizational risk by:

- Rapidly remediating active attacks in the environment.
- Advising on improvements to threat protection practices.
- Referring violations of organizational policies to appropriate stakeholders.

Learning Objectives

- Introduction to Microsoft 365 Threat Protection
- Mitigate Incidents with Microsoft 365 Defender
- Protect Identities using Azure AD Identity Protection
- Remediate Risks with Microsoft Defender for Office 365
- Secure Cloud Apps and Services with Microsoft Defender for Cloud Apps
- Respond to Data Loss Prevention Alerts in Microsoft 365
- Manage Insider Risk in Microsoft Purview
- Investigate Threats using Audit Features in Microsoft 365 Defender and Microsoft Purview
- Protect Against Threats with Microsoft Defender for Endpoint
- Utilize Threat Intelligence and Security Analytics in Microsoft Sentinel

Prerequisites

- Basic understanding of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Microsoft Windows

- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts.

Microsoft Security, Compliance, and Identity Fundamentals (SC-900T00)

MS-SC-900

View schedule and pricing on cdw.com

Summary

In this course students will learn the various security, compliance, and identity concepts.

WHO SHOULD ATTEND:

- Anyone looking to familiarize themselves with the fundamentals of security, compliance, and identity (SCI) across cloud-based and related Microsoft services.

LENGTH: 1 Day

Description

Microsoft Security, Compliance, and Identity Fundamentals will teach you various security, compliance, and identity concepts. After attending you will be able to describe the capabilities of Microsoft's identity and access management solutions and Microsoft security and compliance solutions.

Learning Objectives

- Describe security and compliance concepts
- Describe identity concepts
- Describe the services and identity types of Microsoft Entra ID
- Describe the authentication capabilities of Microsoft Entra ID
- Describe the access management capabilities of Microsoft Entra ID
- Describe the identity protection and governance capabilities of Microsoft Entra
- Describe core infrastructure security services in Azure
- Describe security management capabilities in Azure
- Describe the capabilities in Microsoft Sentinel
- Describe threat protection with Microsoft 365 Defender
- Describe Microsoft's Service Trust portal and privacy capabilities
- Describe the compliance management capabilities in Microsoft Purview
- Describe information protection, data lifecycle management, and data governance capabilities in Microsoft Purview
- Describe the insider risk capabilities in Microsoft Purview
- Describe the eDiscovery and Audit capabilities in Microsoft Purview

Prerequisites

- General understanding of networking and cloud computing concepts.
- General IT knowledge or any general experience working in an IT environment.
- General understanding of Microsoft Azure and Microsoft 365.

Network Forensics and Investigation I

CT-300

View schedule and pricing on cdw.com

Summary

This course focuses on research, filtering, and comparative analysis to identify and attribute the different types of activity on a network.

WHO SHOULD ATTEND:

- Network Administrators seeking to develop security-related skill Incident Responders needing to quickly address system security breaches
- Forensic Analysts seeking a better understanding of network intrusion
- Penetration Testers looking to reduce their detectability

LENGTH: 5 Days

Description

The preponderance of network traffic, particularly web traffic, was an expected outcome of the pivotal role that the Internet has come to play in our daily lives. The sheer volume of traffic and complexity of protocols creates a very diverse and ever-changing landscape within which the network analyst must navigate. Network Forensics and Investigation teaches attendees to differentiate between normal and abnormal network traffic, track the flow of packets through a network, and attribute conversations and actions taken over a network segment to specific hosts or users.

This course focuses on research, filtering, and comparative analysis to identify and attribute the different types of activity on a network. Students will learn how to follow conversations across a wide range of protocols and through redirection and how to develop custom filters for non-dissected protocols.

Learning Objectives

- Create a baseline of the protocols, hosts, and interactions in a network environment
- Identify anomalous network traffic using a combination of in-depth packet analysis and higher-level statistical analysis
- Reconstruct event timelines and accurately correlate, or distinguish between event threads
- Identify and extract network artifacts for further forensic analysis
- Compare observed network traffic to expected topology
- Research and analyze unknown (non-dissected) protocols

Prerequisites

- Firm understanding of TCP/IP networking. CompTIA Network+
- Cisco CNET or similar is recommended
- Experience with a packet analyzer
- Ability to reconstruct a network topology map from pcap data
- CompTIA Security+ or similar knowledge of security threats

Related Courses:

- Endpoint Live Forensics
- Network Forensics & Investigation II

- Automated Network Defense

Network Forensics and Investigation II

CT-301

View schedule and pricing on cdw.com

Summary

This intermediate-level course will teach you how to identify and analyze the most common types of reconnaissance, attack, lateral movement, exfiltration, and command and control traffic found in today's networks.

WHO SHOULD ATTEND:

- Security analysts who need to identify and investigate network intrusions
- Incident responders who need to quickly address a breach
- Forensic investigators who need to examine malicious network attacks

LENGTH: 5 Days

Description

Network Forensics and Investigation II covers a range of techniques from deep-packet analysis to statistical-flow analysis to open-source research and more, using tools such as Wireshark, Network Miner and RSA NetWitness Investigator as well as custom tools and scripts developed by our networking experts. Growing in complexity throughout the week, the course ends with a team exercise where you and your teammates will investigate and report on an extensive, multi-stage intrusion.

Learning Objectives

- Identify and analyze attacks across the various layers of the network stack
- Identify signs of reconnaissance being conducted against a network and recommend mitigation steps to limit the data provided to attackers
- Perform flow analysis to uncover anomalous and malicious activity at a statistical level
- Detect and investigate tunneling, botnet command-and-control traffic, and other forms of covert communications being utilized in a network
- Accurately correlate multiple stages of malicious activity in order to build a complete picture of the scope and impact of a coordinated network intrusion

Prerequisites

- CCNA and/or 1 year of experience as an Incident Handler or similar role
- Experience using a packet analyzer
- Knowledge of common Web App funcationality and architecture
- Some scripting familiarity recommended

Related Courses

- Network Forensics and Investigation I
- Automated Network Defense

OffSec PEN-200 - Penetration Testing with Kali Linux (OSCP)

PEN-200

View schedule and pricing on cdw.com

Summary

Penetration Testing with Kali Linux, is a unique penetration course course that combines traditional course materials with hands-on simulations, using a virtual lab environment.

WHO SHOULD ATTEND:

- Security and other technology professionals who want to learn pentesting
- Seasoned pentesters seeking to sharpen their skills

LENGTH: 5 Days, + 6 Mentoring Sessions

Description

Penetration Testing with Kali Linux is a unique online penetration testing course that introduces learners to the latest pentesting methodologies, tools, and techniques via hands-on experience. PEN-200 simulates a full penetration test from start to finish by immersing the learners into a target-rich and vulnerable network environment.

This foundational-level course is designed for security and other technology professionals who want to take a meaningful step into the world of professional pentesting, as well as seasoned pentesters seeking to sharpen their skills and earn one of the most coveted pentesting certifications.

Learning Objectives

- Using information gathering techniques to identify and enumerate targets running various operating systems.
- Writing basic scripts and tools to aid in the penetration testing process
- Analyzing, correcting, modifying, cross-compiling and porting public exploit code
- Conducting remote, local privilege escalation and clientside attacks
- Identifying and exploiting XSS, SQL injection and file inclusion vulnerabilities in web applications
- Leveraging tunneling techniques to pivot between networks
- Creative problem solving and lateral thinking skills

Prerequisites

- Solid understanding of TCP/IP networking
- Reasonable Windows and Linux administration experience
- Familiarity with basic Bash and/or Python scripting

Python for Reverse Engineers

RE-500

View schedule and pricing on cdw.com

Summary

This course is geared towards reverse engineers and introduces how to use Python to accelerate, automate, and optimize reverse engineering tasks.

WHO SHOULD ATTEND:

- Intermediate reverse engineers interested in automating repetitive tasks

LENGTH: 5 Days

Description

Python Reverse Engineers is geared towards the reverse engineer and introduces the Python language with a focus on using it to accelerate, automate, and optimize reverse engineering tasks. The course begins with an introduction to the Python language, a review of object types and flow statements, then delves into file operations, modules, working with the CTypes library for interaction with Windows operating systems, debugging, and IDA scripting.

Learning Objectives

- Compose Python scripts to automate repetitive tasks
- Perform tasks with the Windows API from Python using the CTypes library
- Implement a scriptable Windows debugger using Python and CTypes
- Use the IDAPython API to automate common reverse engineering tasks in IDA

Prerequisites

- Successful completiong of Malware Reverse Engineering
- Familiarity with programming/scripting
- Strong understanding of operating system internals
- Experience in C programming

Related Courses

- Assemly for Reverse Engineers
- Malware Reverse Engineering

SCOR - Implementing and Operating Cisco Security Core Technologies

SCOR

View schedule and pricing on cdw.com

Summary

Master the skills and technologies needed to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks.

WHO SHOULD ATTEND:

- Security Engineers
- Network Engineers
- Network Designers
- Network Administrators
- Systems Engineers
- Consulting Systems Engineers
- Technical Solutions Architects
- Cisco Integrators/Partners
- Network Managers
- Cisco integrators and partners

LENGTH: 5 Days

Description

The Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 course helps you prepare for the Cisco© CCNP© Security and CCIE© Security certifications and for senior-level security roles. In this course, you will master the skills and technologies you need to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. You will learn security for networks, cloud and content, endpoint protection, secure network access, visibility, and enforcement. You will get extensive hands-on experience deploying Cisco Firepower Next-Generation Firewall and Cisco ASA Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. You will get introductory practice on Cisco Stealthwatch Enterprise and Cisco Stealthwatch Cloud threat detection features.

This course, including the self-paced material, helps prepare you to take the exam, Implementing and Operating Cisco Security Core Technologies (350-701 SCOR), which leads to the new CCNP Security, CCIE Security, and the Cisco Certified Specialist – Security Core certifications.

Learning Objectives

- Describe information security concepts and strategies within the network
- Describe common TCP/IP, network application, and endpoint attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on the Cisco ASA appliance and Cisco Firepower Next-Generation Firewall
- Describe and implement basic email content security features and functions provided by the Cisco Email Security Appliance
- Describe and implement web content security features and functions provided by the Cisco Web Security Appliance
- Describe Cisco Umbrella security capabilities, deployment models, policy management, and Investigate console
- Introduce VPNs and describe cryptography solutions and algorithms

- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco IOS VTI-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower NGFW
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and EAP authentication
- Provide a basic understanding of endpoint security and describe AMP for Endpoints architecture and basic features
- Examine various defenses on Cisco devices that protect the control and management plane
- Configure and verify Cisco IOS Software Layer 2 and Layer 3 Data Plane Controls
- Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- Describe the basics of cloud computing and common cloud attacks and how to secure cloud environment

Prerequisites

- Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA) v1.0 course
- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts
- Familiarity with the basics of networking security concepts

Secure Web App Development Overview - Java / JEE

SC-301

View schedule and pricing on cdw.com

Summary

This is a lab-intensive, hands-on Java / JEE security training course that provides 360-degree coverage of Java application security.

WHO SHOULD ATTEND:

- Experienced Java developers who wish to get up and running on developing well defended software applications.

LENGTH: 5 Days

Description

Offered as a private class only.

Secure Java Web Application Development Lifecycle is a lab-intensive, hands-on Java / JEE security training course that provides 360-degree coverage of Java application security. In this course, students begin with penetration testing, hunting for bugs in Java web applications. They then thoroughly examine best practices for defensively coding web applications, covering all the OWASP Top Ten as well as several additional prominent vulnerabilities (such as file uploads, CSRF and direct object references). Students will repeatedly attack and then defend various assets associated with fully functional web applications and services. This hands-on approach drives home the mechanics of how to secure JEE web applications in the most practical of terms.

Finally, students examine the controls (defenses) related to the phases that attackers work through when exploiting web applications. The course focuses on three specific activities that are interrelated and move the security process farther to the left in the development process. The course ends with an extensive discussion of what a mature application security presence would provide to the developers within an organization.

Learning Objectives

- Ensure that any hacking and bug hunting is performed in a safe and appropriate manner
- Identify defect/bug reporting mechanisms within their organizations
- Work with specific tools for targeted vulnerabilities
- Avoid common mistakes that are made in bug hunting and vulnerability testing
- Understand the concepts and terminology behind defensive, secure coding including the phases and goals of a typical exploit
- Develop an appreciation for the need and value of a multilayered defense in depth
- Understand potential sources for untrusted data
- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- To test web applications with various attack techniques to determine the existence of and effectiveness of layered defenses
- Prevent and defend the many potential vulnerabilities associated with untrusted data
- Understand the vulnerabilities of associated with authentication and authorization
- Detect, attack, and implement defenses for authentication and authorization functionality and services
- Understand the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks
- Detect, attack, and implement defenses against XSS and Injection attacks
- Understand the risks associated with XML processing, file uploads, and server-side interpreters and how to best eliminate or mitigate those risks

- Learn the strengths, limitations, and use for tools such as code scanners, dynamic scanners, and web application firewalls (WAFs)
- Understand techniques and measures that can used to harden web and application servers as well as other components in your infrastructure
- Recognize and characterize existing and planned defensive controls
- Relate controls and activities to the phases of a typical exploit
- Understand and implement the processes and measures associated with the security development lifecycle (SDL)
- Identify appropriate security objectives and regulations including evolving privacy considerations
- Develop a list of risk escalators as well as potential mitigations based on an understanding of vulnerabilities
- Recognize design features that can significantly increase an application's attack surface
- Build an asset inventory and begin the process of prioritizing their value
- Work with a baseline asset inventory to develop an initial asset inventory for a software application
- Understand and apply defensive options to data assets

Prerequisites

- Familiarity with Java and JEE is required.
- Real world programming experience is highly recommended.
- Ideally students should have approximately 6 months to a year of Java and JEE working knowledge.

Securing Web Applications Overview

SC-200

View schedule and pricing on cdw.com

Summary

This course equips you with the foundational concepts of defensive and secure coding, going beyond the "penetrate and patch" approach by learning to integrate security into your applications from the get-go.

WHO SHOULD ATTEND:

- Web Developers
- Technical Stakeholders
- Software Engineers
- System Administrators

LENGTH: 2 Days

Description

Securing Web Applications Overview is geared for web developers and technical stakeholders who need to produce secure web applications, integrating security measures into the development process from requirements to deployment and maintenance. This overview-level course explores core concepts and challenges in web application security, showcasing current, real-world examples that illustrate the potential consequences of not following these best practices. Go beyond theory and learn practical skills directly applicable to your work: ethical hacking, bug hunting, detection, and mitigation of threats to authentication and authorization functionalities. You'll understand the mechanics and threats of Cross-Site Scripting (XSS) and Injection attacks and comprehend the risks and mitigation strategies associated with XML processing, software uploads, and deserialization.The final portion of this course builds on the previously learned mechanics for building defenses by exploring how design and analysis can be used to build stronger applications from the beginning of the software lifecycle.

Learning Objectives

- Perform hacking and bug hunting in a safe and appropriate manner.
- Identify defect/bug reporting mechanisms within their organizations.
- Setup and use various tools and techniques to determine a web application’s operational environment.
- Setup and use various tools and techniques to enumerate all aspects of a web application and vulnerabilities.
- Work with specific tools for targeted vulnerabilities.
- Determine common mistakes that are made in bug hunting and vulnerability testing.
- Define concepts and terminology behind defensive, secure coding including the phases and goals of a typical exploit.
- Develop an appreciation for the need and value of a multilayered defense in depth.
- Determine potential sources for untrusted data.
- Distinguish the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections.
- Determine the existence of and effectiveness of layered defenses to test web applications with various attack techniques.
- Prevent and defend potential vulnerabilities associated with untrusted data.
- Confirm the vulnerabilities associated with authentication and authorization.
- Detect, attack, and implement defenses for authentication, authorization, functionality and services as well as XSS and Injection attacks.
- Describe the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks.
- Assess the risks associated with XML processing, file uploads, and server-side interpreters and how to best eliminate or mitigate those risks.

- Comprehend the strengths, limitations, and use for tools such as code scanners, dynamic scanners, and web application firewalls (WAFs).
- Apply techniques and measures that can be used to harden web and application servers as well as other components in your infrastructure

Prerequisites

- Basic understanding of web development and web architecture
- Some familiarity with basic programming concepts.
- Basic understanding of web security concepts.

Security Engineering on AWS

AWS-300

View schedule and pricing on cdw.com

Summary

Security Engineering on AWS demonstrates how to efficiently use AWS security services to stay secure in the AWS Cloud, with a focus on recommended security practices for enhancing the security of your data and systems in the cloud. This course highlights the security features of AWS key services including compute, storage, networking, and database services. You will learn how to leverage AWS services and tools for automation, continuous monitoring and logging, and responding to security incidents.

WHO SHOULD ATTEND:

- Security engineers, architects, analysts, and auditors
- Individuals who are responsible for governing, auditing, and testing an organization's IT infrastructure, as well as ensuring conformity of the infrastructure to security, risk, and compliance guidelines

LENGTH: 3 Days

Description

Offered as a private class only.

Security Engineering on AWS will enable you with the skills and knowledge to safeguard your organization's reputation and profits, and improve security operations.
This three-day, intermediate-level course is led by an expert AWS instructor who will guide you through the security practices that AWS recommends for enhancing the security of data and systems in the cloud. You will learn to efficiently use AWS security services including Amazon Security Lake, Amazon Detective, AWS Control Tower, AWS Secrets Manager, Amazon CloudWatch, Amazon GuardDuty, and more for automation, continuous monitoring and logging, and responding to security incidents.

Learning Objectives

- Assimilate and leverage the AWS shared security responsibility model
- Mange user identity and access management in the AWS cloud
- Implement better security controls for your resources in the AWS cloud
- Manage and audit your AWS resources from a security perspective
- Monitor and log access and usage of AWS compute, storage, networking, and database services
- Assimilate and leverage the AWS shared compliance responsibility model
- Identify AWS services and tools to help automate, monitor, and manage security operations on AWS
- Perform security incident management, cloud resiliency, and business continuity in the AWS cloud
- Use AWS security services such as AWS Identity and Access Management, Amazon Virtual Private Cloud, AWS CloudTrail, Amazon CloudWatch, AWS Key Management Service, AWS CloudHSM, AWS Config, AWS Service Catalog, and AWS Trusted Advisor

Prerequisites

- Have attended the AWS Security Fundamentals course
- Experience with governance, risk, compliance regulations, and control objectives
- Working knowledge of IT security practices
- Working knowledge of IT infrastructure concepts
- Familiarity with cloud computing concepts

SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

SFWIPF

View schedule and pricing on cdw.com

Summary

This course shows you how to implement and configure Cisco Secure Firewall Threat Defense for deployment as a next-generation firewall at the internet edge.

WHO SHOULD ATTEND:

- Network security engineers
- Administrators

LENGTH: 5 Days

NOTE: This course is replacing SSNGFW - Securing Networks with Cisco Firepower Next Generation Firewall which is going EoL.

Description

The Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) training shows you how to implement and configure Cisco Secure Firewall Threat Defense for deployment as a next-generation firewall at the internet edge. You'll gain an understanding of Cisco Secure Firewall architecture and deployment, base configuration, packet processing, and advanced options, and conducting Secure Firewall administration troubleshooting.

Learning Objectives

- Describe Cisco Secure Firewall Threat Defense
- Describe Cisco Secure Firewall Threat Defense Deployment Options
- Describe management options for Cisco Secure Firewall Threat Defense
- Configure basic initial settings on Cisco Secure Firewall Threat Defense
- Configure high availability on Cisco Secure Firewall Threat Defense
- Configure basic Network Address Translation on Cisco Secure Firewall Threat Defense
- Describe Cisco Secure Firewall Threat Defense policies and explain how different policies influence packet processing through the device
- Configure Discovery Policy on Cisco Secure Firewall Threat Defense
- Configure and explain prefilter and tunnel rules in the prefilter policy
- Configure an access control policy on Cisco Secure Firewall Threat Defense
- Configure security intelligence on Cisco Secure Firewall Threat Defense
- Configure file policy on Cisco Secure Firewall Threat Defense
- Configure Intrusion Policy on Cisco Secure Firewall Threat Defense
- Perform basic threat analysis using Cisco Secure Firewall Management Center
- Perform basic management and system administration tasks on Cisco Secure Firewall Threat Defense
- Perform basic traffic flow troubleshooting on Cisco Secure Firewall Threat Defense
- Manage Cisco Secure Firewall Threat Defense with Cisco Secure Firewall Threat Defense Manager

Prerequisites

Understanding of the following topics:

- TCP/IP
- Basic routing protocols
- Firewall, VPN, and IPS concepts

SISE - Implementing and Configuring Cisco Identity Services Engine

SISE

View schedule and pricing on cdw.com

Summary

Implementing and Configuring Cisco Identity Services Engine (SISE) teaches how to deploy and use Cisco© Identity Services Engine (ISE) v3.x, an identity, and access control policy platform that simplifies the delivery of consistent, highly secure access control across wired, wireless, and VPN connections.

WHO SHOULD ATTEND:

- Network security engineers
- Network security architects
- ISE administrators
- Senior Security Operations Center (SOC) personnel responsible for Incidence Response
- Cisco integrators and partners

LENGTH: 5 Days

Description

Implementing and Configuring Cisco Identity Services Engine (SISE) v4.0 teaches how to deploy and use Cisco© Identity Services Engine (ISE) v3.x, an identity, and access control policy platform that simplifies the delivery of consistent, highly secure access control across wired, wireless, and VPN connections. This hands-on course provides you with the knowledge and skills to implement and apply Cisco ISE capabilities to support use cases for Zero Trust security posture. These use cases include tasks such as policy enforcement, profiling services, web authentication, guest access services, BYOD, endpoint compliance services, and Terminal Access Controller Access Control Server (TACACS+) device administration.

Through hands-on practice via lab exercises, you will learn how to use Cisco ISE to gain visibility into what is happening in your network, streamline security policy management, and contribute to operational efficiency. This course helps you prepare to take the Implementing and Configuring Cisco Identity Services Engine (300-715 SISE) exam, which leads to CCNP© Security and the Cisco Certified Specialist – Security Identity Management Implementation certifications.

Learning Objectives

- Describe the Cisco Identity Services Engine (ISE)
- Explain Cisco ISE deployment
- Describe Cisco ISE policy enforcement components
- Describe Cisco ISE policy configuration
- Troubleshoot Cisco ISE policy and third-party Network Access Device (NAD) support
- Configure guest access
- Configure hotspots and guest portals
- Describe the Cisco ISE profiler services
- Describe profiling best practices and reporting
- Configure a Cisco ISE BYOD solution
- Configure endpoint compliance
- Configure client posture services
- Configure Cisco ISE device administration
- Describe Cisco ISE TrustSec configurations

Prerequisites

- Familiarity with the Cisco IOS© Software Command-Line Interface (CLI) for wired and wireless devices
- Familiarity with Cisco AnyConnect©_ Secure Mobility Client
- Familiarity with Microsoft Windows operating systems
- Familiarity with 802.1X

SSCP: Systems Security Certified Practitioner

ISC-300

View schedule and pricing on cdw.com

Summary

Earning a globally recognized IT security administration and operations certification like the SSCP is a great way to grow your career and better secure your organization's critical assets.

SSCP certification demonstrates you have the advanced technical skills and knowledge to implement, monitor and administer IT infrastructure using security best practices, policies and procedures established by the cybersecurity experts at ISC2.

WHO SHOULD ATTEND:

- IT administrators, managers, directors and network security professionals responsible for the hands-on operational security of their organization's critical assets.

LENGTH: 5 Days

Description

Offered as a private class only.

The Systems Security Certified Practitioner (SSCP) certification course will prepare you to pass the SSCP exam and become a Systems Security Certified Practitioner. It will provide you with in-depth coverage of the skills and concepts in the seven domains of systems security including: Access Controls, Security Operations and Administration, Risk Identification and Analysis, Incident Response and Recovery, Cryptography, and Network Security.

Learning Objectives

- Compare access control systems and how they should be implemented to protect the system and data using the different levels of confidentiality, integrity, and availability.
- Determine working processes for management and information owners, custodians, and users to ensure proper data classifications are defined.
- Analyze safeguards for mitigating risk and utilize risk identification, monitoring, and analysis domain identities to identify, measure, and control losses associated with adverse events.
- Use consistent approaches and concepts in order to mitigate damages, recover business operations, and avoid critical business interruption, and emergency response and post-disaster recovery in the handling of Incident Response and Recovery.
- Differentiate between key cryptographic concepts and how to apply them, implement secure protocols, key management concepts, key administration and validation, and Public Key Infrastructure as it applies to securing communications in the presence of third parties.
- Identify the Networks and Communications Security needed to secure network structure, data transmission methods, transport formats, and the security measures used to maintain integrity, availability, authentication, and confidentiality of the information being transmitted.
- Define technical and non-technical attacks and the protection need for organizations attacks including concepts in endpoint device security, cloud infrastructure security, securing big data systems, and securing virtual environments.

Prerequisites

- Minimum of one-year cumulative paid work experience in one or more of the seven domains of the SSCP CBK.

Threat Hunting with Python

PY-300

View schedule and pricing on cdw.com

Summary

This intermediate-level course teaches students how to take threat hunting hypotheses generated from contextual data or threat intelligence feeds, and write Python scripts that interact with various data sources.

WHO SHOULD ATTEND:

- Security analysts who want to develop threat hunting skills
- Threat hunters who need to develop custom capabilities beyond their avialable toolset
- Security engineers whoa re responsible for improving detection and monitoring capabilities

LENGTH: 3 Days

Description

Threat Hunting with Python teaches students how to take threat hunting hypotheses generated from contextual data or threat intelligence feeds, and then write Python scripts that interact with various data sources and perform data analytics to determine the validity of those hypotheses. Techniques include the use of advanced data structures, active data gathering using SCAPY and other tools, scripting database or SIEM queries, and more. Successful students will gain the ability to script or automate a variety of custom threat hunting tasks, and speed up their threat hunting processes.

Learning Objectives

- Test cyber threat hunting hypotheses by creating Python scripts that perform data gathering and analytics
- Use advanced data structures to store, search, and manipulate data
- Write Python code to interact with a variety of systems such as SIEM platforms and endpoints, as well as static data sources such as log files and traffic captures
- Increase the speed and effectiveness of cyber threat hunting activities through scripting and automation

Prerequisites

- Intermediate-level programming experience with Python (this is not a course in how to code)
- Successful completion of the Network Forensics and Investigation II course, or comparable experience in security investigations

Related Courses

- Hacker Methodologies for Security Professionals
- Network Forensics and Investigation II
- Endpoint Live Forensics

Understanding Operating Systems

OS-100

View schedule and pricing on cdw.com

Summary

This is a foundational course that exposes students to the underpinnings of modern desktop operating systems and the components that are most vulnerable to attack. This course will provide an essential foundation for courses in malware analysis, intrusion analysis, and penetration testing.

WHO SHOULD ATTEND:

- Those who wish to learn how to analyze components of operating systems.

LENGTH: 5 Days

Description

Understanding Operating Systems is a foundational course that exposes students to the underpinnings of modern desktop operating systems and the components that are most vulnerable to attack. It covers the principles of process, memory, and I/O management that drive all modern operating systems and includes hands-on labs to discover how they are implemented in Microsoft Windows and Linux. After attending this course, you will be able to describe how the components of operating systems work and interact, use built-in tools to analyze these components, and have an excellent foundation for courses in malware analysis, intrusion analysis, and penetration testing.

-

Learning Objectives

- Describe how modern desktop operating systems function
- Explain the principles of process, memory, and I/O management and distinguish the methods used across common operating systems
- Identify and monitor the standard boot processes of Windows and Linux systems
- Use trusted command-line and GUI-based tools to ascertain the status of a running system
- Retrieve and edit a host's network configuration
- Perform basic user and group management tasks
- Describe the foundational security mechanisms in Windows and Linux systems

Prerequisites

- Familiarity with the use of at least one common desktop operating system
- Experience with VMware software is an advantage, but not required

Category: IT and Security Frameworks

Application Security and Development (STIG)

STIG-300

View schedule and pricing on cdw.com

Summary

This is an intermediate-level, lab-intensive, hands-on application security training course essential for developers, designers, architects, QA, Testing, and other personnel who need to deliver secure applications within the Department of Defense.

WHO SHOULD ATTEND:

- Experienced Java developers who wish to get up and running on developing well defended software applications using the STIG guidelines.

LENGTH: 5 Days

Description

Offered as a private class only.

DISA's Application Security and Development STIG, in conjunction with the associated checklist, provides a comprehensive listing of requirements and needs for improving and maintaining the security of software applications and systems within the Department of Defense. This course fills in the context, background, and best practices for fulfilling those requirements and needs. As with all of our courses, we maintain tight synchronization between the latest DISA releases and our materials. A key component to our coverage of DISA's Security Technical Implementation Guides (STIGS), this course is a companion course with several developer-oriented courses and seminars

Application Security and Development (STIG) is a lab-intensive, hands-on application security training course essential for developers, designers, architects, QA, Testing, and other personnel who need to deliver secure applications within the DOD. In addition to teaching basic programming skills, this course digs deep into sound processes and practices that apply to the entire software development lifecycle.

In this course, students thoroughly examine best practices for defensively coding web applications, including XML processing, rich interfaces, and both RESTful and SOAP-based web services. Students will repeatedly attack and then defend various assets associated with fully-functional web applications and web services. This hands-on approach drives home the mechanics of how to secure web applications in the most practical of terms.

Learning Objectives

- Understand potential sources for untrusted data
- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- To test web applications with various attack techniques to determine the existence of and effectiveness of layered defenses
- Prevent and defend the many potential vulnerabilities associated with untrusted data
- Understand the vulnerabilities of associated with authentication and authorization
- To detect, attack, and implement defenses for authentication and authorization functionality and services
- Understand the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks
- To detect, attack, and implement defenses against XSS and Injection attacks
- Understand the concepts and terminology behind defensive, secure, coding
- Understand the use of Threat Modeling as a tool in identifying software vulnerabilities based on realistic threats against meaningful assets
- Perform both static code reviews and dynamic application testing to uncover vulnerabilities in Java-based web applications
- Design and develop strong, robust authentication and authorization implementations within the context of JEE

- Understand the fundamentals of XML Digital Signature and XML Encryption as well as how they are used within the web services arena
- To detect, attack, and implement defenses for both RESTful and SOAP-based web services and functionality
- Understand techniques and measures that can used to harden web and application servers as well as other components in your infrastructure
- Understand and implement the processes and measures associated with the Secure Software Development (SSD)
- Acquire the skills, tools, and best practices for design and code reviews as well as testing initiatives
- Understand the basics of security testing and planning
- Work through a comprehensive testing plan for recognized vulnerabilities and weaknesses

Prerequisites

- Familiarity with Java and JEE is required
- Real-world programming experience is highly recommended
- Ideally students should have approximately 6 months to a year of Java working knowledge.

Certified CMMC Professional (CCP)

CS-200

View schedule and pricing on cdw.com

Summary

The Cybersecurity Maturity Model Certification (CMMC), managed by The Cyber AB (formerly known as the CMMC Accreditation Body or the CMMC-AB), is a program through which an organization's cybersecurity program maturity is measured by their initial and ongoing compliance with applicable cybersecurity practices, as well as their integration of corresponding policies and plans into their overall business operations.

Who Should Attend:

- This course is a prerequisite for the Certified CMMC Professional program, and it prepares students for the Certified CMMC Professional (CCP) certification exam. Students might consider taking this course to learn how to perform CMMC certification readiness checks within their own organization, or as a consultant to other Organizations Seeking Certification (OSC). The CCP certification is also a required step toward becoming a Certified CMMC Assessor (CCA), so students might take this course to begin down the path toward CCA certification.

Length: 5 Days

Description

This course prepares students for the Certified CMMC Professional (CCP) certification, which authorizes the holder to use The Cyber AB Certified CMMC Professional logo, to participate as an Assessment Team Member under the supervision of a Lead Assessor, and to be listed in the CMMC Marketplace. The CCP certification is also prerequisite for the Certified CMMC Assessor (CCA) certification.

Learning Objectives

- Identify the threats to the Defense Supply Chain and the established regulations and standards for managing the risk.
- Identify the sensitive information that needs to be protected within the Defense Supply Chain and how to manage it.
- Describe how the CMMC Model ensures compliance with federal acquisitions regulations.
- Identify responsibilities of the Certified CMMC Professional, including appropriate ethical behavior.
- Establish the Certification and Assessment scope boundaries for evaluating the systems that protect regulated information.
- Prepare the OSC for an Assessment by evaluating readiness.
- Use the CMMC Assessment Guides to determine and assess the Evidence for practices.
- Implement and evaluate practices required to meet CMMC Level 1.
- Identify the practices required to meet CMMC Level 2.
- As a CCP, work through the CMMC Assessment process.

Prerequisites

- Some foundational education or experience in cybersecurity.
- College degree in a cyber or information technical field with 2+ years of experience; or 2+ years of equivalent experience (including military) in a cyber, information technology, or assessment field.

CompTIA A+

TIA-100

View schedule and pricing on cdw.com

Summary

CompTIA's A+ certification is the industry standard for validating the foundational skills needed by today's computer support technicians. Candidates are better prepared to troubleshoot, and problem solve, and technicians better understand a wide variety of issues ranging from networking and operating systems to mobile devices and security. A+ supports the ability to connect users to the data they need to do their jobs regardless of the devices being used.

WHO SHOULD ATTEND:

- Individuals seeking CompTIA A+ certification (220-1001 and 220-1002)

LENGTH: 5 Days

Description

In this course that's focused on CompTIA A+ certification exam preparation, you'll gain the needed knowledge of basic computer hardware and operating systems. You will cover the essential principles of installing, building, upgrading, repairing, configuring, troubleshooting, optimizing, and preventative maintenance on desktop and laptop computers. You will also learn elements of customer service and communication skills necessary to work with clients. Instructor-led practice exams and quizzes help reinforce course concepts and exam readiness. This international vendor-neutral certification requires that you pass two exams: CompTIA A+ Essentials Exam 220-1101 and Practical Application Exam 220-1102. It is also included in the approved list of certifications to meet DoD Directive 8570.1 requirements.

This course includes two exam vouchers.

Learning Objectives

- Install and configure PC system unit components and peripheral devices.
- Install, configure, and troubleshoot display and multimedia devices.
- Install, configure, and troubleshoot storage devices.
- Install, configure, and troubleshoot internal system components.
- Explain network infrastructure concepts.
- Configure and troubleshoot network connections.
- Implement client virtualization.
- Support and troubleshoot laptops.
- Support and troubleshoot mobile devices.
- Support and troubleshoot print devices.
- Support operating systems.
- Install, configure, and maintain operating systems.
- Maintain and troubleshoot Microsoft Windows.
- Configure and troubleshoot network connections.
- Manage users, workstations, and shared resources.
- Implement physical security.
- Secure workstations and data.
- Troubleshoot workstation security issues.
- Support and troubleshoot mobile operating systems and applications.
- Implement operational procedures.

Prerequisites

- End-user skills with Windows-based PCs
- Basic knowledge of computing concepts

Related Courses

- CompTIA Advanced Security Practitioner (CASP+)
- CompTIA Cloud+
- CompTIA Cyber Security Analyst (CySA+)
- CompTIA Network+
- CompTIA PenTest+

Database Security (STIG)

STIG-200

View schedule and pricing on cdw.com

Summary

This is an intense introductory database security training course essential for DBAs, QA, testing, and other personnel who need to deliver secure database applications and manage secure databases within the Department of Defense.

WHO SHOULD ATTEND:

- DBAs
- System Administrators
- Developers
- Enterprise Team Members

LENGTH: 3 Days

Description

Offered as a private class only.

DISA's Database STIG, in conjunction with both generic and product-specific checklists, provides a comprehensive listing of requirements and needs for improving and maintaining the security of Database Management Systems within the Department of Defense. This course fills in the context, background, and best practices for fulfilling those requirements and needs. As with all of our courses, we maintain tight synchronization between the latest DISA releases and our materials. The close ties between this STIG and the Applications Security and Development STIG are reflected in the coverage of application issues within the context of this course. A key component to our coverage of DISA's Security Technical Implementation Guides (STIGS), this course is a companion course with several developer-oriented courses and seminars

Database Security is an intense database security training course essential for DBAs, QA, Testing, and other personnel who need to deliver secure database applications and manage secure databases within the DoD. In addition to teaching basic skills, this course digs deep into sound processes and practices that apply to the entire software development lifecycle. Perhaps just as significantly, students learn about current, real examples that illustrate the potential consequences of not following these best practices.

Data, databases, and related resources are at the heart of the DoD's IT infrastructures, and must be protected accordingly. In this course, students repeatedly attack and then defend various assets associated with a fully-functional database. This approach illustrates the mechanics of how to secure databases in the most practical of terms.

Learning Objectives

- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- Be able to review and test databases to determine the existence of and effectiveness of layered defenses and required checks
- Prevent and defend the many potential vulnerabilities associated with untrusted data
- Understand the concepts and terminology behind supporting, designing, and deploying secure databases
- Appreciate the magnitude of the problems associated with data security and the potential risks associated with those problems
- Understand the currently accepted best practices for supporting the many security needs of databases.
- Understand the vulnerabilities associated with authentication and authorization within the context of databases and database applications
- Understand the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks

- Perform both static reviews and dynamic database testing to uncover vulnerabilities
- Design and develop strong, robust authentication and authorization implementations
- Understand the fundamentals of Encryption as well as how it can be used as part of the defensive infrastructure for data

Prerequisites

- Approximately 6 months to one year of database working knowledge.

HCISPP: HealthCare Information Security and Privacy Practitioner

ISC-204

View schedule and pricing on cdw.com

Summary

The HealthCare Information Security and Privacy Practitioner (HCISPP) educational course are intended to communicate to the audience the basic structure, the essentials of the legal basis, the issues of and the information security and privacy particulars within the described context of the American healthcare delivery system. An integral part of this course is to prepare the attendee (with the required minimum experience) to sit for the (ISC)² HCISPP certification examination.

Description

Offered as a private class only.

Learning Objectives

- Determine the Healthcare environment components, third-party relationships, and foundational health data management concepts.
- Compare information governance frameworks, roles and responsibilities, security, and privacy policies as well as standards and procedures.
- Identify the impact of healthcare information technologies on privacy and security.
- Verify regulatory requirements, regulations and controls and the privacy and security compliance frameworks.
- Define security objectives, attributes, security definitions, concepts and security and privacy governance.
- Verify basic risk management methodologies and the information risk management life cycles.
- Participate in risk assessment consistent with a role in the organization and remediate gaps.
- Identify risk response and control assessment procedures from within organizational risk frameworks as well as continuous monitoring.

Prerequisites

- 5 or more years of professional practice of which 2 should be in a healthcare environment.

Information Assurance (STIG) Overview

STIG-100

View schedule and pricing on cdw.com

Summary

This is a comprehensive two-day course that delves into the realm of Information Assurance, empowering you to enhance your cybersecurity skills, understand the essentials of STIGs, and discover cutting-edge web application security practices.

WHO SHOULD ATTEND:

- IT Professionals
- Developers
- Project Teams
- Technical Leads
- Project Managers
- Testing/QA Personnel
- Key stakeholders such as IT Managers, CISOs and decision-makers

LENGTH: 2 Days

Description

The Information Assurance (STIG) Overview is a comprehensive two-day course that delves into the realm of Information Assurance, empowering you to enhance your cybersecurity skills, understand the essentials of STIGs, and discover cutting-edge web application security practices. This immersive experience is tailored for IT professionals, developers, project teams, technical leads, project managers, testing/QA personnel, and other key stakeholders who seek to expand their knowledge and expertise in the evolving cybersecurity landscape. The course focuses on the intricacies of best practices for design, implementation, and deployment, inspired by the diverse and powerful STIGs, ultimately helping participants become more proficient in application security.

The first half of the course covers the foundations of DISA's Security Technical Implementation Guides (STIGs) and learn the ethical approach to bug hunting, while exploring the language of cybersecurity and dissecting real-life case studies. Our expert instructors will guide you through the importance of respecting privacy, working with bug bounty programs, and avoiding common mistakes in the field.

The next half delves into the core principles of information security and application protection, as you learn how to identify and mitigate authentication failures, SQL injections, and cryptographic vulnerabilities. You'll gain experience with STIG walkthroughs and discover the crucial steps for securing web applications.

Throughout the course, you'll also explore the fundamentals of application security and development, including checklists, common practices, and secure development lifecycle (SDL) processes. You'll learn from recent incidents and acquire actionable strategies to strengthen your project teams and IT organizations. You'll also have the opportunity to explore asset analysis and design review methodologies to ensure your organization is prepared to face future cybersecurity challenges.

Learning Objectives

- Concepts and terminology behind defensive coding
- Threat Modeling as a tool in identifying software vulnerabilities based on realistic threats against meaningful assets
- Entire spectrum of threats and attacks that take place against software applications in today's world
- Role that static code reviews and dynamic application testing to uncover vulnerabilities in applications
- Vulnerabilities of programming languages as well as how to harden installations
- Basics of Cryptography and Encryption and where they fit in the overall security picture
- Requirements and best practices for program management as specified in the STIGS

- Processes and measures associated with the Secure Software Development (SSD)
- Basics of security testing and planning

Prerequisites

- Basic understanding of information security concepts and terminology.
- Familiarity with web application architecture and development.
- Knowledge of networking and web protocols (e.g., HTTP, HTTPS, TCP/IP).
- Experience with programming languages commonly used in web application development, such as JavaScript, Python, Java, or C# would be helpful but not required, as this is not a hands-on class.
- A general understanding of operating systems, databases, and web servers.

ISACA Certified Information Security Manager (CISM)

ISACA-250

View schedule and pricing on cdw.com

Summary

Validate your proficiencies for handling the challenges and responsibilities of a modern IT security manager with a CISM, which focuses on information security governance, information security risk management, information security program development, and incident management. This advanced-level course prepares you for the Certified Information Security Manager® exam.

WHO SHOULD ATTEND:

- Information Security Managers
- Information Security Consultants
- CIOs and CISOs

LENGTH: 3 Days

Description

Certified Information Security Manager® (CISM®) affirms your ability to assess risks, implement effective governance, and proactively respond to incidents. With a highlight on emerging technologies such as AI and blockchain, it guarantees your skillset meets evolving security threats and industry requirements. By addressing top-of-mind concerns like data breaches and ransomware attacks, crucial for IT professionals, this certification ensures you are staying ahead of the pace of change.

Learning Objectives

- Ensure that an enterprise's information is protected
- Have the expertise needed to reduce risk and protect the enterpris
- Design, develop, implement and manage an effective security management program
- Establish and maintain an IT governance framework aligned with business objectives
- Identify and manage information security risks
- Have an understanding of the format and structure of the CISM certification exam
- Have knowledge of the various topics and technical areas covered by the exam
- Practice with specific strategies, tips and techniques for taking and passing the exam

Prerequisites

- 5 years of IT and security experience

ITIL Foundation

ITIL-201

View schedule and pricing on cdw.com

Summary

This course will introduce students to the key components of the ITIL framework. They are the Service Value System and the Four Dimensions model. The purpose of Foundation is to introduce readers to the management of modern IT-enabled services, to provide them with an understanding of the common language and key concepts, and to show them how they can improve their work and the work of their organization with ITIL guidance.

WHO SHOULD ATTEND:

- IT Professionals
- IT Support Staff
- Application, Project, and Business Managers
- Any member of an IT team involved in the delivery of IT Services.

LENGTH: 3 Days

Description

The new ITIL Foundation course will introduce students to the key components of the ITIL framework. They are the Service Value System and the Four Dimensions model. While v3 focused on the 26 processes and functions included in the service lifecycle, ITIL provides a holistic end-to-end picture of what it really means to contribute to business value, and also integrates concepts from models such as Lean IT, Agile and DevOps. The purpose of Foundation is to introduce readers to the management of modern IT-enabled services, to provide them with an understanding of the common language and key concepts, and to show them how they can improve their work and the work of their organization with ITIL guidance.

An exam voucher is included with this course. You may schedule your exam when ready.

Learning Objectives

- Understand the key concepts of service management.
- Understand how the ITIL guiding principles can help an organization adopt and adapt service management.
- Understand the four dimensions of service management.
- Understand the purpose and components of the ITIL service value system.
- Understand the activities of the service value chain, and how they interconnect.
- Know the purpose and key terms of 15 ITIL practices, and details of 7 ITIL practices.
- Prepare for the ITIL 4 Foundation exam.

Prerequisites

- There are no pre-requisites for this course, although a basic knowledge of Service Management concepts will be helpful.

CDW
Education

Part E – Signature Forms

AEPA 025-F
Cyber Security and Training

Instructions

Contained herein are forms that **require a signature** from an authorized person at your company. All items found within this document are **mandatory**. Failure to sign the required areas, sections, or signature lines may lead AEPA to consider your company's proposal as **non-responsive**.

To submit the required signed forms, follow these steps:

1. Read the documents in their entirety.
2. Complete all forms and sign when required.
3. Return the forms and pages in their correct order and scan one (1) single PDF format titled ***"Part E – Signature Forms – Name of Responding Company"*** (i.e. one PDF document for all signature forms).
4. Submit Part E, along with other required documents in Bonfire.

*Note, a solicitation checklist has been provided to review with your submission.

The following sections will need to be completed prior to submission as one (1), single PDF titled "Part E – Signature Forms – Name of Responding Company".

Uniform Guidance "EDGAR" Certification Form – ****signature required***
Solicitation Affidavit – ****signature required***
Acceptance of Solicitation & Contract – ****signature required***

Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7. Clean Air Act and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended, contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein.		
Respondent Certification (By Item)	**Respondent Certification:** **YES**, I agree	**Initial**
1. Violation of Contract Terms and Conditions	Yes	DB
2. Termination for Cause of Convenience	Yes	DB
3. Equal Employment Opportunity	Yes	DB
4. Davis-Bacon Act	Yes	DB
5. Contract Work Hours and Safety Standards Act	Yes	DB
6. Right to Inventions Made Under a Contract or Agreement	Yes	DB
7. Clean Air Act and Federal Water Pollution Control Act	Yes	DB
8. Debarment and Suspension	Yes	DB
9. Byrd Anti-Lobbying Amendment	Yes	DB
10. Procurement of Recovered Materials	Yes	DB
11. Profit as a Separate Element of Price	Yes	DB
12. General Compliance with Participating Agencies	Yes	DB
13. Governing Law; Forum Selection.	Yes	DB

CDW Government LLC
Name of Business


Signature of Authorized Representative

Dario Bertocchi
Printed Name

9/16/24
Date

Solicitation Affidavit

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

Dario Bertocchi	230 N. Milwaukee Avenue
Authorized Representative (Please print or type)	Mailing Address
VP Contracting Operations	Vernon Hills, IL 60061
Title (Please print or type)	City, State, Zip
	9/16/24
Signature of Authorized Representative	Date

Acceptance of Solicitation & Contract

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	CDW Government LLC	**Date**	9/16/24
Address	230 N. Milwaukee Avenue	**City, State Zip**	Vernon Hills, IL 60061
Contact Person	Stephanie Kessler	**Title**	Deputy Program Manager
Authorized Signature		**Title**	VP Contracting Operations
Email	dariber@cdw.com	**Phone**	203.851.7049

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Solicitation Checklist

Instructions: Utilize the checklist below, reviewing to confirm that all the required documents have been uploaded to Public Purchase, in their ***specified/required format***, by the due date and time listed for this solicitation. ***Submissions not following the specified/required format may result in being marked non-responsive and may not be considered for evaluation.*** Respondents are reminded that failure to follow, comply with, and adhere to the enclosed instructions of this solicitation may result in their response being deemed non-responsive. AEPA, its Member Agencies, affiliate agencies, and authorized representatives are not responsible for bid proposals that are incomplete, unreadable, or received after the solicitation deadline submission date.

"x"	**Document Title, Uploaded to Bonfire** *(Respondent must submit documents in the required title/format)*	**Format of Uploaded Document**	**Notes**
	Bid Bond – if Required, see Part A if applicable.	Upload PDF copy of the bid security.	The original bid security must be received by Lakes Country Service Cooperative by due date and time.
	Part C – State-Specific Forms – ***Name of Responding Company***	Single, Scanned PDF	**New Jersey Only Requirement.** Signatures Required.
	Part D - Questionnaire – ***Name of Responding Company*** Includes: ● Company Information ● Service Questionnaire ● Exceptions ● Deviations	Single, Scanned PDF	**Required.**
	Part E – Signature Forms – ***Name of Responding Company*** Includes: ● Uniform Guidance "EDGAR" Certification ● Solicitation Affidavit ● Acceptance of Solicitation & Contract	Single, Scanned PDF	**Required.** Signatures required.
	Part F – Pricing Schedule – ***Name of Responding Company***	Excel Workbook	**Required.**
	Price List and/or Catalog – ***Name of Responding Company***	Upload PDF	**Required.**
	Exhibit A – Marketing Plan – ***Name of Responding Company***	Scanned PDF	**Optional.** Form not provided by AEPA, Respondent Created

Contents

1-Xpel- AEPA Go to Marketing Plan E F 1
1-Xpel Flyer Cybersecurity Solutions web (1) (4) 9
2-Xpel Assessment Flyer 11
3-AEPA Xpel 2024 Presentation 12
Slide Number 1 12
Slide Number 2 13
Slide Number 3 14
Slide Number 4 15
Slide Number 5 16
Slide Number 6 17
Slide Number 7 18
Slide Number 8 19
Slide Number 9 20
Slide Number 10 21
Slide Number 11 22
Slide Number 12 23
Slide Number 13 24
Slide Number 14 25
Slide Number 15 26
Slide Number 16 27
Slide Number 17 28
Slide Number 18 29
Slide Number 19 30
Slide Number 20 31
Slide Number 21 32
Slide Number 22 33
Slide Number 23 34
Slide Number 24 35
Slide Number 25 36
Slide Number 26 37
Slide Number 27 38
Slide Number 28 39
Slide Number 29 40
Slide Number 30 41
Slide Number 31 42

Slide Number 32 43
Slide Number 33 44
Slide Number 34 45
Slide Number 35 46
Slide Number 36 47
Slide Number 37 48
Slide Number 38 49
Slide Number 39 50
Slide Number 40 51
Slide Number 41 52
Slide Number 42 53
4-Xpel Flyer Suite 3 3824 (1) (3) 54
5-Xpel 2024 Presentation Training 56
6-Xpel Essentials Quote Flyer-SLCGP (1) (3) 150
7-Corporate Technology Certifications 152
8-Cybersecurity References 154
1-(Amd) Forward Edge Amended Part E - Signature Forms - signed -9-30-2 156
2-Uniform Guidance Edgar Part F 164

Vision Forward and Forward Edge Go-to-Market Strategy for AEPA Cooperative Contract

Solicitation Category - E: Security Solutions

Regions 3: East North Central, Region 4: West North Central, Region 5: South Atlantic

Introduction

In response to the AEPA Solicitation Category E, Forward Edge can provide a complete suite of security solutions, including video surveillance, access control, and designing network security, addressing the diverse needs of educational institutions. Forward Edge is a leading K-12 technology solutions provider in Ohio, dedicated to empowering schools to reach tomorrow's learners. With a commitment to delivering cutting-edge solutions and services, Forward Edge is focused on helping educational institutions thrive in the digital age, enabling students to succeed in an increasingly technology-driven world. As a trusted partner, Forward Edge offers a range of technology solutions that are designed to enhance the learning experience and promote academic success.

The Marketing strategy will be multi-faceted and span various channels to reach key decision-makers within AEPA member agencies and their participating entities. We will highlight our commitment to being a partner for educational institutions and our unique ability to tailor solutions to the diverse needs of districts.

Contract Launch and Ongoing Communications

- **Targeted Launch Announcements:** Initiate the contract with targeted announcements to current agency partners and potential customers within the AEPA network. Utilize email campaigns, social media posts, and press releases emphasizing the benefits of the contract, including streamlined procurement and cost savings.
    - Tactics we will employ to communicate our contract include:
        - Targeted Email campaign with 3 emails
            - 1 email highlighting Forward Edge's value proposition
            - 1 email highlighting testimonials and case studies from current customers
            - 1 email highlighting commitment to compliance and relevant regulations, while highlighting any potential grant opportunities to aid in purchasing
        - Social media engagement -
            - Following and engaging with AEPA members
            - Promote Forward Edge's presence at industry events (*see event list below*)
        - Issue a Co-Branded Press Release to AEPA members and post on Forward Edge's blog page
- **Dedicated AEPA Landing Page:**
    - Dedicated landing page on Forward Edge's website showcasing the AEPA partnership, contract details, and key benefits. Include clear calls to action,

such as "Contact Us for AEPA Pricing" or "Request a Demo."

- **AEPA State Lead Agency Collaboration:**
    - Graphic and content support from the Forward Edge Marketing Team
        - Co-branded flyers and social media posts
        - Newsletter content and write-ups
        - Talking points about key benefits of our security solutions

Key Messaging Points

Our approach to designing security solutions for districts focuses on proactive threat detection and prevention, empowering educational institutions to create safe and secure learning environments. Key considerations for choosing Forward Edge include:

- Comprehensive security solutions
- Compliance and data protection
- Scalability and flexibility
- Experience and flexibility
- Multi-state Service Capabilities

Marketing and Promotion

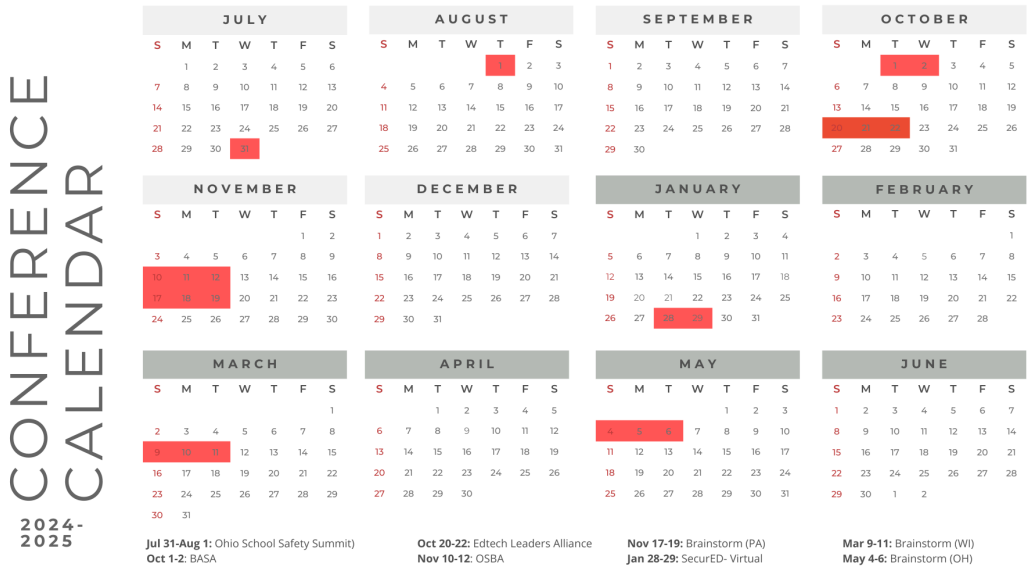
- **Digital Marketing and Email Campaigns:** Produce ads, email marketing campaigns and other digital marketing channels like social media with co-branded content highlighting contract details. Utilize engaging visuals and concise messaging to capture attention and drive interest.
    - Email campaigns highlighting grant funding and resources available for Security upgrades (example)
    - Dedicated email blast to members and prospective members with clear and concise information on how to procure Forward Edge solutions through the AEPA contract

- **Search Engine Optimization (SEO)**: Optimize Forward Edge's website and online content for relevant keywords to improve visibility in search engine results and attract organic traffic.

- **Trade Shows and Events:** Implement indirect marketing tactics to enhance brand awareness and reach a broader audience, including thought leadership articles, webinars, and participation in relevant industry events.
    - Current and proposed schedule of Trade show events to reach audiences Nationwide:
        - FETC (Florida)
        - OETC (Ohio)
        - Edtech Leaders Alliance (Ohio)
        - OSBA (Ohio)
        - Brainstorm (Pennsylvania, Wisconsin and Ohio)
        - SecureED (Illinois)
        - COSN
        - TAI (Iowa)

    - NETA (Nebraska)
    - GaETC (Georgia)
- Schedule of tradeshows with sponsorships secured -





-
- Leverage Forward Edge Critical Manufacturer Partnerships
    - Highlight our stack of solutions
    - Sales SPIFFS
    - Co-Presentations and Event Sponsorships

- Hosting Instructional Webinars and Networking Events for AEPA members
    - Technology Lunch & Learns

Details on Dedicated Landing Page for AEPA Contract

- **Prominent AEPA Contract Display:** Feature the AEPA contract prominently on the Forward Edge website, including a dedicated section with relevant information and resources. Ensure easy navigation and clear calls to action.
- **Success Stories:** Showcase testimonials and case studies from educational institutions benefiting from Forward Edge's solutions, particularly those procured through the AEPA contract.

Measurement and Optimization

Forward Edge has the capability and resources to track key performance indicators such as website traffic, lead generation, email opens and clicks, and social media engagement to measure the effectiveness of the marketing strategy outlined in this plan. We will analyse the data on a quarterly basis and made adjustments as needed to ensure we're reaching the right audience with correct messaging.

Conclusion

The AEPA cooperative contract offers a strategic pathway to strengthen Forward Edge's presence in the education sector, specifically in regards to security offerings to Regions 3,4, and 5. By implementing this go-to-market strategy, we can maximize the contract's potential, fostering strong relationships with AEPA agencies, and empowering educational institutions to safeguard their digital environments with confidence. Out plan leverages a variety of tactics to build awareness, generate new leads and ultimately drive sales.

Xpel Forward Go-to-Market Strategy for AEPA Cooperative Contract

Solicitation Category - F: Cybersecurity and Training

Introduction

The AEPA cooperative contract represents a powerful opportunity to expand Xpel's reach and impact within the education sector. This strategy outlines a comprehensive approach to leverage the contract, ensuring maximum visibility and engagement among current and potential agencies. Xpel is positioned to address the needs outlined in the AEPA RFP, offering a K-12 specific cybersecurity suite of solutions to members. Our approach focuses on proactive threat detection and prevention, empowering educational institutions to create safe and secure learning environments.

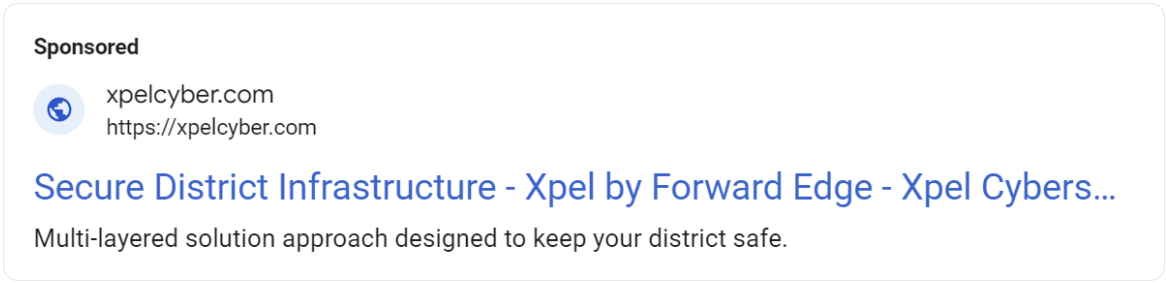
The Marketing strategy will be multi-faceted and span various channels in order to reach key decision-makers within AEPA member agencies and their participating entities. We will highlight our commitment to being a partner for educational institutions and our unique ability to tailor solutions to the diverse needs of districts.

Contract Launch and Ongoing Communications

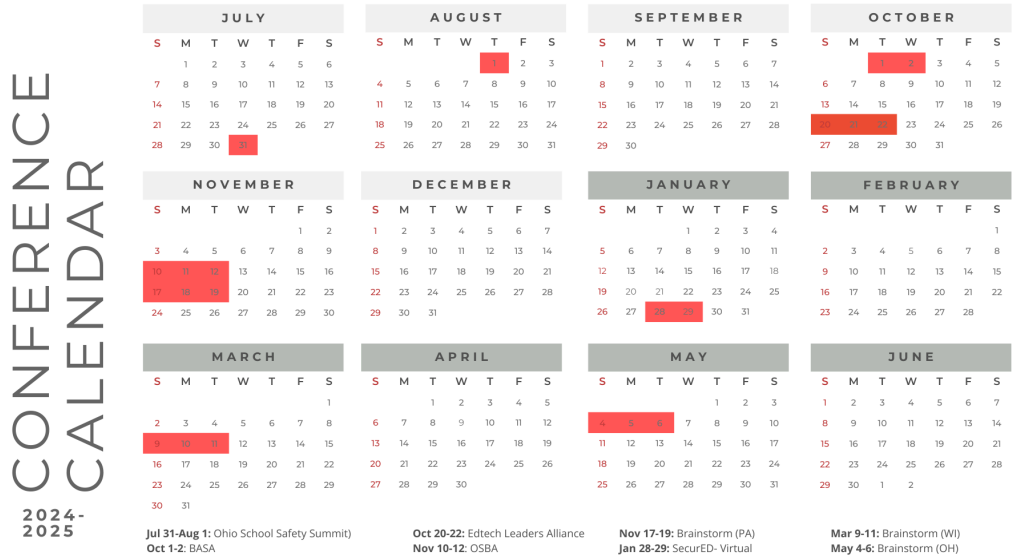
- **Targeted Launch Announcements:** Initiate the contract with targeted announcements to current agency partners and potential customers within the AEPA network. Utilize email campaigns, social media posts, and press releases emphasizing the benefits of the contract, including streamlined procurement and cost savings.
    - Tactics we will employ to communicate our contract include:
        - Targeted Email campaign with 3 emails
            - 1 email highlighting Xpel's value proposition
            - 1 email highlighting testimonials and case studies from current customers
            - 1 email highlighting how members can purchase and walking them through the process
        - Social media engagement -
            - Following and engaging with AEPA members
            - Promote Xpel's presence at industry events (*see event list below*)
        - Issue a Co-Branded Press Release to AEPA members and post on Xpel's blog page
- **Dedicated AEPA Landing Page:**
    - Dedicated landing page on Xpel's website showcasing the AEPA partnership, contract details, and key benefits. Include clear calls to action, such as "Contact Us for AEPA Pricing" or "Request a Demo."
- **AEPA State Lead Agency Collaboration:**
    - Graphic and content support from the Forward Edge Marketing Team
        - Co-branded flyers and social media posts
        - Newsletter content and write-ups on Xpel
        - Talking points about key benefits of Xpel

Marketing and Promotion

- **Digital Marketing and Email Campaigns:** Produce ads, email marketing campaigns and other digital marketing channels like social media with co-branded content highlighting contract details. Utilize engaging visuals and concise messaging to capture attention and drive interest.
    - Email campaigns highlighting grant funding and resources available for Cybersecurity (example)
    - Online Ads highlighting solution and AEPA contract details



- **Trade Shows and Events:** Implement indirect marketing tactics to enhance brand awareness and reach a broader audience, including thought leadership articles, webinars, and participation in relevant industry events.
    - Current and proposed schedule of Trade show events to reach audiences Nationwide:
        - FETC (Florida)
        - OSSS (Ohio)
        - BASA (Ohio)
        - Edtech Leaders Alliance (Ohio)
        - OSBA (Ohio)
        - Brainstorm (Pennsylvannia, Wisconsin and Ohio)
        - SecureED - IL
        - NICE (Texas)
        - National K-12 Cybersecurity Leadership Conference (Georgia)
        - IEI National and Regional Conferences (Nationwide)
    - Schedule of tradeshows with sponsorships secured -



    -
    - Leverage Xpel and Forward Edge Critical Manufacturer Partnerships
        - Sales SPIFFS
        - Co-Presentations and Event Sponsorships
- Hosting Instructional Webinars for AEPA members
    - Technology Lunch & Learns on Cybersecurity
        - Topics include: Life of a Cyber Alert, How does your Cyber Stack, stack up?
- Cybersecurity Awareness Training Videos
    - Cyber Awareness Training Videos

Details on Dedicated Landing Page for AEPA Contract

- **Prominent AEPA Contract Display:** Feature the AEPA contract prominently on the Xpel website, including a dedicated section with relevant information and resources. Ensure easy navigation and clear calls to action.
- **Success Stories:** Showcase testimonials and case studies from educational institutions benefiting from Xpel's cybersecurity solutions, particularly those procured through the AEPA contract.

Measurement and Optimization

Xpel by Forward Edge has the capability and resources to track key performance indicators such as website traffic, lead generation, email opens and clicks, and social media engagement to measure the effectiveness of the marketing strategy outlined in this plan. We will analyse the data on a quarterly basis and made adjustments as needed to ensure we're reaching the right audience with correct messaging.

Conclusion

The AEPA cooperative contract offers a strategic pathway to strengthen Xpel's presence in

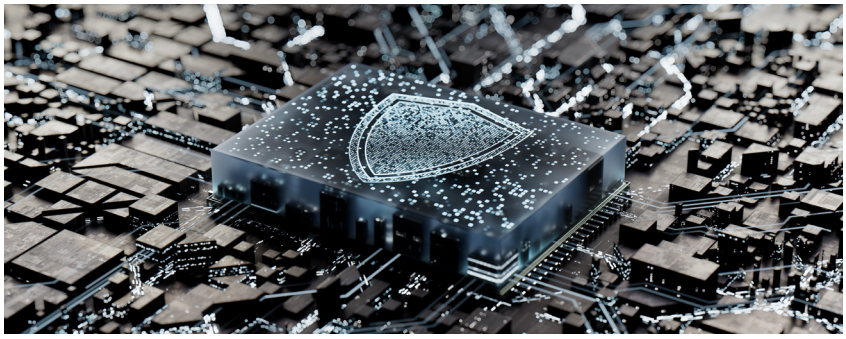
the education sector. By implementing this go-to-market strategy, we can maximize the contract's potential, fostering strong relationships with AEPA agencies, and empowering educational institutions to safeguard their digital environments with confidence. Our plan leverages a variety of tactics to build awareness, generate new leads and ultimately drive sales.

xpel by Forward Edge

Managed Cybersecurity Solutions

Don't dismiss cyberthreats. Dismantle them.

Navigate cybersecurity challenges with the advantage of Xpel by Forward Edge, the emerging leader in next-generation cybersecurity solutions designed specifically for the K-12 environment. Xpel by Forward Edge safeguards your district with intelligence driven strategies.



Our Solutions

Managed Cybersecurity

Security Engineering Solutions

vCISO and Security Training

Next-Level Alignment for Unmatched Defense in Depth

The security professionals at Xpel by Forward Edge understand the critical importance of cybersecurity in the education sector, especially in K-12 districts where young learners and sensitive data are involved. Our strategy isn't just proactive; it's a step ahead —meticulously engineered to align with the industry's gold standards, the NIST and CIS cybersecurity frameworks.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

CIS. Center for Internet Security®

A Layered Approach to Cybersecurity

Transform your district's cybersecurity posture with next generation solutions designed to address the increasing threat to school finances, sensitive data and operational and instructional integrity.

Our Solutions Protect, Detect, and Respond.



> "Our district has taken measures to reduce our exposure to cyber threats this year through the deployment of Xpel's Managed Cybersecurity Solutions. With 24/7 event log monitoring, analysis, and alerting, vulnerability scanning, and anti-phishing education for our staff, they've helped us improve our overall cyber security posture."

-DIRECTOR OF TECHNOLOGY OF AN OHIO CAREER CENTER, 2023

xpel by Forward Edge

xpelcyber.com
513.761.3343

Schedule a Meeting Today
or go to: **qrfy.com/r/schedule**

Xpel by Forward Edge Cybersecurity Assessment

Xpel by Forward Edge provides a comprehensive 5-part Assessment of your cybersecurity posture, with a roadmap containing reporting, recommendations, actionable next steps, and a post-assessment review of findings.



Proctored Assessment



Vulnerability Scan



Dark Web Monitoring



Phishing Campaign

Proctored Assessment: The assessment is an exhaustive, proctored deep-dive into your organization, designed to reveal district-wide potential security vulnerabilities across eighteen risk categories of potential exposure.

Dark Web Scan: The Dark Web Scan is conducted against the relevant domain(s), it is an identity theft prevention tool that identifies compromised domain information on the Dark Web.

Phishing Campaign: This campaign provides data on which employees have been baited by the phishing email and highlights the Customer-specific need for security awareness training to identify suspicious emails and apply security awareness best practices.

Vulnerability Scan: The Vulnerability Scan detects and classifies exposed entry points into networks and systems on which cyber attackers capitalize by scanning for known threats, out-of-date hardware, software and other appliances.

Findings Review: Forward Edge will meet with Customers and review findings from above four cybersecurity posture analysis assessments and provide reporting and recommendations.

Schedule Your Assessment >

qrfy.com/r/schedule



Managed Cybersecurity

Scalable, Lasting Solutions with Education in Mind

Partner Managed Services

Managed Network Engineering Services provides your District the confidence that a proactive and well-maintained systems maintenance process is in place.

Curriculum & Technology Integration

Former educators and technology integration coaches bring a suite of professional learning services including coaching, assessments micro credentialing, bootcamps and more.

Managed Cybersecurity

Improve your District's cybersecurity posture with our suite of Next Generation technology tools to significantly mitigate risk.

xpel by Forward Edge

Architectural Technology Designer

Technology Designer that provides reliable, efficient, and future-proofing K-12 technology solutions and planning.

On-Site Services

Experienced desktop engineers provide daily technology support for Districts, helping to strategize project implementation, planning and completion.

Cabling Solutions

End-to-end Flexible cabling solutions that anticipate new technologies and ensure technology is effectively integrated into Districts.

Xpel Cybersecurity Suite

Managed Cybersecurity

- **EDR**
  Endpoint Detection & Response
- **SIEM**
  Security Information Event Management - Log Analytics
- **Vulnerability Management**
  Internal & External Scanning/ Cumulative Actionable Reporting
- **IDS/IPS**
  Intrusion Detection & Prevention Solutions
- **Dark Web Monitoring**
  Continuous Domain Monitoring
- **Phishing Threat Simulations**
  Real Time Security Training
- **vCISO**
  Virtual Chief Information Security Officer
- **User Awareness Training**
  Security Training Modules Designed for K-12 Audiences
- **SOC Monitoring**
  24/7/365 Eyes-on-Glass Security Operations Center Monitoring

vCISO

- NIST/CIS Security Framework Alignment - Policy Support
- Incident Response Playbook Development
- Data Privacy Compliance
- **Security Assessment**
  Comprehensive Organizational Cybersecurity Analysis - 18 Critical Risk Categories
- **Network Audit**
  Comprehensive Analysis of IT Infrastructure
- **Penetration Testing:**
  Internal and External
- **Strategic Planning**
  Lifecycle Management & Fiscal Forecasting

Security Training

- Security Awareness Training
- Professional Development
- Phishing Threat Simulations
- Tabletop Exercises

Engineering Solutions

- Backup Solutions
- Firewall Solutions
- Authentication Solutions
- Vulnerability Management
- Network Asset Discovery
- Incident Response / Forensics / Recovery
- Project Based Engineering Support

Physical Security

- Video Surveillance
- Access Control

Engineering Solutions

- Backup Solutions
- Firewall Solutions
- Vulnerability Management
- Network Asset Discovery
- Incident Response / Forensics / Recovery
- Project Based Level I - Level III Support

Physical Security

- Video Surveillance
- Access Control

Awards we've earned along the way.

Cooperative Purchasing Contract Awards

BuyBoard® National Purchasing Cooperative

equalis GROUP

Supporting District Administration:

Cyber Liability Insurance

Federal & State Data Privacy

General Compliance

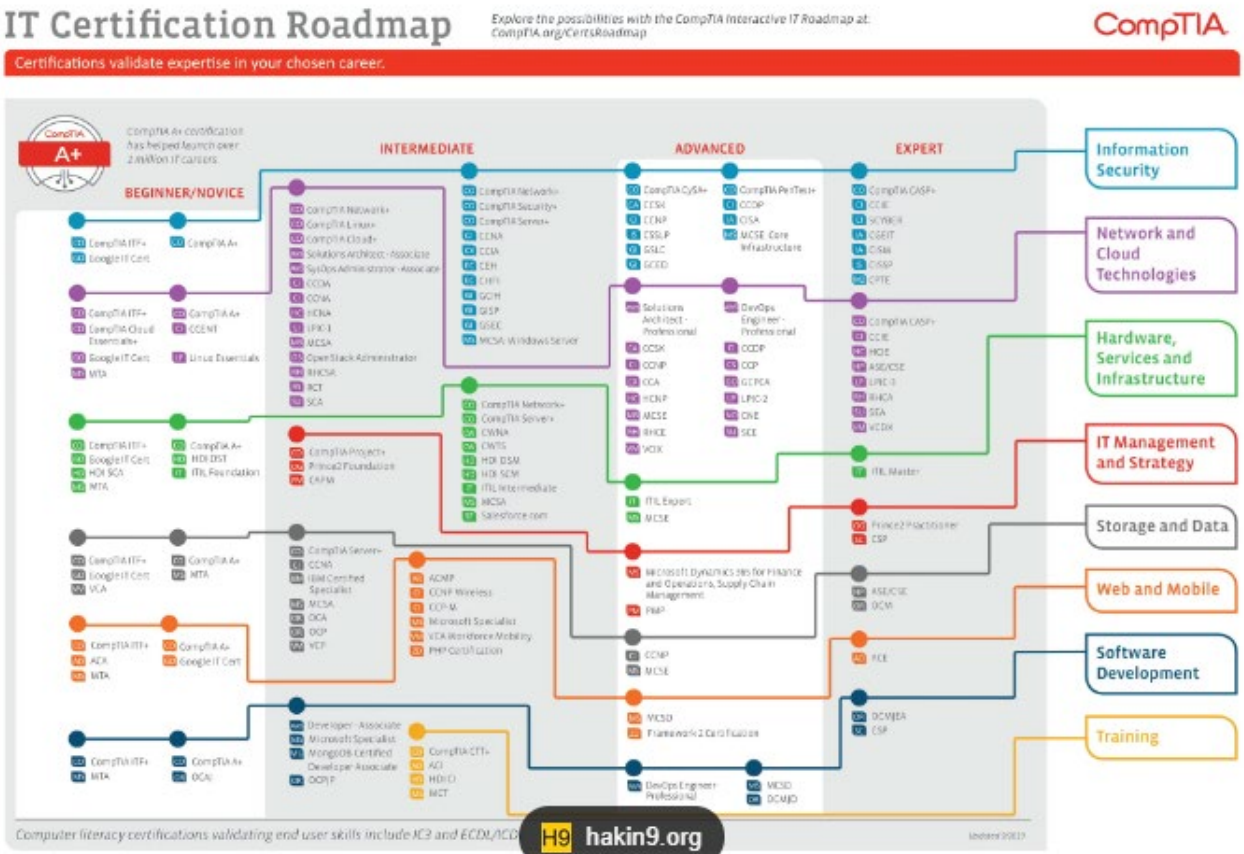
Securing K-12 Technology Environments from:

Ransomware & Funds Transfer Fraud

Theft of District PII & Sensitive Data

Disruption to the Operational, Administrative & Instructional Access to Technology Tools

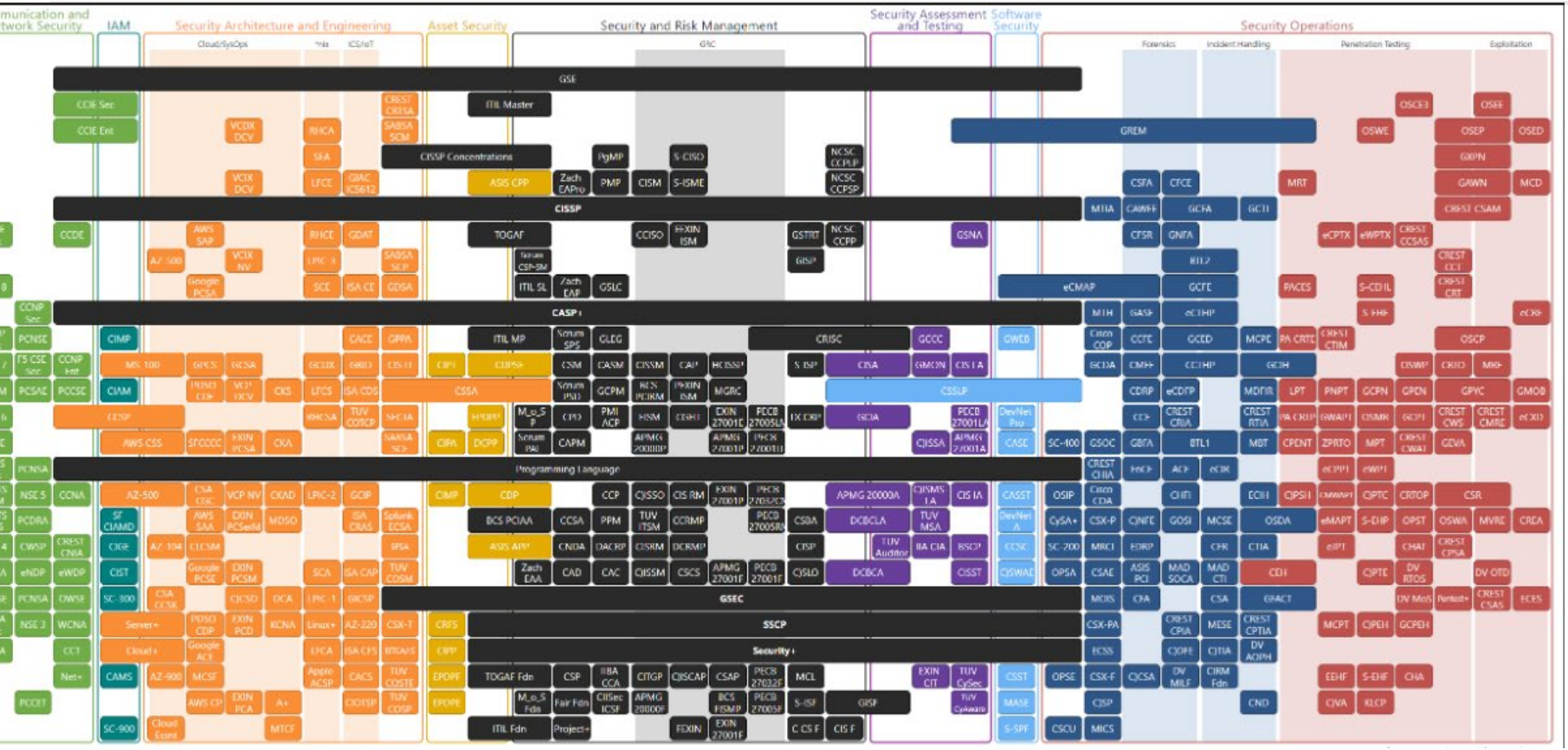




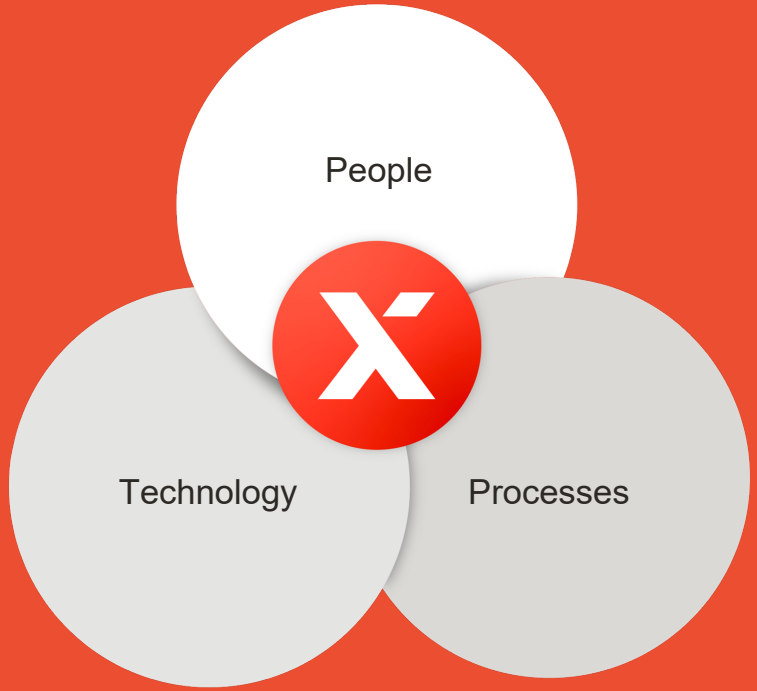
H9 hakin9.org

xpel
by Forward Edge

Cybersecurity - A Distinct Engineering Discipline
437 Certifications



Complete Cybersecurity Suite for K-12 Education.



xpel
by Forward Edge

Follow the Framework:

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CIS. Center for Internet Security®



Cybersecurity Professionals are in Demand Nationwide

Estimated 3.5 Million Unfilled Cybersecurity Jobs through 2025

-eSentire 2023 Official Cybersecurity Jobs Report

Cybersecurity Engineer Annual Salary

$122,140

K-12 Tech Director Annual Salary

$82,310

Nationwide Averages - ZipRecruiter 1/2024



Common Security Controls at K12 School Districts

- Partial Security Controls
- Backups & Testing
- Firewalls
- Patches & Fixes
- Segmentation

Continued Challenges for K12 School Districts

- Can't Hire/ Afford Cyber Engineer
- Active Monitoring 24/7
- Time to Evaluate & Implement Cyber Tools
- Continuous Investment in Dynamic Requirements
- Develop Training Plans for Teachers & Staff to Decrease Exposure to Cyber Threats
- Incident Response Resources

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/ 7/ 365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR

SIEM

24/7/365 SOC MONITORING

VULNERABILITY MANAGEMENT

DARK WEB MONITORING

INTRUSION DETECTION AND PREVENTION

RISK ASSESSMENT

SECURITY TRAINING

vCISO

Servers
Critical Workstations

SentinelOne

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR

SIEM

24/7/365 SOC MONITORING

VULNERABILITY MANAGEMENT

DARK WEB MONITORING

INTRUSION DETECTION AND PREVENTION

RISK ASSESSMENT

SECURITY TRAINING

vCISO

Core

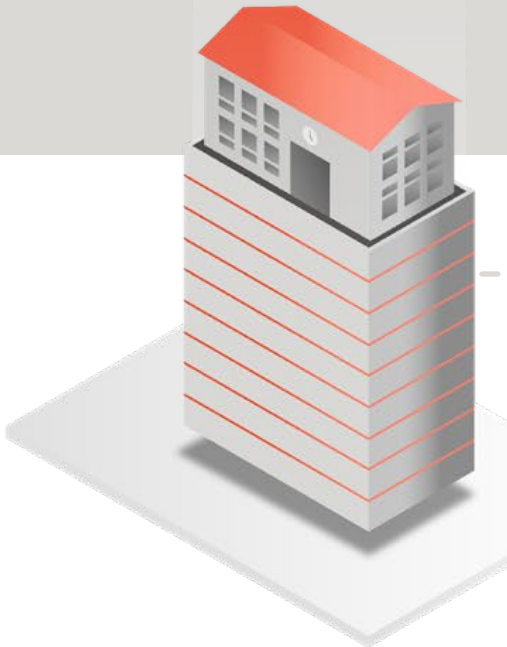
vCenter/ESXi

Servers & Workstations

Firewall

CONNECTWISE

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

xpel
by Forward Edge

24/7 SOC Certifications





















Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

Internal & External Scanning
Cumulative Reporting

Qualys.

Our Advanced Cyber Defense for Education Stack

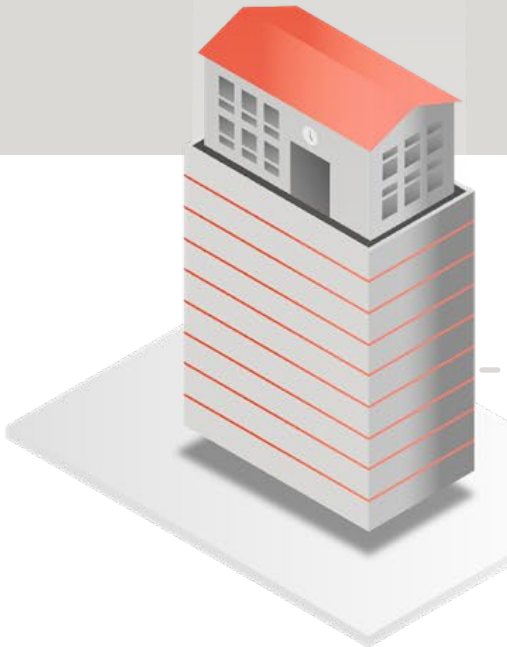


EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

Continuous
Domain Monitoring

CONNECTWISE

Our Advanced Cyber Defense for Education Stack



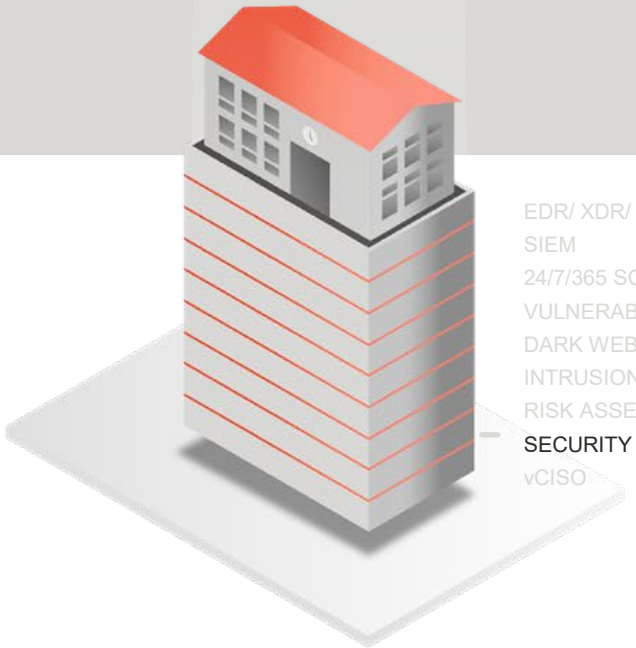
EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT — 18 Risk Categories
SECURITY TRAINING
vCISO

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

Phishing Threat Simulations and User Awareness Training

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

Security Policy Support for District Administration & IT

SOC Security Operations Center

24/7 Monitoring

What is it?

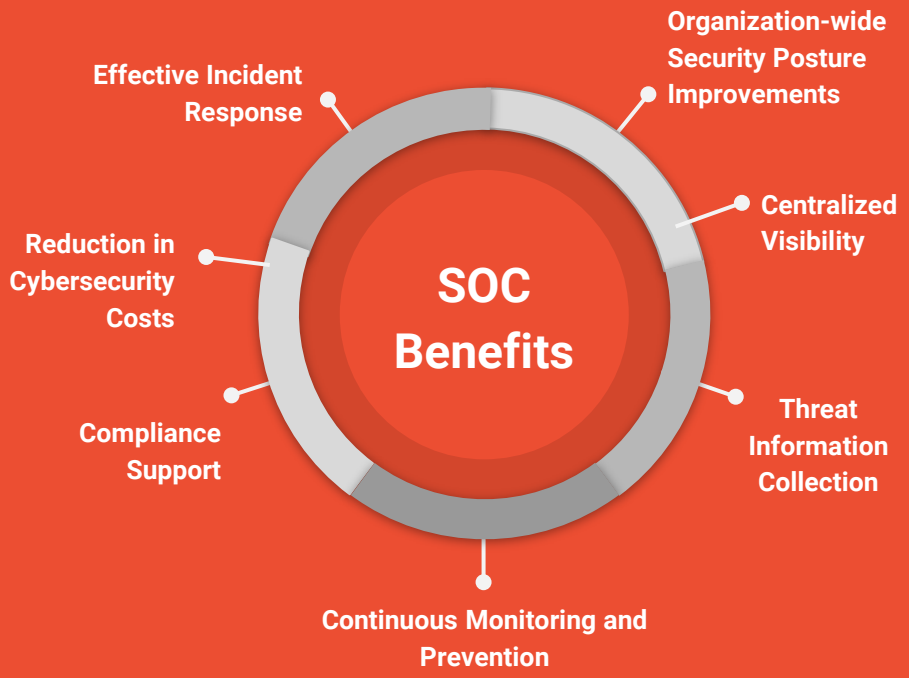
Simply put, a security operations center (SOC – pronounced “sock”) is a team of experts that proactively monitor an organization’s ability to operate securely. Members of a SOC team are responsible for a variety of activities, including proactive monitoring, incident response and recovery, remediation activities, compliance, and coordination and context.

Benefits

- Combines Automation with Human Resources to Threat Response
- Allows Centralized Organization-Wide Visibility
- Gain Transparency and Control on Security
- Improve Incident Response Times
- Reduces Impact of a Breach
- Improve Management Practices Post Incident

SOC Security Operations Center

24/7 Monitoring



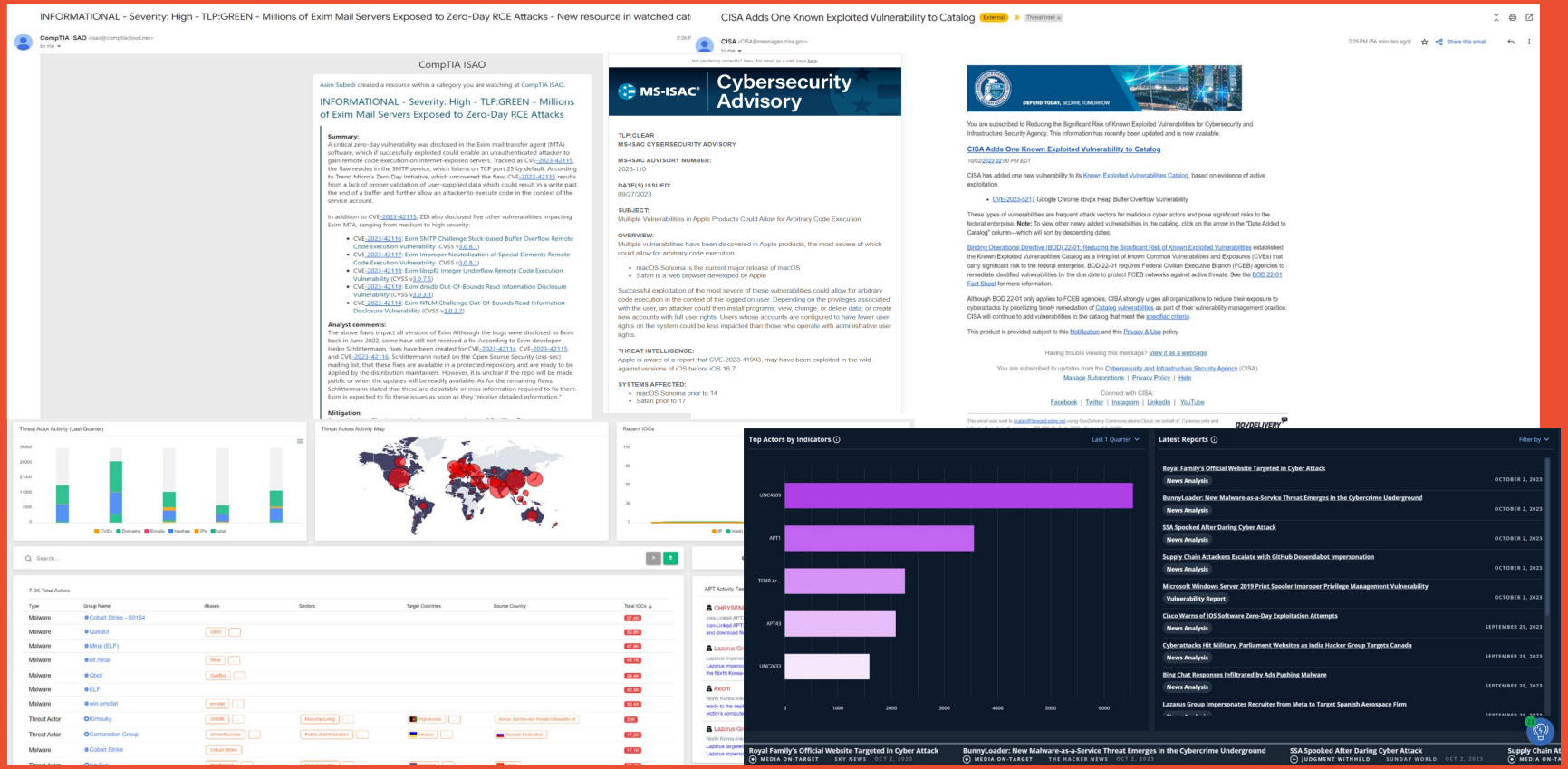
The Xpel Security Operations Center

Additional Benefits

Benefits of the Xpel SOC

- Continuous Monitoring and Prevention 24/7/365
- Access to K-12 Security Analysts adding a vital human intelligence to security tools.
- Improved MTTD/MTTR
- Hyper Focus on K-12 Environments - Crowdsourcing of Alerts
- Reduction of False Positive Alert Fatigue - Intelligence-Driven Noise Reduction
- True Positives Identification Efficiencies - Custom threat indicators designed to specifically address K-12 Environments
- High Value Detections - Over 60% of alerts identified by Xpel SOC are internally generated

Threat Intelligence



vCISO
virtual Chief Information Security Officer

Strategic Planning and Annual CSR

Lifecycle Management & Fiscal Forecasting

NIST/CIS Alignment - Policy Support

Incident Response Playbook Development

Data Privacy Compliance

Security Assessment

Comprehensive Analysis of Organizations Cybersecurity Posture - 18 Critical Risk Categories

Network Audit

Comprehensive Analysis of IT infrastructure
Penetration Testing: Internal & External

NIST / CIS Alignment - Security Policy Support

Development of Security Policy and Procedures Best Practices that will contribute to a continually improving cybersecurity posture designed to meet the goals of the first implementation group of the Center for Internet Security (CIS) controls.

Policy List

- Change Management
- Cloud Computing
- Code of Ethics
- Data Access and Password
- Data Classification
- Data Retention
- Encryption
- Facility Security
- HR Corrective Action
- Human Resource Security
- Information Security
- Information Security Risk Assessment
- Interconnection Agreement
- Logging and Monitoring
- Perimeter Security and Administrative
- Policy of Standard Exception Request Form
- Policy of Standard Exception Request Procedure
- Policy of Standard Variance
- Security Incident Response
- Service Provider Security
- Social Media
- Software Development
- System Configuration
- Telecommuting
- Vulnerability Identification
- System Updates

vCISO
virtual Chief Information Security Officer



Security Assessment

Comprehensive analysis of district-wide cybersecurity posture designed for K-12 environments.

18 Critical Risk Categories

- Inventory
- Endpoint Security
- Software
- Account Security
- Network Security
- Banking
- Antivirus
- Firewall
- Content Filter
- Backups
- Maintenance
- Data
- Authentication
- Closet Security
- Training
- Policy
- Assessment
- Insurance

Security Focused Training

The Xpel Cyber Hub is a one-stop shop for all your cyber training needs.

Click the links to check out the Cyber Hub as well as our overview video on how to use the Cyber Hub.

Cyber Hub Portal →

Cyber Hub Video →



Security Awareness Training



Professional Development

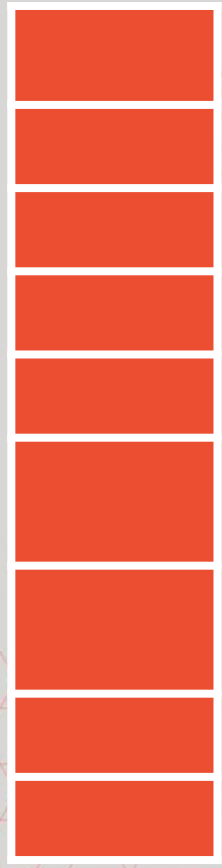


Phishing Threat Simulations



Tabletop Exercises

Realistic intent scenarios to test Incident Response Teams



Windows/ Mac/ Linux Servers (Virtual and Physical)

vCenter / ESXi Servers

Firewall - In District

Core Switches (Routing Enabled)

Superintendent Suite - Laptops/ Desktops

Treasury Suite / Business Manager - Laptops/ Desktops

Other Admin Staff (Secretary/ Principal/ Nurse/ IT Department)

Total Staff Email Account (All but Students)

*Physical Vulnerability Scanner Required

Learn More About Our Solutions

“[Insert Testimonial]”

- Our MFA Solution
- Training Awareness Videos
- Training Sample Material
  - Additional Technical Personnel Articles
  - Infographics
  - Informative Emails

Solution Pricing Request Form

bit.ly/XpelSolutionPricing

Thank You!



Contact Me:

Denise Caccavari
dcaccavari@forward-edge.net
(513)761-3343 ext. 116

Schedule a Meeting

Thank You!



Contact Me:

Casey Gessler
cgessler@forward-edge.net
(219)-501-9377

< Schedule a Meeting

Thank You!



Contact Me:

Kehlan Rutan
krutan@forward-edge.net
(513)295-6809

< Schedule a Meeting

Thank You!



Contact Me:

Jeff Langdon
jlangdon@forward-edge.net
(513)869-9588

< Schedule a Meeting

Thank You!



Contact Me:

Grant Slusher
gslusher@forward-edge.net
(513)800-9600

< Schedule a Meeting

Thank You!



Contact Me:

Ben Carson
bcarson@forward-edge.net
(513)390-7232

< Schedule a Meeting

Thank You!



Contact Me:

David Gammell
dgammell@forward-edge.net
(513)761-3343 ext. 112

< Schedule a Meeting

Thank You!



Contact Me:

Katey Schroeder
kschroeder@forward-edge.net
(513)886-4648

< Schedule a Meeting

Our complete cybersecurity suite for K-12 education.

Navigate cybersecurity challenges with the advantage of Xpel by Forward Edge, the emerging leader in next-generation cybersecurity solutions designed specifically for the K-12 environment. Xpel by Forward Edge safeguards your district with intelligence driven strategies.

Xpel Cybersecurity Suite

Managed Cybersecurity

- **EDR**
  Endpoint Detection & Response
- **SIEM**
  Security Information Event Management - Log Analytics
- **Vulnerability Management**
  Internal & External Scanning/ Cumulative Actionable Reporting
- **IDS/IPS**
  Intrusion Detection & Prevention Solutions
- **Dark Web Monitoring**
  Continuous Domain Monitoring
- **Phishing Threat Simulations**
  Real Time Security Training
- **vCISO**
  Virtual Chief Information Security Officer
- **User Awareness Training**
  Security Training Modules Designed for K-12 Audiences
- **SOC Monitoring**
  24/7/365 Eyes-on-Glass Security Operations Center Monitoring

vCISO

- **NIST/CIS Security Framework Alignment - Policy Support**
- **Incident Response Playbook Development**
- **Data Privacy Compliance**
- **Security Assessment**
  Comprehensive Organizational Cybersecurity Analysis - 18 Critical Risk Categories
- **Network Audit**
  Comprehensive Analysis of IT Infrastructure
- **Penetration Testing:**
  Internal and External
- **Strategic Planning**
  Lifecycle Management & Fiscal Forecasting

Security Training

- **Security Awareness Training**
- **Professional Development**
- **Phishing Threat Simulations**
- **Tabletop Exercises**

Engineering Solutions

- **Backup Solutions**
- **Firewall Solutions**
- **Authentication Solutions**
- **Vulnerability Management**
- **Network Asset Discovery**
- **Incident Response / Forensics / Recovery**
- **Project Based Engineering Support**

Physical Security

- **Video Surveillance**
- **Access Control**

Learn more at: **xpelcyber.com**

xpelcyber.com

Don't dismiss cyberthreats. Dismantle them.

Cybersecurity Suite

xpel by Forward Edge



Managed Cybersecurity 2024
TRAINING GUIDE

Scalable, Lasting Solutions with Education in Mind

Partner Managed Services

Managed Network Engineering Services provides your District the confidence that a proactive and well-maintained systems maintenance process is in place.

Curriculum & Technology Integration

Former educators and technology integration coaches bring a suite of professional learning services including coaching, assessments micro credentialing, bootcamps and more.

Managed Cybersecurity

Improve your District's cybersecurity posture with our suite of Next Generation technology tools to significantly mitigate risk.

xpel by Forward Edge

Architectural Technology Designer

Technology Designer that provides reliable, efficient, and future-proofing K-12 technology solutions and planning.

On-Site Services

Experienced desktop engineers provide daily technology support for Districts, helping to strategize project implementation, planning and completion.

Cabling Solutions

End-to-end Flexible cabling solutions that anticipate new technologies and ensure technology is effectively integrated into Districts.

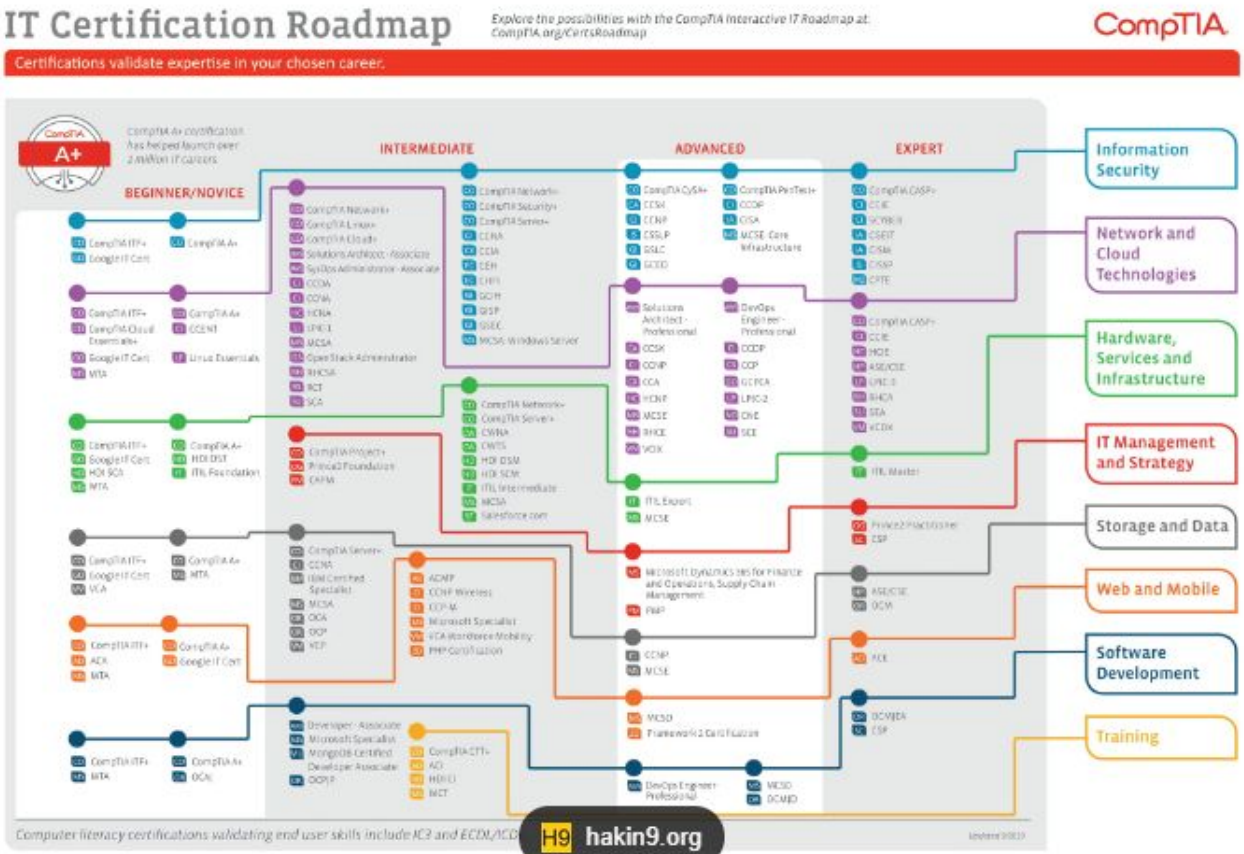
Talking Points

1. General Forward Edge Introduction

2. Xpel Introduction: While Forward Edge has always been in the business of network security we recognized that a distinct brand could communicate our commitment to security by defining cybersecurity as a distinct engineering discipline with skills that depart from traditional network engineering best practices and the daily focus of our NOC engineers. Xpel represents an acknowledgment of this and is intended to communicate the seriousness of this dedicated security practice powered by Forward Edge and informed by the 20 years of K-12 focused engineering expertise.

3. Xpel by Forward Edge is now a mature, national award-winning full security suite featuring a 24/7 Security Operations Center staffed by dedicated professional security engineers and analysts.

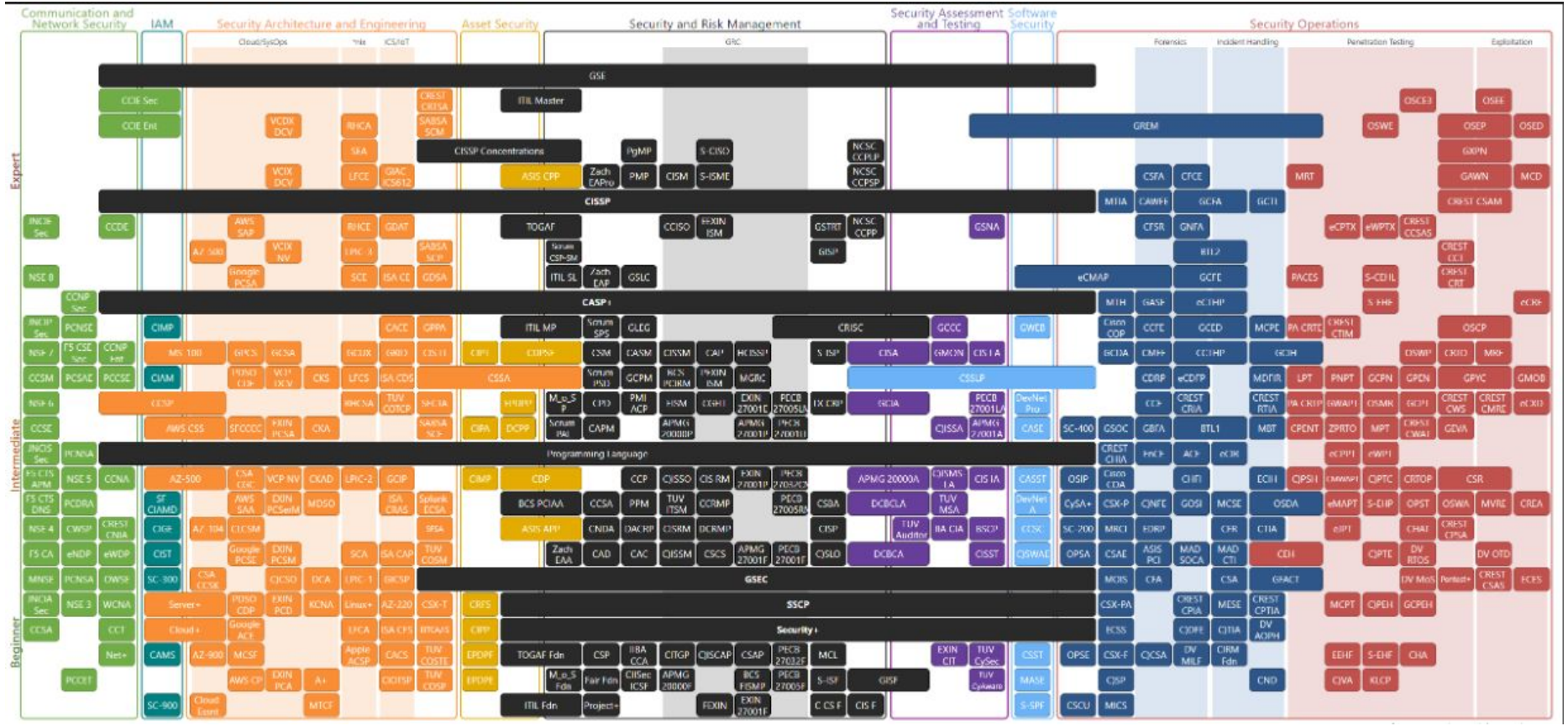
4. Introduce the Xpel value proposition: It's not the [enterprise], tools it’s what we do with them.”



H9 hakin9.org

xpel
by Forward Edge

Cybersecurity - A Distinct Engineering Discipline
437 Certifications


Communication and Network Security
IAM
Security Architecture and Engineering
Asset Security
Security and Risk Management
Security Assessment and Testing
Software Security
Security Operations
Forensics
Incident Handling
Penetration Testing
Exploitation
Expert
Intermediate
Beginner
GSE
CISSP
CASP+
Programming Language
GSEC
SSCP
Security+
CISSP Concentrations
ITIL Master
GREM
TOGAF
CRISC
CSSLP
GSNA
eCMAP
ASIS CPP
PMP
CISM
CISA
CCSP
AWS CSS
AZ-500
AZ-104
AZ-900
SC-300
SC-900
Server+
Cloud+
Net+
Linux+
CCNA
CCNP Sec
CCIE Sec
CCIE Ent
CCDE
NSE 8
NSE 7
NSE 6
NSE 5
NSE 4
NSE 3
FS CSE Sec
FS CSE Hrt
FS CTS APM
FS CTS DNS
FS CA
CCSM
PCSAE
PCCSE
PCNSE
PCNSA
PCDRA
CWSP
eNDP
eWDP
CWSI
WCNA
CCT
CAMS
PCCET
CIAM
CCSE
CGE
CIST
CCSA
JNCIE Sec
JNCIS Sec
JNCIA Sec
CREST CRTSA
SABSA SCM
RHCA
LFCE
GIAC ICS612
SABSA SCF
ISA CE
GDSA
LPIC-3
SCE
RHCE
GDAT
VCDX DCV
VCIX DCV
VCIX NV
AWS SAP
Google PCSA
Zach EAPro
Zach EAP
GSLC
PgMP
S-CISO
S-ISME
NCSC CCPUP
NCSC CCPSP
NCSC CCPP
GSTRT
GISP
HEXIN ISM
CCISO
Scrum CSP-SM
Scrum SPS
Scrum PSD
Scrum PAL
ITIL SL
ITIL MP
GLEG
GCCC
GWEB
S-ISP
GMCN
CIS I A
MGRC
PCEB 27001P
PCEB 27005LA
PCEB 27001LA
PCEB 27001A
DevNet Pro
DevNet A
CASE
SC-400
GSOC
GBTA
BTL1
MBT
CPENT
ZPRTO
MPT
CREST CWAT
GEVA
CREST CHIA
HNCP
ACP
eCIR
eCPPT
eWPT
CASST
OSIP
Cisco CDA
CIHT
ECIH
CPSIH
CWAPT
CIPTC
CRTOP
CSR
CySA+
CSK-P
CNFE
GOSI
MCSE
OSDA
eMAPT
S-DHP
OPST
OSWA
MVRE
CREA
SC-200
MRCI
EDRP
CFR
CTIA
ePT
CHAE
CREST CPTSA
OPSA
CSAE
ASIS PCI
MAD SOCA
MAD CTI
CDH
CPTE
DV RTOS
DV OTD
MCRS
CPA
CSA
GRACT
DV MoS
Pentest+
CREST CSAS
ECES
CSK-PA
CREST CPIA
MESE
CREST CPTIA
MCPT
CPEH
GCPEH
ECSS
CDPE
CDTIA
DV ACPH
CSK-F
CJCSA
DV MILF
CIRM Fdn
EEHF
S-EHF
CHA
CJSP
CND
CJVA
XLCP
CSCU
MICS
OPSE
CSST
MASE
S-SPF
EXIN CIT
TUV CySec
TUV CyAward
GISF
S-ISF
C CS F
CIS F
EXIN 27001F
FDXIN
Project+
ITIL Fdn
M_o_R Fdn
Fair Fdn
CISSec ICSF
APMG 20000F
BCS FISMP
PECB 27005F
PECB 27032F
MCL
CSAP
CITGP
CJISCAP
IIBA CCA
TOGAF Fdn
CSP
EPDPF
EPDPE
CRFS
CIRP
TUV COSTE
TUV COSP
TUV COSM
TUV COSTP
TUV COSTC
BTCA/S
ISA/IEC 62443
ISA CFS
ISA CRAS
Splunk ECSA
Apple ACSP
CACS
Linux+
AZ-220
CSK-T
LFCA
KCNA
EXIN PCD
EXIN PCM
EXIN PCA
EXIN PCSM
EXIN PCSeM
A+
MTCE
Cloud Essn
AWS-CP
MCSF
Google ACE
PDSO CDP
SCA
ISA CAP
DCA
CJCSO
BRCSP
LPIC-1
CSA CCSK
AWS SAA
MDSO
SFCIAMD
CLCSM
SFSA
CKAD
LPIC-2
GCIP
VCP-NV
CSA CCAK
CKS
LFCS
ISA CDS
SHCTA
SABSA SCP
SABSA SCL
GPPA
CACE
MS-100
GPCS
GCSA
GCDX
GMDD
CDS-I
CDPP
CDPSP
CSSA
CIMP
CIAMD
CCDP
AWS CCP
SFCCCC
EXIN PCSA
CKA
CIPA
DCPP
HPWPT
SHCNA
TUV COTCP
CIPM
CAPM
M_o_R IP
PMI ACP
HSM
CEHT
APMG 20000IP
APMG 27001P
PECB 27001I
IX CISP
DCBA
CJISSA
APMG 27001A
APMG 20000A
DCBCLA
DCBCA
CJISMS LA
CIS IA
TUV MSA
TUV Auditor
IIA CIA
BSCP
CJISST
CJISWAE
CJSLO
CCP
CJISSO
CIS RM
EXIN 27001P
PECB 27002PA
PECB 27005RA
CSQA
CISP
CNDA
DACRP
CISRM
DCRMP
CCRMP
PPM
TUV ITSM
CCSA
BCS PCIAA
ASIS APP
Zach EAA
CAD
CAC
CJISSM
CSCS
APMG 27001F
PECB 27001F
CMP
CDP
ASIS CPA
CSA CCIC
VCP-NV
CKAD
LPIC-2
GCIP
SF CIAMD
AWS SAA
DXIN PCSeM
MDSO
CLCSM
Google PCSE
EXIN PCSM
SCA
ISA CAP
CSA CCSK
CJCSO
DCA
LPIC-1
BRCSP
PDSO CDP
EXIN PCD
KCNA
Linux+
AZ-220
CSK-T
Google ACE
LFCA
ISA CFS
BTCA/S
Apple ACSP
CACS
TUV COSTE
EXIN PCA
A+
MTCE
AWS-CP
TUV COSP
Cloud Essn
MCSF
AZ-900
CAMS
PCCET
SC-900
CCSA
CCT
Net+
WCNA
NSE 3
CWSI
CCNA
CCNP Hrt
PCNSA
PCDRA
CREST CNIA
eNDP
eWDP
CWSP
NSE 5
NSE 4
NSE 6
NSE 7
NSE 8
CCDE
INCIE Sec
INCIP Sec
PCNSE
CCSM
PCSAE
PCCSE
CCSE
JNCIS Sec
JNCIA Sec
FS CTS APM
FS CTS DNS
FS CA
MNSE
CWSP
CIST
CGE
CWSA
CCSP
AWS CSS
SFCCCC
EXIN PCSA
CKA
SHCNA
SABSA SCL
GPPA
CACE
MS-100
GPCS
GCSA
GCDX
GMDD
CDS-I
CDPP
CDPSP
CSSA
CIMP
CIAMD
CCDP
AWS CCP
VCP-NV
CKS
LFCS
ISA CDS
SHCTA
TUV COTCP
CIPM
CAPM
M_o_R IP
PMI ACP
HSM
CEHT
APMG 20000IP
APMG 27001P
PECB 27001I
IX CISP
DCBA
CJISSA
APMG 27001A
APMG 20000A
DCBCLA
DCBCA
CJISMS LA
CIS IA
TUV MSA
TUV Auditor
IIA CIA
BSCP
CJISST
CJISWAE
CJSLO
CCP
CJISSO
CIS RM
EXIN 27001P
PECB 27002PA
PECB 27005RA
CSQA
CISP
CNDA
DACRP
CISRM
DCRMP
CCRMP
PPM
TUV ITSM
CCSA
BCS PCIAA
ASIS APP
Zach EAA
CAD
CAC
CJISSM
CSCS
APMG 27001F
PECB 27001F
CMP
CDP
ASIS CPA

Xpel Cybersecurity Suite

Managed Cybersecurity

- **EDR**
  Endpoint Detection & Response
- **SIEM**
  Security Information Event Management - Log Analytics
- **Vulnerability Management**
  Internal & External Scanning/Cumulative Actionable Reporting
- **IDS/IPS**
  Intrusion Detection & Prevention Solutions
- **Dark Web Monitoring**
  Continuous Domain Monitoring
- **Phishing Threat Simulations**
  Real Time Security Training
- **vCISO**
  Virtual Chief Information Security Officer
- **User Awareness Training**
  Security Training Modules Designe for K-12 Audiences
- **SOC Monitoring**
  24/7/365 Eyes-on-Glass Security Operations Center Monitoring

vCISO

- **NIST/CIS Security Framework Alignment - Policy Support**
- **Incident Response Playbook Development**
- **Data Privacy Compliance**
- **Security Assessment**
  Comprehensive Organizational Cybersecurity Analysis - 18 Critical Risk Categories
- **Network Audit**
  Comprehensive Analysis of IT Infrastructure
- **Penetration Testing:**
  Internal and External
- **Strategic Planning**
  Lifecycle Management & Fiscal Forecasting

Security Training

- **Security Awareness Training**
- **Professional Development**
- **Phishing Threat Simulations**
- **Tabletop Exercises**

Engineering Solutions

- **Backup Solutions**
- **Firewall Solutions**
- **Vulnerability Management**
- **Network Asset Discovery**
- **Incident Response / Forensics / Recovery**
- **Project Based Engineering Support**

Physical Security

- **Video Surveillance**
- **Access Control**

Engineering Solutions

- Backup Solutions
- Firewall Solutions
- Vulnerability Management
- Network Asset Discovery
- Incident Response / Forensics / Recovery
- Project Based Level I - Level III Support

Physical Security

- Video Surveillance
- Access Control

Awards we've earned along the way.

Cooperative Purchasing Contract Awards

BuyBoard National Purchasing Cooperative

equalis GROUP

ASC Allied States Cooperative

npp gov

Supporting District Administration:

Cyber Liability Insurance

Federal & State Data Privacy

General Compliance

Securing K-12 Technology Environments from:

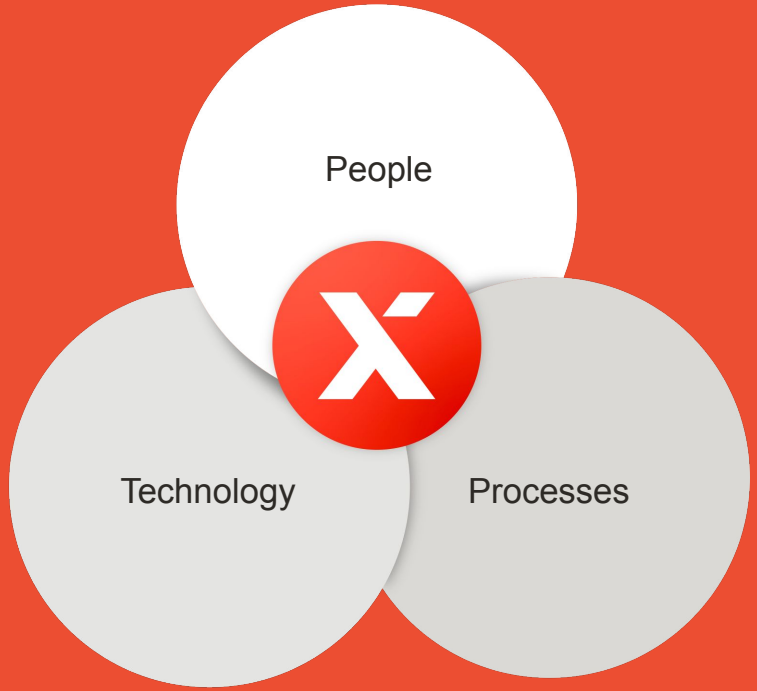
Ransomware & Funds Transfer Fraud

Theft of District PII & Sensitive Data

Disruption to the Operational, Administrative & Instructional Access to Technology Tools



Complete Cybersecurity Suite for K-12 Education.



xpel
by Forward Edge

Follow the Framework:

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CIS. Center for Internet Security®



Why the Frameworks Matter - Talking Points

1. **Data Privacy Compliance**
2. **Safe Harbor**
3. **Best Practices**

"Adopting all 18 CIS controls can help prevent up to 97% of cyberattacks."
-Connectwise Cybersecurity Center, Posted 12/15/2020, Kevin Prince

Cybersecurity Professionals are in Demand Nationwide

Estimated 3.5 Million Unfilled Cybersecurity Jobs through 2025

-eSentire 2023 Official Cybersecurity Jobs Report

Cybersecurity Engineer Annual Salary

$122,140

K-12 Tech Director Annual Salary

$82,310

Nationwide Averages - ZipRecruiter 1/2024



Common Security Controls at K12 School Districts

- Partial Security Controls
- Backups & Testing
- Firewalls
- Patches & Fixes
- Segmentation

Continued Challenges for K12 School Districts

- Can't Hire/ Afford Cyber Engineer
- Active Monitoring 24/7
- Time to Evaluate & Implement Cyber Tools
- Continuous Investment in Dynamic Requirements
- Develop Training Plans for Teachers & Staff to Decrease Exposure to Cyber Threats
- Incident Response Resources

INTRODUCING THE Xpel STACK



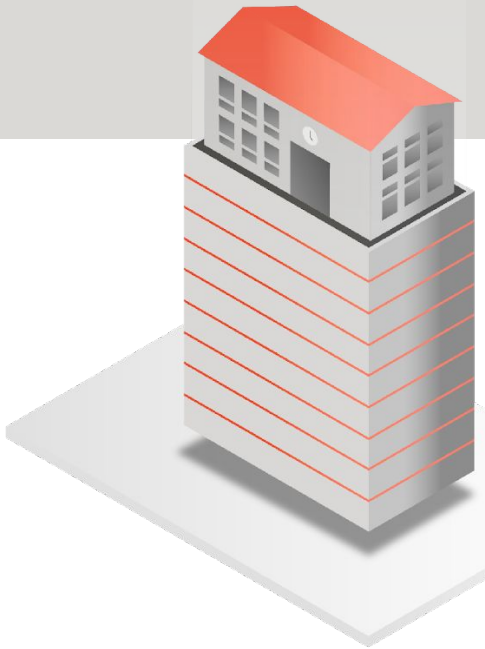
It's not the tools.
It's what we do with them.

-Grant Slusher

1. **Trackside Team**: Around 75 people travel to each race to set up, run, and sometimes repair the car. This includes engineers, mechanics, and performance analysts [1].
2. **Operational Staff**: Each team is allowed a maximum of 58 operational staff who work directly with the car during a race weekend. This includes the pit crew, engineers, mechanics, and drivers [2].
3. **Headquarters Team**: The total number of people involved in an F1 team can range from 300 to 1,200, depending on the team's size and resources [1].

-David Gammell "Formula 1 Analogy"

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR

Servers
Critical
Workstations

SentinelOne

SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

EDR/XDR/MDR - What is it?

Endpoint Detection and Response (EDR) and Extended/Managed Detection and Response (X/MDR) are enterprise cybersecurity solutions that provide automated cyber threat detection and response through data visibility, threat intelligence, and big data analytics. While EDR is an effective defense against cyberattacks, X/MDR expands on EDR with additional protections at the network, server, cloud, and application levels.

The primary functions of an EDR security system are to:

- **Monitor and collect activity data from endpoints that could indicate a threat**
- **Analyze this data to identify threat patterns**
- **Automatically respond to identified threats to remove or contain them, and notify security personnel**
- **Forensics and analysis tools to research identified threats and search for suspicious activities**

Talking Points

Where is it deployed?

24/7 Monitored SentineoneOne Agents:

Virtual Servers/Physical Servers

Administrative Suite (Superintendent Suite, Treasures/Business Suites, IT, Guidance, Nurses, Principals, etc.)

Anywhere sensitive data lives.

8/5 Workdays

Faculty Devices

How is it Deployed? Agents installed on devices.

(Windows, Linux OS's - NOT Chromebooks or MaciOS)

Talking Points

- **SentinelOne “Control” version licenses/agents are installed on all critical devices. (District responsible for installation unless Managed Services customer.)**

- **SentinelOne:**
  - **(a.) Kills:** All active content in documents, executables, and sub-processes are stopped. The agent enables Kill for processes that act contrary to normal endpoint behavior, or do not fit the actions of the application the process is hiding in.

  - **(b.) Quarantines:** The Quarantine option encrypts malicious executables, and moves them to a confined path. Quarantined files can be retrieved from the SentinelOne Management console for further analysis i.e. detonation in a sandbox.

  - **(c.) Remediates:** The Remediate response measure removes linked libraries, deletes seed files, and restores the configuration of the OS, application, and user settings to the state before an attack began.

  - **(d.) Rollback:** Restores the endpoint to a saved VSS snapshot, undoing the changes made by the malicious process and its associated assets. This option is best for ransomware mitigation and disaster recovery because it undoes all changes made to files, like encryption.

  - **(e.) Disconnect from Network:** SentinelOne offers the option to disconnect an endpoint from the network. This feature enables an administrator to isolate an endpoint from everything except the SentinelOne management console. This preventative measure can stop an incident spreading while the alert is investigated.

Talking Points

- SentinelOne is Consistently in the Gartner's Top 5 Magic Quadrant Leader Board. Cyber liability underwriters are looking for the most advanced products disclosed on their applications for coverage.
- District has full access to SentinelOne console w/ full visibility (everything but admin).
- Xpel SOC has the ability to remote in via the S1 console 24/7 and take affected device(s) offline (Protocols regarding Xpel SOC actions are determined during onboarding.)
- SentinelOne's "Ransomware Rollback" feature enables organizations to restore their encrypted files to a pre-attack state (by leveraging the VSS shadow copy OS functionality) effectively reversing the effects of a ransomware attack with less than 4 hours of lost data. In a ransomware attack, the XDR solution can quickly roll back the affected files to their original state before the encryption occured.

IMPORTANT DIFFERENTIATOR: The Xpel SOC team maximizes the effectiveness of the EDR by writing custom detection rules. This enables the team to address specific threats unique to both the district's specific environment as well as K-12 environments as a sector.

This hyper and singular focus on the K-12 sector heightens the fidelity of the alerts and makes MTTD/MTTR more impactful. The Xpel SOC provides detailed reports available on the CyberHub that provide a comprehensive overview of the district's deployments. These reports include data on active agents, ticket workflows, and deployment graphs, helping teams identify and address blind spots in their security estate. Finally, ***all threats identified are crowdsourced and applied universally at the parent level to all Xpel SOC customers.***

SentinelOne Further Learning Resources

1.) Connectwise - SentinelOne “Control” Licenses and Connectwise SOC 24/7 Integration)

https://www.connectwise.com/webinars/behind-the-scenes-sentinelone-edr-connectwise-soc

2.) Ransomware Rollback feature

What is Ransomware Rollback? - SentinelOne

3.) SentinelOne vs Crowdstrike

SentinelOne vs. CrowdStrike | Cybersecurity Comparisons

4. Threat Threshold Alert - Detection Engines

Inside of SentinelOne there are different Detection Engines that make up SentinelOne's Cloud Detection AI.

- Static AI Engine
- Behavioral AI Engine
- Cloud Intelligence Engine
- STAR Rules Engine

Read more on the SentinelOne Detection Engines, you can visit the whole series here.

SentinelOne Detection Engines

Static AI Engine 101

Much like cloud security, AI itself is a broad field and machine learning (ML) is a subset of this field. ML is exactly as the name suggests: machines learning to perform a task with high accuracy. ML models can be trained for any number of uses, from the academic (e.g., to differentiate between photographs of dalmatian puppies or chocolate chip ice cream) to the highly practical, such as differentiating between benign files and malware.

At the highest level of abstraction, our Static AI Engine consists of supervised machine learning algorithms which analyze files **before they execute**, examining the file structure and searching for historical patterns synonymous with malicious intent. Digging in a little deeper, the Static AI Engine is a classifier engine, categorizing the files being scanned in a number of classes, such as benign, suspicious, malicious, and so on. Ultimately, the decision tree algorithm delivers a predictive confidence level for a file's maliciousness. For ML models to perform well, they must be trained over a large data set. SentinelOne's classifier algorithms have been trained across nearly a billion samples over the past decade, and our threat researchers are continuously improving the models against the latest threats.

- Fileless attacks, ·

Ransomware, including polymorphic ransomware ,

- Zero-day exploits
- Credential theft
- Privilege escalation
- Malicious scripts
- MITRE tactics and techniques

SentinelOne Detection Engines

.

The Behavioral AI Engine has several characteristics:

· Autonomous operation: It functions fully with or without an internet connection to the SaaS management console. The intelligence of the engine is built within the agent itself such that there is no round-trip latency to the cloud for analysis.

· Real-time: The agent monitors all kernel-level processes as they are launched.

· Post-execution: Unlike the Static AI Engine, which examines files *before* they are executed, the Behavioral AI Engine is constantly observing all processes as they execute.

Storyline™: Patented visualization technology that tracks what's happening inside of each cloud workload.

SentinelOne Detection Engines

Application Control Engine 101

SentinelOne's Application Control Engine is a highly specialized drift prevention engine within our real-time CWPP agent that is focused on preserving immutability of containers and virtual machines (VMs). It accomplishes this by detecting any binaries or scripts created and executed after the VM or container starts. Stated another way, ***the Application Control Engine ensures that only executables from the original container image run in the workload instance***.

Originally, the engine was designed to protect immutability of containerized workloads running within Kubernetes and other container orchestration systems such as Hashicorp Nomad and AWS ECS. However, the cloud security innovators at SentinelOne expanded the scope to include Linux VMs. In short, the Application Control Engine reduces the attack surface of your immutable container architecture.

Cloud Threat Intelligence Engine 101

Unlike the Static and Behavioral AI Engines, which use AI, the SentinelOne Cloud Threat Intelligence Engine is a rules-based reputation engine which uses signatures to detect known malware. It is important to note that SentinelOne's CWPP solution does not rely solely upon signatures. Any solution that relies solely upon signatures is woefully underprepared for cloud workload protection warfare.

Even though signatures are easily evaded by sophisticated threat actors, not every threat actor is sophisticated, and known malware is still often used. And so, the use of signatures still has a place in detecting known malware, while advanced threats (e.g., zero-day exploits, fileless attacks, polymorphic ransomware, etc.) still require a more modern, AI-powered arsenal.

Connectwise MDR

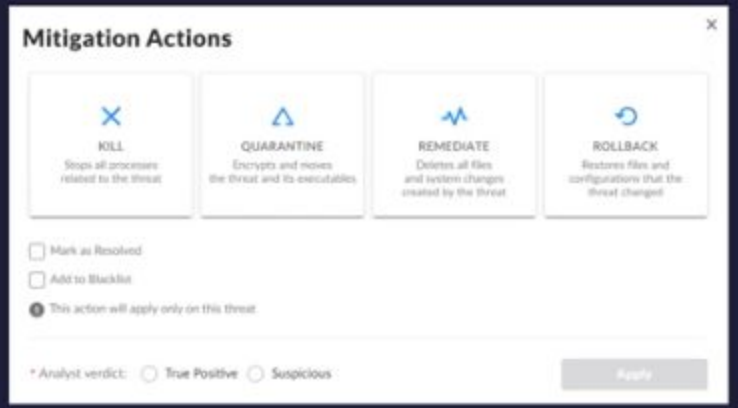
How ConnectWise MDR Works

Workstations & Servers → Alerts → ConnectWise Cloud ↔ Analysis ↔ ConnectWise SOC → Remediation/Notification → You

Remediation on your behalf

This includes:

- Stopping all processes related to the threat.
- Encrypting and quarantining the threat and its executables.
- Disconnecting the system from the network to prevent spread of malicious activity.
- Deleting files and system changes created by the threat.
- Restoring files and configurations that the threat had changed.



xpel
by Forward Edge

Our Advanced Cyber Defense for Education Stack

PERCH
a ConnectWise solution



EDR/ XDR/ MDR

SIEM

24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

Core
vCenter/ESXi
Servers &
Workstations
Firewall

CONNECTWISE

SIEM - What is it?

SIEM stands for Security, Information, and Event Management. SIEM technology aggregates log data, security alerts, and events into a centralized platform to provide real-time analysis for security monitoring.

SIEM software works by collecting log and event data produced from applications, devices, networks, infrastructure, and systems to draw analysis and provide a holistic view of an organization's information technology.

Without a SIEM it would be extremely difficult for a SOC to achieve its mission. A modern SIEM offers:

- Log aggregation: A SIEM collects the log data and correlates alerts, which analysts use for threat detection and hunting.
- Context: Because a SIEM collects data across all the technology in the organization, it helps connect the dots between individual incidents to identify sophisticated attacks.
- Using analytics and AI to correlate alerts and identify the most serious events, a SIEM cuts down on the time to identify potential threats because it aggregates sys logs at a platform level vs local device level.
- Automated response: Built-in rules allow SIEMs to identify probable threats and block them without the interaction of people.

Where is it deployed?

SIEM should be deployed everywhere you can send or collect logs from.

Some examples are:

- Core Switches / Routers - (logs forwarded)
- Firewalls - (logs forwarded)
- Servers - (agent)
- VPN Concentrator / Gateways - (logs forwarded)
- Critical Desktops (at a minimum) - (agent)

How is it Deployed? Agents installed on devices or logs forwarded and collected. A single agent is designated as the “log collector” repository. (In the event an agent cannot be installed on a device we use log forwarding.)

Talking Points

SIEM is increasingly more relevant as bad actors are finding ways to circumvent EDR by strategically staying below the EDR threat alert thresholds. While EDR is only looking at files/malware, etc., SIEMs collect and analyze sys logs for context. EDR is not able to detect Brute Force Attacks or Authentication events.

Some examples of log-related alerts:

- Report from antivirus software that a device is infected by malware
- Report from firewall about traffic to/from a prohibited network address
- Attempt to access a critical system from an unknown host or IP address
- Repeated failed attempts to access a critical system
- Change in user privileges
- Usage of insecure or prohibited protocols/ports
- Brute Force attacks are seen through the SIEM because these attacks aren't malware based, but based around user behavior.
- Distributed Denial of Service attacks also use network traffic to stall or comprise a machine and in turn does not need malware to function.

IMPORTANT DIFFERENTIATOR: The Xpel SOC team "designs" Event Notifications specific to the district; we add event notification packages specific to that districts devices (i.e. if a district has a Sonicwall firewall we will add a Sonicwall event notification package.) Most event notifications are vendor agnostic but the Xpel SOC fine tunes each environment in this way to maximize the effectiveness of the SIEM.

Talking Points

Key Features

Key Features of CW SIEM

Real-Time Monitoring: Continuously monitors network traffic, user activity, and system behavior.
Threat Detection: Uses advanced analytics and machine learning to identify potential security threats.
Scalability: Built on the Elastic Stack, CW SIEM can scale to handle large volumes of data.

Elastic Stack Components

Winlogbeat, Auditbeat, and Filebeat - CW SIEM uses several data shippers from the CW SIEM agent to collect and send data to the SIEM. Understanding the differences between Winlogbeat, Auditbeat, and Filebeat is crucial for explaining the capabilities of CW SIEM to clients.

Winlogbeat (Windows Logs)

Purpose: Winlogbeat is designed to collect and ship Windows event logs to Elasticsearch or Logstash.

Key Points:

Target Platform: Specifically for Windows environments.
Data Collected: Security events, application logs, system logs.

USE CASES: Monitoring user login events, tracking changes in system configurations, detecting potential security breaches on Windows systems.

Talking Points

Key Features

Auditbeat (MACOS Logs)

Purpose: Auditbeat focuses on auditing the activities of users and processes on a system, providing detailed security monitoring.

Key Points:

Target Platform: Primarily used on MacOS and Linux, but also supports Windows.

Data Collected: File integrity data, user logins, process execution events, system call activities.

Use Cases: Ensuring compliance, detecting suspicious activity, monitoring critical file changes, and tracking user actions.

Filebeat (Network Device Logs like Core/Firewall/VCenter etc.)

Purpose: Filebeat is a lightweight shipper for forwarding and centralizing log data. Filebeat for us is what we use on the log forwarding from network devices (firewalls and switches).

Key Points:

Target Platform: Cross-platform, supporting various operating systems.

Data Collected: Log files from applications, network devices, and services.

Use Cases: Collecting application logs, aggregating logs from various sources, and feeding them into Elasticsearch for analysis.

Talking Points

What is a SIEM?

Security Information and Event Management

A SIEM works by collecting log and event data generated by an organization's systems, devices, and applications and brings them into the centralized platform for analysis and reporting.

When the SIEM identifies a threat through a set of predetermined rules, an alert is generated for human review.

Why do I need it?

- Auditing and Compliance Requirements
- Full Visibility of Everything Happening Within the Network
- Dramatically Decreases the Time it Takes to Identify Threats
- Detailed Forensic Analysis in the Event of Major Security Breaches

Connectwise SIEM (formerly Perch) Further Learning Resources

1. **Connectwise University**
   https://docs.connectwise.com/ConnectWise_Business_Knowledge/Perch

2.)

ConnectWise SIEM Recorded Demo | Extra Threat Protection

3.)

https://info.connectwise.com/cybersecurity/perch/siem-youtube-video?_gl=1*1gyg4lu*_ga*MzA1MTAxNDk4LjE3MDExMDE1MjY.*_ga_QSGE0F7K8V*MTcxNTYyNDQ3Mi43LjEuMTcxNTYyNDU0Ny42MC4wLj

4.) ConnectWise SIEM - ConnectWise

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR

SIEM

24/7/365 SOC MONITORING

VULNERABILITY MANAGEMENT

DARK WEB MONITORING

INTRUSION DETECTION AND PREVENTION

RISK ASSESSMENT

SECURITY TRAINING

vCISO

SOC - What is it?

A SOC is a team of experts that proactively monitor an organization's ability to operate securely. Members of a SOC team are responsible for a variety of activities, including proactive monitoring, incident response and recovery, remediation activities, compliance, and coordination and context.

Benefits of a SOC

- Reduces Impact of a Breach
- Allows Organization-Wide Visibility
- Gain Transparency and Control on Security
- Improve Incident Response Times - Improved MTTD and MTTR
- Improve Management Practices Post Incident
- Combines Automation with Human Resources to Threat Response

The Xpel Security Operations Center

Additional Benefits

Benefits of the Xpel SOC

- Continuous Monitoring and Prevention 24/7/365
- Access to K-12 Security Analysts adding a vital human intelligence to security tools.
- Improved MTTD/MTTR
- Hyper Focus on K-12 Environments - Crowdsourcing of Alerts
- Reduction of False Positive Alert Fatigue - Intelligence-Driven Noise Reduction
- True Positives Identification Efficiencies - Custom threat indicators designed to specifically address K-12 Environments
- High Value Detections - Over 60% of alerts identified by Xpel SOC are internally generated

Alert Fatigue is Real

Public sector organizations, with IT security staff, are estimated to allow more than 50% of alerts to go unaddressed. - Cybercrime Magazine - May 2023

Every alert takes 30 minutes/False positives take even longer - IDC April, 2023

Talking Points

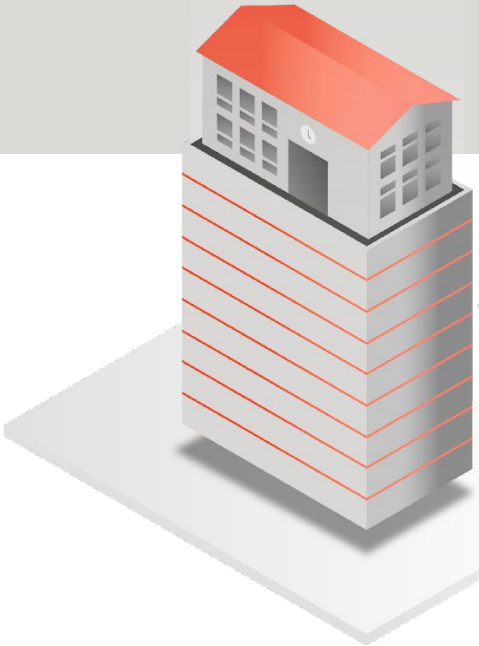
IMPORTANT DIFFERENTIATOR:

The Xpel SOC team offers **24/7/365** “eyes-on-glass” monitoring performed by trained security analysts. In excess of **60% of the alerts investigated by the Xpel SOC Team are identified by custom detection rules** (hashes, etc). The creation of these detection rules can come from a variety of sources. Most originate from threat hunting and the behavior AI in SentinelOne; the Xpel SOC then turns these into static detections so that they are not allowed to run for any amount of time. Some detection rules, however, originate from outside sources from different threat intel feeds.

This enables the team to address threats unique to both the district’s specific environment as well as K-12 environments as a sector. This hyper and singular focus on the K-12 sector heightens the fidelity of the alerts and makes MTTD/MTTR more impactful.

Finally, ***all threats identified are crowdsourced and applied universally at the parent level to all Xpel SOC customers.***

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING

VULNERABILITY MANAGEMENT

DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING
vCISO

Internal & External Scanning
Cumulative Reporting

Qualys.

Vulnerability Management What is it?

Xpel by Forward Edge leverages their advanced partnership with Qualys vulnerability management solutions to provide school districts global visibility into IT systems vulnerabilities.

The Xpel (Internal and External) Vulnerability Scan detects and classifies exposed entry points into networks and systems on which cyber attackers capitalize by scanning for known threats, out-of-date hardware, software and other appliances. This critical layer in our cyber defense arsenal cumulatively detects critical vulnerabilities and misconfigurations across network devices, operating systems, and applications per industry standard hardening CIS benchmarks. The Xpel SOC team provides prioritized identified vulnerabilities to supports the most impactful and time-sensitive remediation

The robust reporting not only identifies holes and weaknesses but also provides criticality scores and remediation suggestions in an easy to understand format you can quickly act on!

- External VS Internal
- Deployment - Agent or Virtual
- Frequency - Monthly? Continuous?
- Scanning Solution vs Managed Solutions
- Importance of Product Reporting
  - Vulnerability by group/type/location
  - Risk Category
  - Remediation instructions

TALKING POINTS

IMPORTANT DIFFERENTIATOR: Xpel's **Qualys** vulnerabilities reports include all CVE's (Common Vulnerabilities and Exposures) regardless if a solution is known or not.

> ***Note:*** *Districts are actively being encouraged to utilize MS-ISAC's* ***free*** *external scans. These scans* ***ONLY*** *report CVE's found* ***that have a known remediation****.*

Reports are highly customizable.

- Format, customers can choose between PDF, CSV, Excel, Word Doc, HTML and other formats.
- Priorities. Customers can choose whether to sort the vulnerabilities by criticality or IP address. In one report it will list the vulnerabilities and all IPs associated with that Vulnerability. In the other report it will list the IP address and all the vulnerabilities associated with that IP.
- Vulnerability by group/type/location
- Risk Category
- ***Includes actionable remediation instructions - i.e. links to patches!***

Note: Xpel's SOC team can customize scans at the request of the district at any time. (Example: District can request a "rescan" to a designated IP range to verify a district's vulnerability remediation action or patch was successful.)

External Vs Internal

	External Vulnerability Scans	Internal Vulnerability Scans
Scope	Internet-facing systems	Internal machines
Purpose	Looks at how hackers can breach internet-facing assets, web apps and ports	Looks for vulnerabilities in your local apps, devices and servers
Frequency	Continuous or in response to changes	Regular schedule or continuous
Compliance	External standards and regulations	Internal security policies, regulations
Reporting	Severity, time to fix, remediation advice	Internal vulnerability reports, patching, SLAs

APPLE | IOS AND IPADOS

CVE-2024-23296

Apple Multiple Products Memory Corruption Vulnerability

Apple iOS, iPadOS, macOS, tvOS, and watchOS RTKit contain a memory corruption vulnerability that allows an attacker with arbitrary kernel read and write capability to bypass kernel memory protections.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2024-03-06
- **Due Date:** 2024-03-27

Examples of CVEs

A classic example of a CVE is the recent Log4j vulnerability report (CVE-2021-44228). It contains detailed information about a vulnerability of the popular Java logging framework, Apache Log4j. Many service providers, like AWS, Cloudflare and Twitter, were affected by this vulnerability.

Another example is the ProxyShell vulnerability. It affected Microsoft Exchange servers by allowing remote code execution. It was announced via CVE-2021-34473, CVE-2021-34523 and CVE-2021-31207.

Our Advanced Cyber Defense for Education Stack



EDR/ XDR

SIEM

24/7/365 SOC MONITORING

VULNERABILITY MANAGEMENT

DARK WEB MONITORING

INTRUSION DETECTION AND PREVENTION

RISK ASSESSMENT

SECURITY TRAINING

vCISO

Continuous Domain Monitoring

CONNECTWISE

Dark Web Monitoring - What is it?

Dark Web monitoring is a form of threat intelligence that involves the continuous scanning for a district's personal information on the Dark Web. This typically involves looking for information associated with the district's internet domain name (and subdomains). This is done through searching through the Dark Web and using threat intelligence to monitor websites for specific information indicators. The benefit of Dark Web monitoring is that it identifies exposed data and the amount of time that your data is exposed. By actively monitoring the Dark Web at all times and mitigating exposed assets or identities, these tools give cybercriminals less time to exploit your confidential information, preventing further information leaks.

Why it's important…

The types of risks that can be exposed through a dark web monitor include:

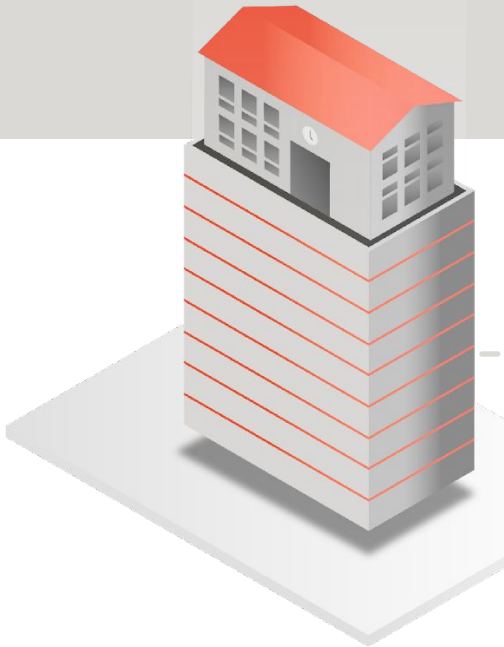
- Third-party breaches
- Data dumps to hacking forums and criminal chatrooms
- P2P leaks
- Accidental leaks
- Brand misuse
- Impersonations
- Domain Spoofing
- Potential threats
- Staff using emails for personal use
- Exposing district credentials on non-district websites.

Dark Web Scanning Further Learning Resources

Dark Web Scanning: Understanding the Why and How | ConnectWise

dark-web-scanning-understanding-the-why-and-how.pdf (connectwise.com)

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING

INTRUSION DETECTION AND PREVENTION

RISK ASSESSMENT
SECURITY TRAINING
VCISO

IDS/IPS - What is it?

Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) work together to enhance network security:

1. Firewall:
    - A firewall acts as a filter for network traffic based on predefined security rules.
    - It sets boundaries for data flow, allowing or denying traffic based on protocols.
    - Firewalls analyze data packets against security protocols, determining whether data should be permitted or blocked.
2. Intrusion Detection System (IDS):
    - IDS identifies potential threats and weaknesses in networked systems.
    - It watches over network activities, flagging irregularities for review without directly affecting data flow.
    - IDS systems come in various forms, including network-based (NIDS) and host-based (HIDS) variants.
    - It differentiates between normal network operations and anomalous behavior, evaluating traffic against known patterns of misuse.
3. Intrusion Prevention System (IPS):
    - An IPS plays an assertive role by actively preventing identified threats from compromising the network.
    - It not only detects but also takes preventive actions against threats.
    - When combined with a firewall and IDS, an IPS enhances security.
    - The firewall filters initial traffic, while the IDS and IPS analyze the filtered traffic for potential threats

Talking Points

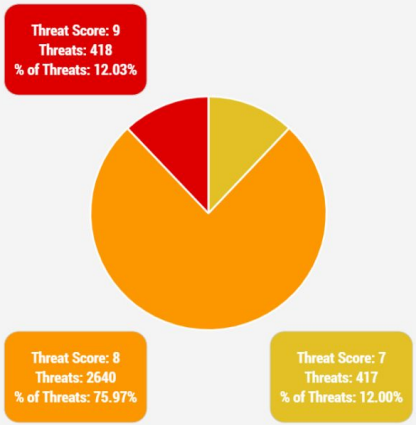


Dark3 Snapshot

Total Threats Seen	New Threats Seen	Auto-Block Currently Enabled?	Current Auto-Block Threshold	Total Threats Blocked	New Threats Blocked
111475	3475	YES	8	94139	3052

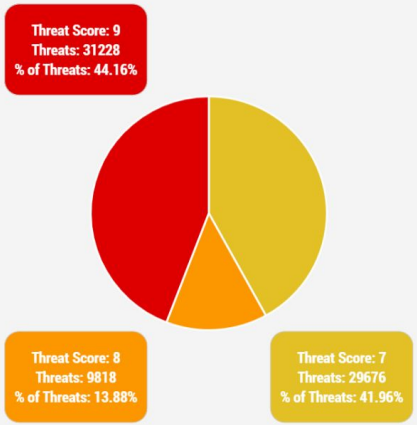
New Threats Identified (05-21-2024 to 06-20-2024)

Individual IP's and domains observed for the first time in this range

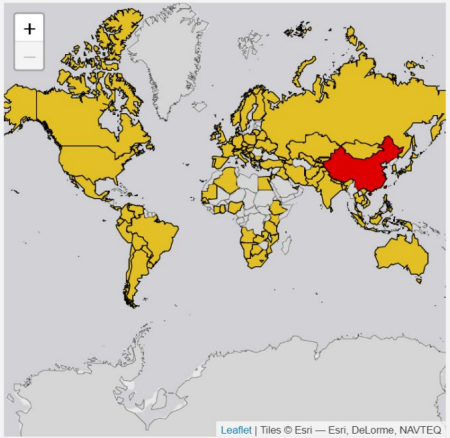


New Threat Connections (05-21-2024 to 06-20-2024)

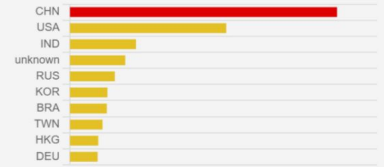
Number of interactions between threats and your network



Geographical Distribution of New Threats (05-21-2024 to 06-20-2024)



Top Ten Countries By New Threats (05-21-2024 to 06-20-2024)



Talking Points

The Dark Cubed set-it-and-forget-it solution delivers 100% automated threat detection and blocking, is deployed in minutes, is 100% SaaS, and requires no new hardware, no software to install, no agents, and no cyber security analysts needed to operate.

Dark Cubed operates by receiving the syslogs from the on prem firewall. Each external IP address seen in the traffic is given a risk score based on several factors. By default if Dark Cubed sees traffic to or from an external IP address rated 8 or greater it will amend the blocklist of the internal firewall to include that IP address.

District does not have an on prem firewall?….always recommend on site firewall because:

- Control at the perimeter of district network.
- Ability to do IDS/IPS directly at district's connection to the outside world
- Ability to apply bandwidth shaping, content filter, etc
- Geo-Blocking
- Option to add VPN
- Anti-malware / Anti-Spyware protections
- *Protection from upstream peer networks / shared networks (Eg…what we sometime see at the ITC's doing - not best practices.) - Chris Infante*

Dark3 Further Learning Resources

Dark3Celerium's DarkCubed Demo - Channel Pitch April 2022 (youtube.com)

https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION

RISK ASSESSMENT — 18 Risk Categories

SECURITY TRAINING
vCISO

Cybersecurity Risk Assessment - What is it?

A cybersecurity risk assessment is an assessment of an organization's ability to protect its information and information systems from cyber threats. **The purpose of a cybersecurity risk assessment is to identify, assess, and prioritize risks to information and information systems**. A cybersecurity risk assessment allows you to do this by identifying the cyber risks that affect your security posture, leading to more informed decision-making on how best to allocate funds to implement security controls and protect your environment.

Security Assessment

Comprehensive analysis of district-wide cybersecurity posture designed for K-12 environments.

18 Critical Risk Categories

- Inventory
- Endpoint Security
- Software
- Account Security
- Network Security
- Banking
- Antivirus
- Firewall
- Content Filter
- Backups
- Maintenance
- Data
- Authentication
- Closet Security
- Training
- Policy
- Assessment
- Insurance

Talking Points

IMPORTANT DIFFERENTIATOR: The Xpel SOC security professionals developed (and continue to improve) a comprehensive Risk Assessment. The assessment covers 18 risk categories and while it is based on CIS controls it also includes ***K-12 specific questions designed to reveal vulnerabilities unique to K-12 environments***. Each question has an impact and probability score as well as actionable remediation instructions.

The assessment is both a standalone engagement as well as a part of the critical infrastructure package. For Xpel Managed customers, the assessment is initially conducted during the onboarding and annually thereafter. It serves as a benchmark for year over year organizational-wide cyber posture metrics as well as a roadmap throughout the year to continually address vulnerabilities.

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR

SIEM

24/7/365 SOC MONITORING

VULNERABILITY MANAGEMENT

DARK WEB MONITORING

INTRUSION DETECTION AND PREVENTION

RISK ASSESSMENT

SECURITY TRAINING

vCISO

Phishing Threat Simulations and User Awareness Training

KnowBe4

Security Focused Training

The Xpel Cyber Hub is a one-stop shop for all your cyber training needs.

Click the links to check out the Cyber Hub as well as our overview video on how to use the Cyber Hub.

Cyber Hub Portal

Cyber Hub Video



Security Awareness Training



Professional Development



Phishing Threat Simulations



Tabletop Exercises

Realistic intent scenarios to test Incident Response Teams

Talking Points

1. **Phishing serves multiple purposes -**
   a. Training to identify threats and
   b. Creates a line of defense at the end of the keyboard where end users report not only simulations BUT also identify and report actual email threats. These reports result in EML tickets created for the Xpel SOC to investigate. Then, if warranted, the SOC adds the hash to the Xpel EDR and domain blocklists.

2. **Phish Alert Button Benefits:**
   - Reinforces the district's security culture
   - Users report suspicious emails with just one click (the hook icon)
   - Xpel SOC team gets early phishing alerts from users, creating a network of "sensors"
   - Email is deleted from the user's inbox to prevent future exposure
   - Easy deployment via MSI file for Outlook and GSuite deployment for Gmail (Chrome) - AD syncing

3. **Comprehensive library containing themed modules featuring:**
   a. **Animated Videos**
   b. **Cyber Tip Tuesdays**
   c. **Bell Announcements**
   d. **Technical Articles**

IMPORTANT DIFFERENTIATOR: The Xpel SOC security professionals investigate tickets generated by end user phishing reports that are NON simulations. ***Every ticket created is investigated, resolved and if warranted, added the hash to the Xpel EDR and domain blocklists - effectively turning the largest threat vectors (end-users at the keyboard) into an impactful frontline of defense***. The Xpel CyberHub provides access to a full library of training resources developed specifically for K-12 employee user awareness security training.

Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR
SIEM
24/7/365 SOC MONITORING
VULNERABILITY MANAGEMENT
DARK WEB MONITORING
INTRUSION DETECTION AND PREVENTION
RISK ASSESSMENT
SECURITY TRAINING

vCISO

Security Policy Support for District Administration & IT

vCISO What is it?

Virtual CISO and Process Review -

Development of Best Practices that will contribute to a continually improving cybersecurity posture ideally designed to meet the goals of the first implementation group of the Center for Internet Security (CIS) framework.

vCISO
virtual Chief Information Security Officer

Strategic Planning and Annual CSR

Lifecycle Management & Fiscal Forecasting

NIST/CIS Alignment - Policy Support

Incident Response Playbook Development

Data Privacy Compliance

Security Assessment

Comprehensive Analysis of Organizations Cybersecurity Posture - 18 Critical Risk Categories

Network Audit

Comprehensive Analysis of IT infrastructure
Penetration Testing: Internal & External

NIST / CIS Alignment - Security Policy Support

Development of Security Policy and Procedures Best Practices that will contribute to a continually improving cybersecurity posture designed to meet the goals of the first implementation group of the Center for Internet Security (CIS) controls.

Policy List

- Change Management
- Cloud Computing
- Code of Ethics
- Data Access and Password
- Data Classification
- Data Retention
- Encryption
- Facility Security
- HR Corrective Action
- Human Resource Security
- Information Security
- Information Security Risk Assessment
- Interconnection Agreement
- Logging and Monitoring
- Perimeter Security and Administrative
- Policy of Standard Exception Request Form
- Policy of Standard Exception Request Procedure
- Policy of Standard Variance
- Security Incident Response
- Service Provider Security
- Social Media
- Software Development
- System Configuration
- Telecommuting
- Vulnerability Identification
- System Updates

vCISO
virtual Chief Information Security Officer



Talking Points

1. **Incident Response Planning**

2. **CSR - Annual**

3. **Data Privacy Compliance**

FERPA (Family Educational Rights and Privacy Act) is the main federal statute governing student data privacy. It mandates that schools safeguard education records and grant parents access to them. Essentially, FERPA defines what information schools can collect, maintain, and disclose, with or without consent from students or their parents.

CIPA (Children's Internet Protection Act). While content filters are commonly used for CIPA compliance, they may not fully protect student data stored in cloud storage. CIPA aims to prevent unauthorized disclosure, use, and dissemination of personal information regarding minors

Protection of Pupil Rights Amendment outlines restrictions related to student privacy in federally funded surveys or evaluations. Schools funded under the Individuals with Disabilities Education Act must also ensure the confidentiality of personally identifiable information.

Why is compliance important?

If a school breaches FERPA, it can lead to an investigation by the U.S. Department of Education. To comply, schools must take reasonable precautions to prevent unauthorized access to student records, such as using encryption for emails and maintaining robust firewalls

CISO and Data Privacy Compliance Further Learning Resources

https://edtechmagazine.com/k12/article/2022/04/understanding-ferpa-cipa-and-other-k-12-student-data-privacy-laws-perfcon

https://www.forbes.com/sites/technology/article/chief-information-security-officer-ciso/

Overcoming Objections



1. No Funds

Cyberattack Incidents are COSTLY

- **Detection and Containment Costs:** Expenses related to identifying and containing the breach, including incident response efforts, investigations, and security measures.
- **Post-Breach Response Costs**: Legal fees, P.R./communication with affected parties, and reputation management contribute to this category.
- **Notification Costs:** Notifying affected individuals and regulatory bodies about the breach incurs costs
- **Credit Monitoring Costs**
- **Other cost examples**: Payroll failure - costs related to cover insufficient funds banking fee for staff.

According to a 2023 U.S. Government Accountability Office report
(a.) the loss of learning following a cyberattack ranged from three days to three weeks, and recovery time can take anywhere from two to nine months.
(b.) The monetary losses to school districts following a cyber incident ranged from $50,000 to $1 million.

https://www.schoolsafety.gov/sites/default/files/2024-02/SchoolSafety.gov%20Cybersecurity%20Resources%20for%20K-12%20Schools%20and%20School%20Districts%20Infographic_February%202024_508C.pdf

2. “Already have some controls in place w/ term contract.”

Most current Xpel client districts have had partial controls in place at the time they engaged our managed cybersecurity services.

Reduced license costs and the value of the overall critical infrastructure support more than offset existing security spend.

Majority of districts see the value in the typical “double-spend” on their existing licenses for critical devices (almost always EDR-related).

3. ITC / ISD has me covered.

State-funded ITC's reduce your security posture to the common denominator or a universal baseline on which bad actors quickly understand how to circumvent and capitalize.

ITC's cybersecurity offerings remain underfunded and under supported. They most often rely on partial controls (maturity assessments, limited EDR deployment, external vulnerability scanning, email content filtering, etc.) and are not in alignment with best practices and almost always offer no 24/7 SOC monitoring and log analytics. Increasingly, we see SOC-in-a-box automated solutions being introduced into K-12 environments which provide a false sense of monitored security as these tools do not address the unique challenges and threats to K-12.

4. My stuff is in the cloud - no data to protect.

The Xpel SOC Team is observing more and more schools rely on web applications for their sensitive data (i.e. SIS systems, transportation software and finances). Districts often respond "No" on the Xpel assessment to internally hosting databases and when asked if they separate guest and student traffic (VLans) from important systems, they state that is all hosted. If critical infrastructure is being hosted in the cloud and through web applications then student and guest devices can access that infrastructure by going to the website associated with it. Previously the critical infrastructure was hosted on an internal server that was segregated and it was best practice to not allow student and guest access. That infrastructure as since moved to web applications with insecure access. (Further research: Snowflake Snowflake Breach Exposes 165 Customers' Data in Ongoing Extortion Campaign (thehackernews.com), Illuminate Data Security Incidents (nyc.gov) etc.)

Cloud data storage is less secure than widely understood; security breaches can occur due to various factors - leading causes include:

1. Phishing Attacks: Cybercriminals use deceptive emails or messages to trick users into revealing sensitive information. These attacks often lead to data exposure or malware downloads.
2. Malicious Insider Actions: Employees with privileged access may intentionally compromise security by leaving backdoors open or installing malware.
3. Misconfigured Access Controls: Improperly configured permissions (e.g., publicly accessible buckets) can expose data to unauthorized users.
4. Unencrypted Data: Storing data without encryption increases the risk of breaches if attackers gain access.
5. Human Errors: Mistakes like sharing sensitive information without restrictions or misconfiguring settings contribute to breaches.

4. My stuff is in the cloud - no data to protect.

We are seeing more and more schools lean more on web applications for their sensitive data like their SIS systems, transportation software and finances. When going through our assessment they answer "No" to hosting databases. And when we ask them if they separate guest and student traffic from important systems, they state that is all hosted.

Security Differences of Cloud Storage vs Local Storage

Cloud storage utilizes remote servers accessed through the internet, while local storage saves data on physical devices directly connected to a user’s device. It excels in remote access, scalability, and security, with distributed storage options and privacy adherence capabilities. Local storage prioritizes direct access, potential cost savings, and reduced reliance on the internet, yet lacks the scalability and security of the cloud.

Here’s the difference between cloud and local storage in terms of accessibility, distribution, security measures, and more:

	Cloud Storage	Local Storage
Data Storage & Accessibility	Hosted on remote servers; accessible via third-party APIs and internet connectivity; access anywhere.	Data is stored on physical mediums (SSDs, HDDs, and USBs), restricting access to specific devices and requiring physical transfer for mobility.
Distribution & Downtime	Uploaded data is divided into blocks and distributed across servers; downtime considerations include poor internet connectivity, power outages, and service maintenance.	Not reliant on the internet; with rapid on-premise access; vulnerable to unanticipated calamities such as fires or floods.
Remote Access & Security Measures	Remote access is enabled; possible security problems resolved by cloud provider protocols; shared resources may affect performance.	Remote access requires VPNs or RDP; provides complete control over data storage, access, and security protocols.
Privacy Regulations & Compliance	Compliance certifications like HIPAA and GDPR are available but within the company's control; regulated data should be safely stored.	With complex compliance processes, requiring firms to create and run protocols for regulated data.
Confidential & Semi-Private Files	Legally protected files should be stored on compliant cloud platforms; industry-specific security procedures required for confidential files.	Highly sensitive files should be stored in purpose-built systems; semi-private files can be stored with strict controls and training.
Data Security & Recovery Measures	Reliable CSPs provide high-level security and backup services; in the event of data loss, recovery is possible.	Users have direct control over data security but are also responsible for backup procedures and permanently lost data in the event of device damage or loss.
Scalability & Infrastructure	Scalable and flexible based on requirements.	Expansion involves getting new hardware, which can be potentially slower or more expensive.
Internet Connectivity & Performance	Data transfer is dependent on good internet access; shared network resources may have an impact on performance.	Not reliant on the internet; data transport and performance are more localized, with possible scaling issues.
Cost & Maintenance	Monthly/annual costs with maintenance handled by the supplier, resulting in cost savings.	Upfront hardware costs, continuous maintenance, and potential repair/replacement costs.

5. Waiting for Federal/State support.

State and Federal “sponsored controls” reduce your security posture to the common denominator or a universal baseline on which bad actors quickly understand how to circumvent and capitalize.



“You don’t have to run faster than the bear to get away. You just have to run faster than the guy next to you.”

– Jim Butcher

6. No “buyin” from administration

Administrators can be motivated by the following considerations:

The implications of escalating cybercrime are far-reaching. Administrators should be most concerned about meeting their responsibilities regarding:

The prevention of fiscal loss from ransomware and fund transfer fraud.

The prevention of exfiltration of sensitive data; IEP’s, PII, SS#’s, etc. and compliance with federal and state data privacy laws.

The prevention of disruption to instruction and operations due to network outages and ensuing technology unavailability.

The Xpel team can assist in engaging your Administration.

- An assessment is a great tool to engage administration.
- Communicate costs of an incident (learning loss, reputational damage, legal exposures, etc)
- Data Privacy compliance - “Safe Harbor” for districts that reasonable conform to cyber frameworks
- Cyber liability insurance - qualifying for coverage

7. Endpoint Access Cloud SaaS

Software-as-a-Service (SaaS) applications offer scalability and convenience, but they also come with security risks. Here are some common vulnerabilities:

1. Flaws in Multi-Tenant Architecture:
    - SaaS applications use a multi-tenant architecture, where data from different customers resides on the same server.
    - If the isolation between tenants is weak, a flaw in the system could allow one tenant to inadvertently access another's data, compromising confidentiality and leading to data leakage.
2. Open Access from Anywhere:
    - Since SaaS apps can be accessed from any location, there's a high risk of unauthorized access.
    - Attackers might exploit weak passwords or use phishing scams to acquire user credentials, undermining data integrity and potentially allowing unauthorized viewing, modification, or deletion of sensitive information.
3. Security Misconfigurations:
    - SaaS software provides security controls, but these controls are often misconfigured or not defined correctly.
    - A single administrator error or omission can expose highly sensitive data and business functions to the public Internet.

To mitigate these risks, organizations should adopt a multi-faceted approach, including robust policies, technologies, and continuous monitoring for SaaS security.

Xpel by Forward Edge Presentation Preparation

A.) Information that can be collected w/out prospect input:

- Number of Students:
- Number of Faculty:
- Number of Admin (Estimate Guidance:):
- Number of Buildings:

B.) ESTIMATED LICENSE COUNTS (See next page):

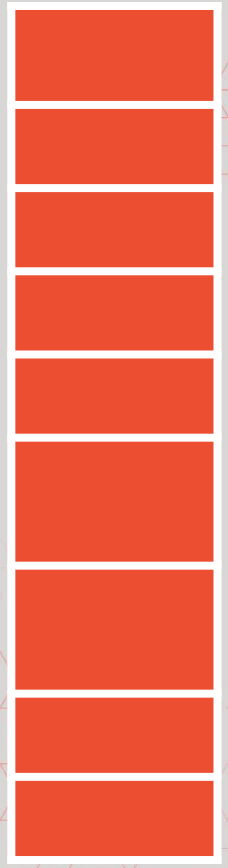
Servers - Virtual and Physical (Estimate Guidance:):
vCenter/ESXi Servers (Estimate Guidance:):
Core / Routing Switch (Estimate Guidance: 1 Per Building):
On-Prem Firewall (Estimate Guidance: 1 Firewall P/):

C.) OTHER USEFUL DISTRICT PROFILE DATA POINTS:

ITC:
ESC:
Purchasing COOPs memberships (Equalis, Buyboard, etc:
ERate %:
INSURERS/Cooperative:

General Notes:

- Known Security Controls already Deployed (EG: Indiana districts have free KnowB4):
- Grants or Funding sources available?
- Research in-region breaches in recent news.



- Windows/ Mac/ Linux Servers (Virtual and Physical)
- vCenter / ESXi Servers
- Firewall - In District
- Core Switches (Routing Enabled)
- Superintendent Suite - Laptops/ Desktops
- Treasury Suite / Business Manager - Laptops/ Desktops
- Other Admin Staff (Secretary/ Principal/ Nurse/ IT Department)
- Total Staff Email Account (All but Students)
- *Physical Vulnerability Scanner Required

MITRE ATT&CK



ATT&CK is knowledge base of adversarial techniques based on real-world observations. ATT&CK focuses on how adversaries interact with systems during an operation, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

What Does ATT&CK Stand For?

ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). MITRE Engenuity ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

Watch this: Get Started | MITRE ATT&CK®

What is the MITRE ATT&CK Framework? - An Easy Guide (sentinelone.com)

Threat Actor Tactics and Techniques



Attack Scenarios

SCENARIO: “INITIAL ACCESS” Bad Actor gains initial access:



A. Exploits Vulnerability
B. Phished Credentials
C. Leaked Credentials (search code repositories / query credentials)

DEFENSE TACTICS
MFA
Patching
Inventory & Protect externally exposed access portals
Password Hygiene (using different passwords for different websites, long and strong passwords, etc.)



Attack Scenarios

SCENARIO: “RESOURCE DEVELOPMENT” Bad Actor gains initial access through:



A. Creation of fake personas
B. Acquiring infrastructure - obtaining necessary servers/domains
Note: Bad actors have all different skills available to them now through the market/ It is now an organized and consolidated “big” business to support bad actor in cyber crime through skill set resources for sale such as “Credential Stealers”, “Landing Ransomware” skill sets, etc.)

DEFENSE TACTICS

A. Domain Monitoring (monitor for typosquatting/URL hijacking/subdomain takeover)
B. Threat Intel Sharing (stay informed)
C. Block Web Traffic (newly registered domains/parked [unused] domains)



Attack Scenarios

SCENARIO: “EXECUTION” Bad Actor initiate:



Run malicious code

- **Botnets**
- **Malware**
- **Ransomware)**

DEFENSE TACTICS

A. **PAM**
B. **EDR - Behavior Monitoring**
C. **Application whitelisting - prevent unauthorized programs from running**



Attack Scenarios

SCENARIO: “PERSISTENCE” Bad Actor establish a lasting presence (Living off the Land / Dwell Time)



For example:
A. Install “backdoors” - gain unauthorized access to system
B. Modify system configurations (scheduled tasks/registry changes/startup modifications)

DEFENSE TACTICS

A. Continuous monitoring of privilege access accounts
B. Strong access management policies
C. Endpoint monitoring
D. Egress network traffic monitoring



Attack Scenarios

SCENARIO: “PRIVILEGE ESCALATION” Bad Actor escalate privilege through:



A. Exploiting system vulnerabilities (Misconfigured systems/scheduled tasks)
B. Credentials dumping (process of extracting)

DEFENSE TACTICS

A. **Least Privilege Access Management**
   (Zero Privilege Accounts/Just-In-Time Accounts/Rotate)
B. **Endpoint Detection**



Attack Scenarios



SCENARIO: “PRIVILEGE ESCALATION” - Mimikatz

Mimikatz is a well-known tool used for post-exploitation activities in cybersecurity, particularly for extracting credentials from memory on Windows systems. “Memory Dumps” refer to the process of capturing the contents of a computer’s memory (RAM) to analyze and extract sensitive information, such as passwords, security tokens, and other credentials.

Here’s a brief overview of how Mimikatz can be used with memory dumps:

1. **Dumping Memory**: Tools like ProcDump or Task Manager can be used to create a memory dump of a process, such as lsass.exe, which handles authentication on Windows systems.
2. **Analyzing the Dump**: Mimikatz can then be used to analyze the memory dump file to extract credentials. This is done using specific commands within Mimikatz.

For example, the command to analyze a memory dump might look like this:

```
mimikatz # sekurlsa::minidump lsass.dmp
mimikatz # sekurlsa::logonpasswords
```

This process is often used by security professionals during penetration testing to identify vulnerabilities, ***but it can also be exploited by malicious actors.***

Attack Scenarios



SCENARIO: “PRIVILEGE ESCALATION” - Mimikatz

Bad actors use Mimikatz to exploit vulnerabilities in Windows systems and extract sensitive information, primarily credentials. Here are some common ways they leverage this tool:

1. Credential Extraction: Mimikatz can retrieve plaintext passwords, hashes, PIN codes, and Kerberos tickets from memory. This allows attackers to gain unauthorized access to systems.
2. Pass-the-Hash Attacks: Attackers use Mimikatz to extract password hashes and use them to authenticate without needing the actual password. This technique is known as pass-the-hash.
3. Pass-the-Ticket Attacks: Mimikatz can manipulate Kerberos tickets, allowing attackers to move laterally within a network using stolen tickets. This is known as pass-the-ticket.
4. Golden Ticket Attacks: Mimikatz can create forged Kerberos tickets, known as Golden Tickets, which give attackers persistent access to a network by impersonating any user.
5. DCSync Attacks: Mimikatz can simulate a Domain Controller (DC) replication request to fetch sensitive account information, including NTLM hashes, without directly interacting with the DC.

Looking Forward

Threat Landscape

- Broadening of K-12 Attack Surfaces
- Russia-Ukraine Conflict
- Growing Adoption of Third-Party Vendors
- Dark AI (AI used to enable or create cyber attacks)

Data Privacy Law and Cyber Liability Insurance

- K-12 required to adopt Framework - NIST (CIS Controls)
- Safe harbor may no longer apply with data exfiltration events
- Mandatory incident reporting.
- Cyber and Ransomware coverage premiums not expected to ease.

Funding

- $200 Million Pilot - 3 Year
- SLCGP - State & Local Cybersecurity Grant Program ($985 million through 2025)
- ERate

Technology

- Adaptive MFA and Biometric Authentication
- Passwordless Authentication (PAMS/IAMS)
- SOC in a BOX
- SOAR -Security Orchestration, Automation and Response (FE SOC - Internal)
- CWPP - Cloud Workload Protection Platform

More Learning Resources!

National Institute of Standards and Technology (nist.gov)

The 18 CIS Critical Security Controls (cisecurity.org)

MS-ISAC (cisecurity.org)

K12 Security Information eXchange (K12 SIX)

Ohio Cyber Range Institute | OCRI

CoSN | Home

CISA K-12 Safeguards

More Learning Resources!

https://edtechmagazine.com/k12/article/2024/06/istelive-24-takeaways-national-cybersecurity-framework-k-12

More Learning Resources!

Check out our FREE Resource Page!

bit.ly/freefedge

National Cybersecurity Alliance's Online Safety Basics

bit.ly/3rRyS9S

CISA's Awareness Toolkit

bit.ly/3EE6LT8

Xpel SOC WINS

Threat Intel Feed and Qualys Scanner Received Threat Intel about CVE-2023-27532. The FIN7 Ransomware Group has been seen exploiting vulnerability. SOC then used Qualys to search for vulnerabilities across all customers. Found that **[CLIENT-DISTRICT REDACTED**] had 2 devices affected by the vulnerability. Once found SOC then notified the TC, **[CLIENT-DISTRICT REDACTED]** of the vulnerabilities and the affected devices with instructions on how to remediate the vulnerability.

Threat Intel Feed and Qualys Scanner Received threat intel about CVE-2023-20178 being actively exploited in the wild. SOC used Qualys to search for that vulnerability and found that 5 devices at **[CLIENT-DISTRICT REDACTED**] are affected. SOC communicated the vulnerable device info to **[CLIENT-DISTRICT REDACTED]** to be remediated.

Escalated Alert from Perch Received a phone call from the Threat Hunting team and had the device quarantined within 3 minutes. [**CLIENT-DISTRICT REDACTED]** re-imaged device and resolved. The malware that was associated with this was tied to SocGholish.

Perch Alert Perch Alert for Failed logins against their firewall. After investigation found it to be a brute force/password spray attack. Was able to contact the **[CLIENT-DISTRICT REDACTED]** Tech admin and get the seen IPs blocked as well as Non-US sources.

Perch Alert Perch Alert for Failed logins against their RDP gateway. Contacted managed services to ensure IIS logging and was able to find the IP of the bruteforce/password spray attack and communicate that to **[CLIENT-DISTRICT REDACTED]**. After initially blocking all Non-US sources, it was revealed that it was also getting hit by US sources and a decision was made to remove RDP and RD Web Access from the device.

Xpel SOC WINS

Perch Alert Perch Alert for failed logins. After investigation found an ongoing brute force attack from 5 different countries on the device Skyward. Worked with **[CLIENT-DISTRICT REDACTED**] to stop and mitigate the attack and change some device configurations for better device hardening.

Phishing reporter Investigated email sent in by several teachers at [CLIENT-DISTRICT REDACTED]. It was coming from their A site, **[ISP REDACTED**]. The email contained a link to a page that asks for the user's email, domain username and password. SOC sent **[CLIENT-DISTRICT REDACTED**] an email and called him to leave a voicemail.

Perch Alert Perch alert for failed logins. Investigated and found brute force attack coming from multiple countries. Worked with Managed Services to find and fix the configuration issue, RDP open to the internet, and stopped the brute force attack.
Perch Alert Perch Alert for failed logins. Investigated and found brute force attack coming from multiple countries. Notified [CLIENT-DISTRICT REDACTED] and recommended configuration changes. **[CLIENT-DISTRICT REDACTED]** made the changes and stopped the attack.

Perch Alert Perch alert for created user and user set password to never expire. Through an investigation we found the device dhcp1 was under active exploitation from a newly released vulnerability in the software SCreenConnect. Worked with the **[CLIENT-DISTRICT REDACTED]** to remove the attackers access and clean up artifacts. Prevented what could have very easily become a ransomware situation.

SentinelOne Alert S1 alert triggered for lateral movement. From [**CLIENT-DISTRICT REDACTED]** - In reviewing the firewall logs, we had 2 compromised staff accounts (non admin), which were being used to log into the vpn to access our network. Both logins originated from the same computer in Canada. Both accounts have been deactivated and passwords changed. Additional restrictions have been enabled on our firewall to limit vpn access.

Phishing reported from Reporter **[CLIENT-DISTRICT REDACTED]** has had several compromised student accounts recently. This one was a compromised staff account that SOC was able to identify. **[CLIENT-DISTRICT REDACTED]** decided to mandate Google 2FA moving forward!

Xpel SOC WINS

Phishing reported from Reporter Investigated phishing email reported by staff member, found compromised student account sending phishing emails.

Perch Alert Discovered Wave Browser.exe on a staff machine, able to add new hash to S1 to mitigate on the alerting device as well as detecting on other devices across multiple districts

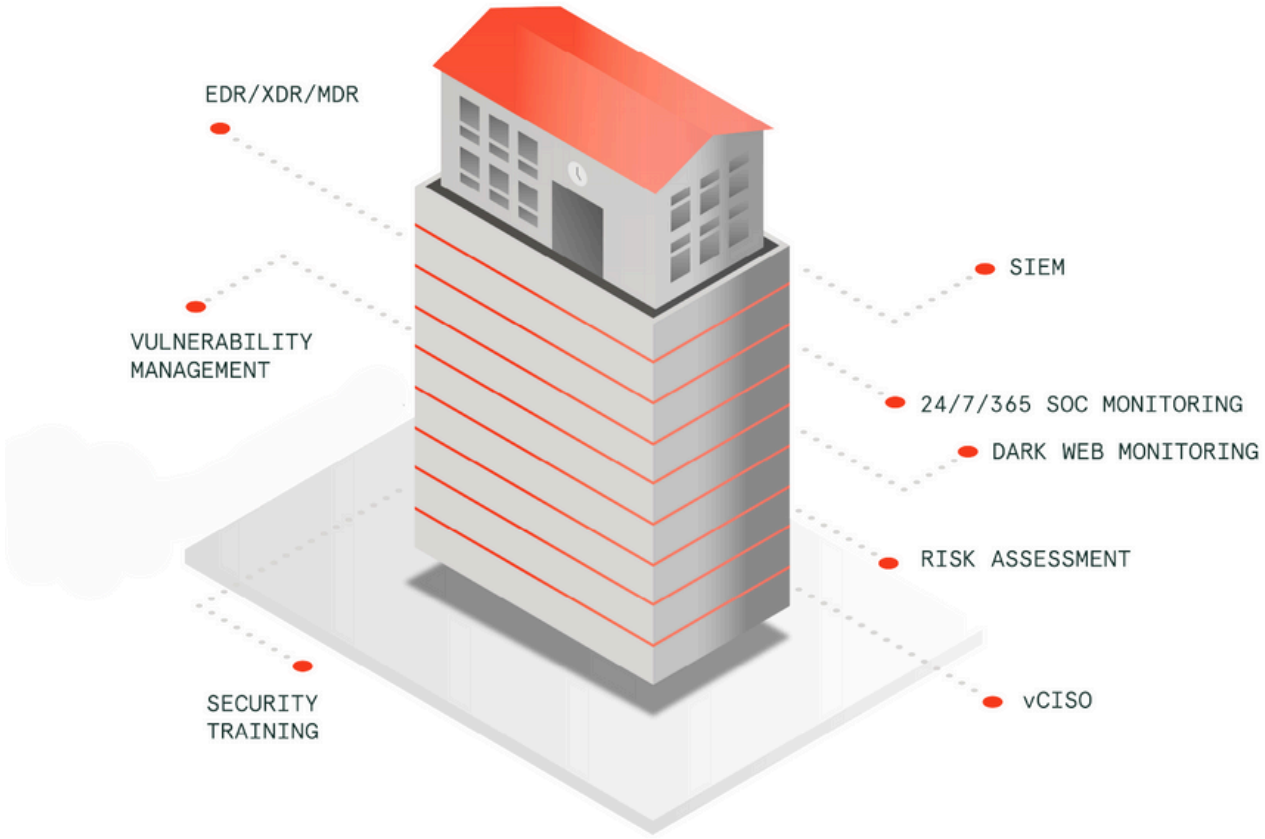
Perch Alert Discovered Ongoing Brute Force Attack on the internet facing device choco. Malicious RDP connections primarily coming from foreign and U.S. sources. Coordinated with **[CLIENT-DISTRICT REDACTE**D] to mitigate threat and block RDP on that device over the internet.

Cybersecurity Essentials Package

xpel by Forward Edge

Don't dismiss cyberthreats. Dismantle them.

Xpel by Forward Edge is a proactive, ***Defense in Depth*, layered approach to K-12 cybersecurity** designed to protect networks and systems from cyber threats such as hacking, ransomware, and data breaches. In alignment with the Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST) cybersecurity framework controls, the Xpel security suite **protects, detects and responds.**



Cyber funding is available - Ohio's State and Local Cybersecurity Grant Program (SLCGP) Applications are due September 16th, 2024!

Safeguard Your District with Xpel Cyber Essentials!
Email us at info@xpelcyber.com to recieve a custom quote in 1 business day or less.

Xpel Essentials

Cybersecurity Protection for K-12 Education

xpel by Forward Edge

Feature	Description	Qty	Included
EDR	Endpoint Detection and Response w/ 24/7/365 Monitoring SentinelOne	Up to 15 Critical Infrastructure Devices	☑
SIEM	Security Information Event Management [SIEM] software to actively aggregate, correlate and monitor syslog activity	Up to 15 Critical Infrastructure Devices	☑
SOC 24/7/365	Xpel SOC Continuous Monitoring and Prevention 24/7/365 xpel by Forward Edge	Included	☑
Dark Web Monitoring	Continuous Dark Web Monitoring	Up to 5,000 IP's	☑
Vulnerability Management	Internal and External Vulnerability Management Qualys.	All District Domains and subdomains	☑
Annual Risk Assessment	Annual Risk Assessment xpel by Forward Edge	Included	☑
vCISO	vCISO Advisory to Strategic Planning and NIST/CIS Alignment, Incident Response Playbook Development, Data Privacy Compliance, etc. xpel by Forward Edge	Included	☑
IDS/ IPS	Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) from Celerium	Optional	
Phishing Threat Simulations	Phishing Threat Simulations from KnowBe4	Optional	
	XPEL ESSENTIALS ANNUAL FEE	**$16,250**	

Forward Edge Corporate Technology Certifications - 2024

Google Educator 2	Lenovo Support	Microsoft MCDE	Extreme EDS Wireless Cloud
Google Admin	Apple ACMT	Microsoft MCIT	Extreme EDS IP Campus
Testout Network Pro	Cisco CCNA	Microsoft MCP	Extreme ECS Wireless Cloud
Testout PC Pro	Google Innovator	Axis ACP	Extreme EDS Campus Fabric
Testout Client Pro	Qualys Vulnerability Management Specialist	ICAgile Project and Delivery Management	Barracuda Backup Certified Engineer
Dell Support	Extreme EDS Management Center	Extreme EDS Wing Wireless	Extreme ECS Campus EXOS
HP Support	Extreme ECS Management Center	Extreme EDS Control	Extreme ECS Access Wireless
Extreme ECS Wireless CORE	ICAgile Certified Professional	StorageCraft Master Engineer	ITIL v3 Foundation Certification
S2 Certification	CompTIA Network+	CompTIA A+	CompTIA Network Vulnerability Assessment Professional
CompTIA Security+	CompTIA Pentest+	CISSP	

Xpel Security Operations Center Certifications - 2024



CISSP



GCIA



GCIH



GCFA



OSCP



CompTIA



Security +



GSLC



GPEN



GWAPT

Forward Edge
The technology edge for education

Cybersecurity References

Greensburg Community Schools - *2,157 students*
Scott Hershauer, Director of Technology
shershauer@greensburg.k12.in.us
(812) 663-4774 ext. 1702

Deer Park Community Schools - *1,238 students*
Cybersecurity Customer
Jay Phillips, Superintendent
phillips.j@dpccsd.org
(513) 891-0222

Tecumseh Local Schools - *1,238 students*
Cybersecurity Customer
Jay Phillips, Superintendent
phillips.j@dpccsd.org
(513) 891-0222

Reading Community School District - *1,656 students*
Cybersecurity Customer
Colette Lewis, Treasurer
clewis@readingschools.org
(513) 554-1800

Wyoming City Schools - *1,975 students*
Cybersecurity Customer
Ronda Johnson, Treasurer
johnsonr@wyomingcityschools.org
(513) 206-7000

Forward Edge
The technology edge for education



West Clermont Local Schools - *8,008 students*
Cybersecurity Customer
Larry Parece, Directory of Technology
parece_l@westcler.org
(513) 943-5000

Part E – Signature Forms

AEPA 025-E
Security Solutions

Instructions

Contained herein are forms that **require a signature** from an authorized person at your company. All items found within this document are **mandatory**. Failure to sign the required areas, sections, or signature lines may lead AEPA to consider your company's proposal as **non-responsive**.

To submit the required signed forms, follow these steps:

1. Read the documents in their entirety.
2. Complete all forms and sign when required.
3. Return the forms and pages in their correct order and scan one (1) single PDF format titled ***"Part E – Signature Forms – Name of Responding Company"*** (i.e. one PDF document for all signature forms).
4. Submit Part E, along with other required documents in Bonfire.

*Note, a solicitation checklist has been provided to review with your submission.

The following sections will need to be completed prior to submission as one (1), single PDF titled "Part E – Signature Forms – Name of Responding Company".

Uniform Guidance "EDGAR" Certification Form – ****signature required***
Solicitation Affidavit – ****signature required***
Acceptance of Solicitation & Contract – ****signature required***

Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7. Clean Air Act and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended, contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein.		
Respondent Certification (By Item)	**Respondent Certification:** **YES**, I agree	**Initial**
1. Violation of Contract Terms and Conditions	Yes, I agree	CLL
2. Termination for Cause of Convenience	Yes, I agree	CLL
3. Equal Employment Opportunity	Yes, I agree	CLL
4. Davis-Bacon Act	Yes, I agree	CLL
5. Contract Work Hours and Safety Standards Act	Yes, I agree	CLL
6. Right to Inventions Made Under a Contract or Agreement	Yes, I agree	CLL
7. Clean Air Act and Federal Water Pollution Control Act	Yes, I agree	CLL
8. Debarment and Suspension	Yes, I agree	CLL
9. Byrd Anti-Lobbying Amendment	Yes, I agree	CLL
10. Procurement of Recovered Materials	Yes, I agree	CLL
11. Profit as a Separate Element of Price	Yes, I agree	CLL
12. General Compliance with Participating Agencies	Yes, I agree	CLL
13. Governing Law; Forum Selection.	Yes, I agree	CLL

Forward Edge, LLC.

Name of Business

Charles L. Logan Jr.

Signature of Authorized Representative

Charles L. Logan Jr.

Printed Name

09-30-2024

Date

Solicitation Affidavit

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

Charles L. Logan Jr.	2724 East Kemper Road
Authorized Representative (Please print or type)	Mailing Address
COO	Cincinnati, Ohio 45241
Title (Please print or type)	City, State, Zip
Charles L. Logan Jr.	09-30-2024
Signature of Authorized Representative	Date

Acceptance of Solicitation & Contract

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	Forward Edge, LLC.	**Date**	09-30-2024
Address	2724 East Kemper Road	**City, State Zip**	Cincinnati, Ohio 45241
Contact Person	Denise Caccavari	**Title**	Director of Cybersecurity Solutions
Authorized Signature	Charles L. Logan Jr.	**Title**	COO
Email	clogan@forward-edge.net	**Phone**	513-761-3343

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Solicitation Checklist

Instructions: Utilize the checklist below, reviewing to confirm that all the required documents have been uploaded to Public Purchase, in their ***specified/required format***, by the due date and time listed for this solicitation. ***Submissions not following the specified/required format may result in being marked non-responsive and may not be considered for evaluation.*** Respondents are reminded that failure to follow, comply with, and adhere to the enclosed instructions of this solicitation may result in their response being deemed non-responsive. AEPA, its Member Agencies, affiliate agencies, and authorized representatives are not responsible for bid proposals that are incomplete, unreadable, or received after the solicitation deadline submission date.

"x"	**Document Title, Uploaded to Bonfire** *(Respondent must submit documents in the required title/format)*	**Format of Uploaded Document**	**Notes**
	Bid Bond – if Required, see Part A if applicable.	Upload PDF copy of the bid security.	The original bid security must be received by Lakes Country Service Cooperative by due date and time.
	Part C – State-Specific Forms – ***Name of Responding Company***	Single, Scanned PDF	**New Jersey Only Requirement.** Signatures Required.
	Part D - Questionnaire – ***Name of Responding Company*** Includes: ● Company Information ● Service Questionnaire ● Exceptions ● Deviations	Single, Scanned PDF	**Required.**
	Part E – Signature Forms – ***Name of Responding Company*** Includes: ● Uniform Guidance "EDGAR" Certification ● Solicitation Affidavit ● Acceptance of Solicitation & Contract	Single, Scanned PDF	**Required.** Signatures required.
	Part F – Pricing Schedule – ***Name of Responding Company***	Excel Workbook	**Required.**
	Price List and/or Catalog – ***Name of Responding Company***	Upload PDF	**Required.**
	Exhibit A – Marketing Plan – ***Name of Responding Company***	Scanned PDF	**Optional.** Form not provided by AEPA, Respondent Created

Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7. Clean Air Act and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended, contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Solicitation Affidavit

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

JOHN WALTZ
Authorized Representative (Please print or type)

2724 E KEMPER ROAD
Mailing Address

CEO
Title (Please print or type)

SHARONVILLE, OHIO 45241
City, State, Zip

Signature of Authorized Representative

09/12/2024
Date

Acceptance of Solicitation & Contract

Association of Educational Purchasing Agencies

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	FORWARD EDGE	**Date**	09/12/2024
Address	2724 E KEMPER ROAD	**City, State Zip**	SHARONVILLE, OH 45241
Contact Person	DENISE CACCAVARI	**Title**	DIRECTOR, CYBERSECURITY SOLUTIONS
Authorized Signature	[signature]	**Title**	CEO
Email	jwaltz@forward-edge.net	**Phone**	513.761.3343

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Contents

1-Exhibit A- Marketing Plan- ResoluteGuard LLC 1
1-Affirmative Action Policy 2
2-Price List and Catalog- ResoluteGuard LLC 3
3-Exhibit B- vCISOSecure Overview 4
4-Exhibit C-vCISOSecure- ESA 6
1-(Amd) ResoluteGuard LLC Amended Part E Signature Forms 7
Part E- Signature Forms- ResoluteGuard LLC.pdf 13
Part E- Signature Forms- ResoluteGuard LLC.pdf 13
21-F - Cyber Security Training Part E Signature Forms.pdf 7
AEPA3.pdf 11
SigPage.pdf 12
2-Part E- Signature Forms- ResoluteGuard LLC 15
Part E- Signature Forms- ResoluteGuard LLC.pdf 15
AEPA3.pdf 16
AEPA4.pdf 17

AEPA Marketing Plan

- Strategy
    - Closely partner with AEPA to leverage AEPA's marketing model
    - Develop/Acquire participating agency target list
    - Develop relationships with individual participating agencies to generate engagement
    - Leverage AEPA resources and participating agencies to implement lead gen program and activities including email campaigns, webinar, educational content and video assets to drive engagement
    - Execute sales plan by calling and email campaigns designed to convert new agency agreements
    - Develop simple playbook for Cyber team and Sales Reps to execute against
    - Develop AEPA membership reference and testimonial program to reinforce conversion

- Marketing
    - Develop marketing calendar of events
    - Develop specific messaging and content for emails, webinars, sales collateral and demos
    - Creation of AEPA member calling scripts and cadence for CRCs and SRs
    - Partner with AEPA to develop email, newsletter, website banners, marketing assets and education/webinar schedule

Affirmative Action Policy

ResoluteGuard, LLC is dedicated to ensuring that all employment decisions are made without regard to race, religion, gender, national origin, age, disability, or any other protected characteristic. ResoluteGuard will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex.

ResoluteGuard, LLC, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of ResoluteGuard, LLC, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex.

ResoluteGuard agrees to comply with any regulations promulgated by the Treasurer pursuant to N.N.S.A. 10:5-31 et seq., as amended and supplemented from time to time and the Americans Disabilities Act.

ResoluteGuard, LLC agrees to inform in writing its appropriate recruitment agencies including, but not limited to, employment agencies, placement bureaus, colleges, universities, that it does not discriminate on the basis of age, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, and that we will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

In conforming with the applicable employment goals, ResoluteGuard , LLC agrees to review all procedures relating to transfer, upgrading, downgrading and layoff to ensure that all such actions are taken without regard to age, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal Law and applicable Federal court decisions.

Employees can report potential violations to the EEO-AAP coordinator or any officer of the company.

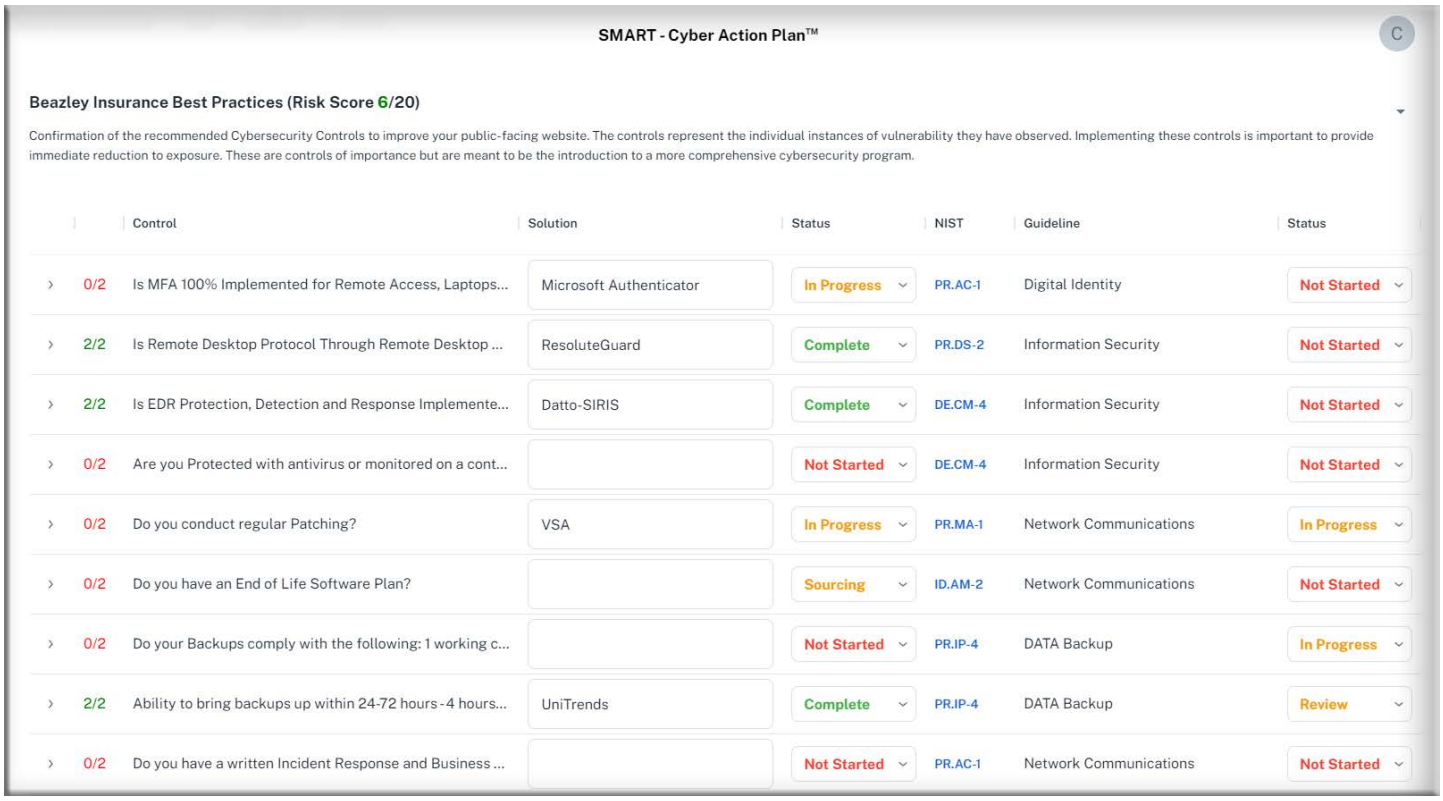
ResoluteGuard does not have a Price List and/or Catalog

RESOLUTE GUARD

Proactive Cybersecurity Risk Management For Members

vCISOSecure

Cybersecurity risk management platform providing administrators & technology teams the tools to accurately manage their cyber risk strategy, objectives, and budget. vCISOSecure provides a structured approach to identifying, managing, and mitigating cyber risks enhancing your resilience against cyber threats, minimizes potential financial and reputational damage, and supports overall business continuity.



SMART - Cyber Action Plan™

Beazley Insurance Best Practices (Risk Score 6/20)

Confirmation of the recommended Cybersecurity Controls to improve your public-facing website. The controls represent the individual instances of vulnerability they have observed. Implementing these controls is important to provide immediate reduction to exposure. These are controls of importance but are meant to be the introduction to a more comprehensive cybersecurity program.

	Control	Solution	Status	NIST	Guideline	Status
0/2	Is MFA 100% Implemented for Remote Access, Laptops...	Microsoft Authenticator	In Progress	PR.AC-1	Digital Identity	Not Started
2/2	Is Remote Desktop Protocol Through Remote Desktop ...	ResoluteGuard	Complete	PR.DS-2	Information Security	Not Started
2/2	Is EDR Protection, Detection and Response Implemente...	Datto-SIRIS	Complete	DE.CM-4	Information Security	Not Started
0/2	Are you Protected with antivirus or monitored on a cont...		Not Started	DE.CM-4	Information Security	Not Started
0/2	Do you conduct regular Patching?	VSA	In Progress	PR.MA-1	Network Communications	In Progress
0/2	Do you have an End of Life Software Plan?		Sourcing	ID.AM-2	Network Communications	Not Started
0/2	Do your Backups comply with the following: 1 working c...		Not Started	PR.IP-4	DATA Backup	In Progress
2/2	Ability to bring backups up within 24-72 hours - 4 hours...	UniTrends	Complete	PR.IP-4	DATA Backup	Review
0/2	Do you have a written Incident Response and Business ...		Not Started	PR.AC-1	Network Communications	Not Started

- **SMART-Cyber Action Plan™ Aligns Insurance Cyber Best Practices** - Aligns executive governance, administrative, and technical resources and activities to your customized plan and strategy, ensuring everyone is on the same page.
    - Rules-based notifications to inform administrators and technical teams of current status and actions required to continuously improve cyber posture.
    - Baseline cyber risk score and continuous improvement risk scores throughout the year.

RESOLUTE GUARD

- **Ongoing CISO Team Knowledge and Guidance -** Providing expert cybersecurity guidance to safeguard your organization's assets and protect against vulnerabilities.

- **Real-time Cybersecurity Risk Management Executive Summary** - Provides up-to-date analysis of your current cybersecurity posture, provides a clear overview of cybersecurity risks and statuses, facilitating better communication between IT teams and executive leadership.

- **Templated Policies & Guidelines (Prioritizing IRP, BCDR, Information Security Policies)** - Templated policies and plans provide a significant advantage in developing essential documentation.

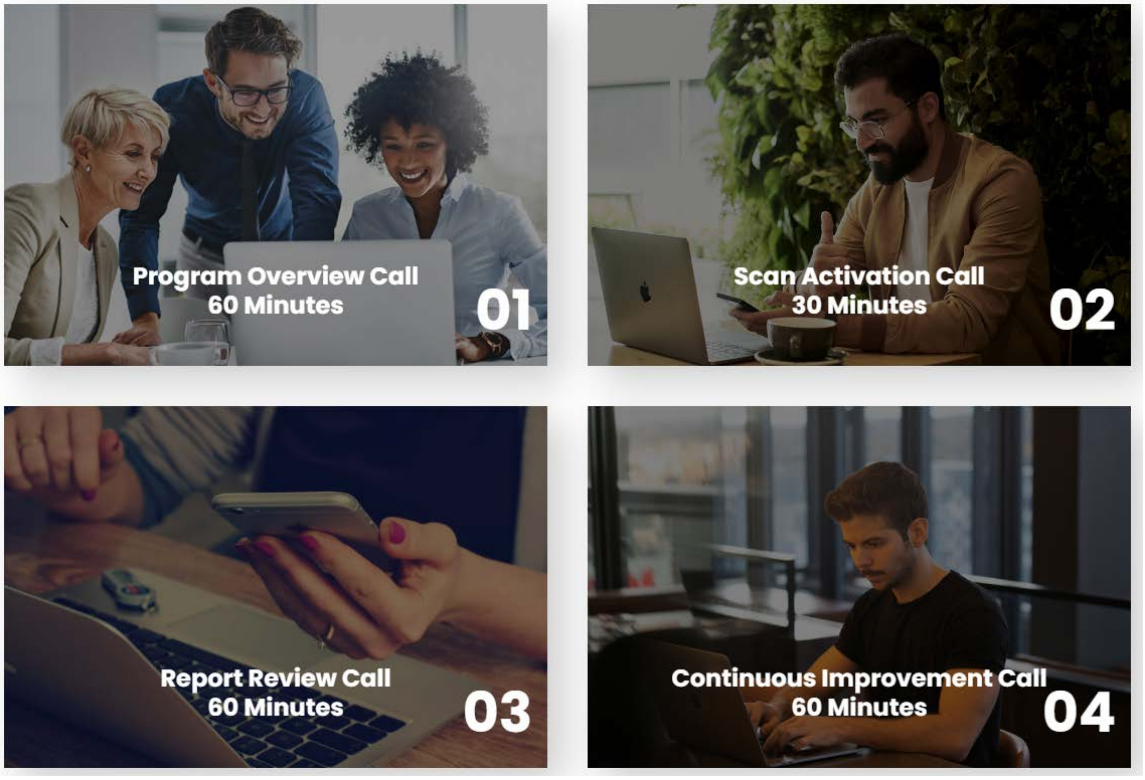
- **Comprehensive Vulnerability Scans & Assessments** - Critical internal network vulnerability scans of your entire network and external scans to identify ALL vulnerabilities and remedial actions on an annual, semi-annual, or quarterly scan frequency.

- **Vulnerability Assessment Report Review Calls** - to communicate high, medium and low risks by probability and severity of potential incident occurring and necessary remedial actions required.

- **Cyber Solution Recommendations** - Based on the current status of your security posture, we'll recommend tailored cyber solutions to meet your specific needs. (EDR, MFA, Backup, Managed SOC, Training; Auto Patching; Penetration Testing and more).

- **Cyber Budget** - prioritize and allocate funds to protect your digital assets, strengthen defenses, and mitigate potential threats.

Member Engagement: Simple 4-Step Process

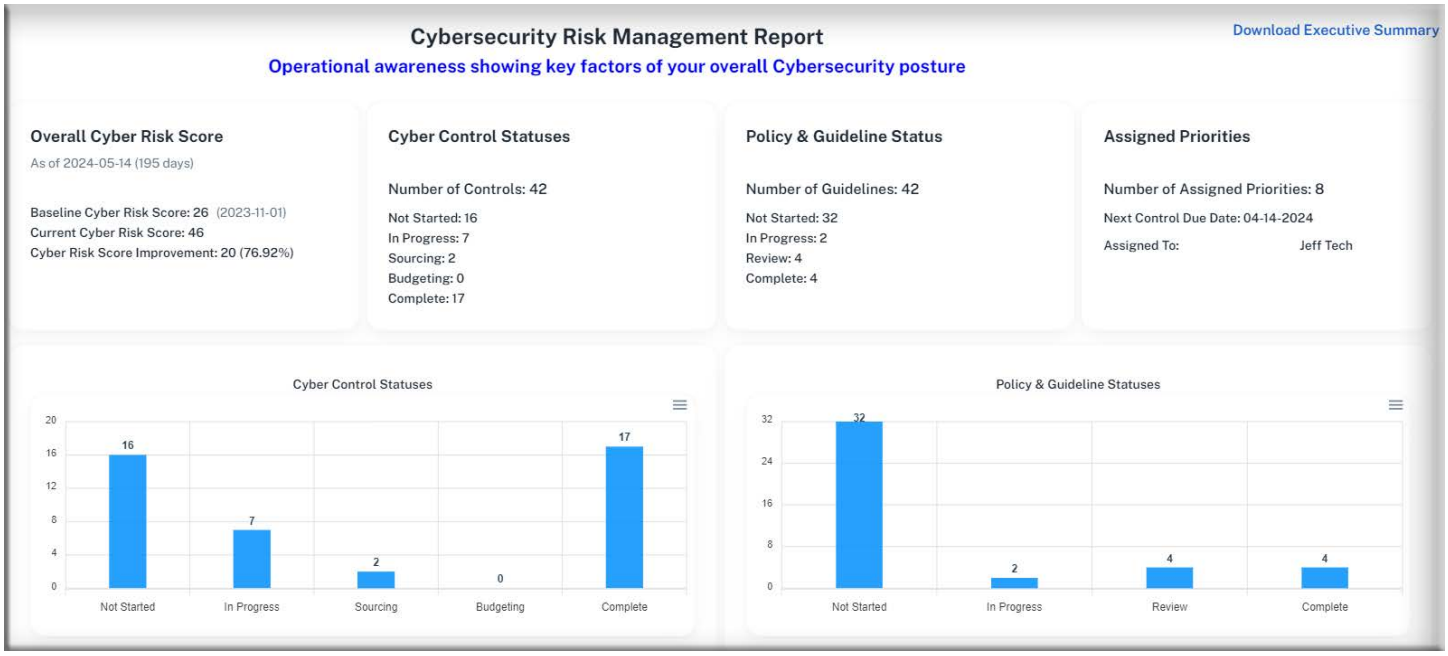


RESOLUTE GUARD

Proactive Cybersecurity Risk Management For ESA's

vCISOSecure

Cybersecurity risk management platform providing administrators & technology teams the tools to accurately manage their cyber risk strategy, objectives, and budget. vCISOSecure's powerful reporting suite enables risk pool underwriters to accurately assess member risk, leading to improved risk management reducing the frequency and severity of claims.



- **SMART-Cyber Action Plan™** - Achieving cyber resilience with a cybersecurity plan addresses and reduces cybersecurity risks at all organizational levels, from senior executives to business processes, implementation, and operations. Customized plans align with insurance cyber best practices, minimizing cyber incidents and reducing the likelihood of claims.
- **Real-Time Member Exposure & Engagement Tracking for Underwriting and Loss Control Teams -** Enhances your ability to manage cyber risk and monitor exposure. This enables risk pools to accurately identify potential vulnerabilities, leading to improved risk management and fewer claims, ultimately providing optimal coverage and maintaining financial health.
- **Real-time Risk Pool Dashboard & Cyber Risk Analysis** - Provides relevant cyber data to accurately assess member risk, status of program implementation, offering insights into baseline cybersecurity postures and continuous improvement during the year.
- **Ongoing CISO Team Knowledge and Guidance** - Providing expert cybersecurity guidance to help members understand risks and protect against vulnerabilities.
- **Member Cyber Risk and Continuous Improvement Scores** - Significantly bolster your member's capacity to manage cybersecurity risks and continuously enhance their cybersecurity posture.

RESOLUTE GUARD

Part E – Signature Forms

AEPA 025-F
Cyber Security and Training

Instructions

Contained herein are forms that **require a signature** from an authorized person at your company. All items found within this document are **mandatory**. Failure to sign the required areas, sections, or signature lines may lead AEPA to consider your company's proposal as **non-responsive**.

To submit the required signed forms, follow these steps:

1. Read the documents in their entirety.
2. Complete all forms and sign when required.
3. Return the forms and pages in their correct order and scan one (1) single PDF format titled ***"Part E – Signature Forms – Name of Responding Company"*** (i.e. one PDF document for all signature forms).
4. Submit Part E, along with other required documents in Bonfire.

*Note, a solicitation checklist has been provided to review with your submission.

The following sections will need to be completed prior to submission as one (1), single PDF titled "Part E – Signature Forms – Name of Responding Company".

Uniform Guidance "EDGAR" Certification Form – ****signature required***
Solicitation Affidavit – ****signature required***
Acceptance of Solicitation & Contract – ****signature required***

Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7. Clean Air Act and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended, contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein. Respondent Certification (By Item)	Respondent Certification: YES, I agree	Initial
1. Violation of Contract Terms and Conditions	YES, I agree	JS
2. Termination for Cause of Convenience	YES, I Agree	JS
3. Equal Employment Opportunity	YES, I Agree	JS
4. Davis-Bacon Act	YES, I Agree	JS
5. Contract Work Hours and Safety Standards Act	YES, I Agree	JS
6. Right to Inventions Made Under a Contract or Agreement	YES, I Agree	JS
7. Clean Air Act and Federal Water Pollution Control Act	YES, I Agree	JS
8. Debarment and Suspension	YES, I Agree	JS
9. Byrd Anti-Lobbying Amendment	YES, I Agree	JS
10. Procurement of Recovered Materials	YES, I Agree	JS
11. Profit as a Separate Element of Price	YES, I Agree	JS
12. General Compliance with Participating Agencies	YES, I Agree	JS
13. Governing Law; Forum Selection.	YES, I Agree	JS

ResoluteGuard, LLC
Name of Business

Jeffrey R. Schobel
Signature of Authorized Representative

Jeffrey R. Schobel
Printed Name

9/16/2024
Date

[redacted]

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

Jeffrey Ryan Schobel	417 Crescent Pkwy Sea Girt NJ 08750
Authorized Representative (Please print or type)	Mailing Address
Chief Executive Officer	
Title (Please print or type)	City, State, Zip
Jeffy R. Schobel	9/28/2024
Signature of Authorized Representative	Date

JUDITH I. KARL
NOTARY PUBLIC OF NEW JERSEY
My Commission Expires Feb. 6, 2026

Judith I. Karl

[redacted]

Association of Educational PURCHASING AGENCIES

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	ResolvteGuard, LLC	**Date**	9/16/2024
Address	417 Crescent Pkwy	**City, State Zip**	Sea Girt NJ 08750
Contact Person	Jeffrey Schobel	**Title**	Chief Executive Officer
Authorized Signature	Jeffrey A. Schobel	**Title**	Chief Executive Officer
Email	jschobel@resolvteguard.com	**Phone**	888-728-6030

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Solicitation Checklist

Instructions: Utilize the checklist below, reviewing to confirm that all the required documents have been uploaded to Public Purchase, in their ***specified/required format***, by the due date and time listed for this solicitation. ***Submissions not following the specified/required format may result in being marked non-responsive and may not be considered for evaluation.*** Respondents are reminded that failure to follow, comply with, and adhere to the enclosed instructions of this solicitation may result in their response being deemed non-responsive. AEPA, its Member Agencies, affiliate agencies, and authorized representatives are not responsible for bid proposals that are incomplete, unreadable, or received after the solicitation deadline submission date.

"x"	**Document Title, Uploaded to Bonfire** *(Respondent must submit documents in the required title/format)*	**Format of Uploaded Document**	**Notes**
	Bid Bond – if Required, see Part A if applicable.	Upload PDF copy of the bid security.	The original bid security must be received by Lakes Country Service Cooperative by due date and time.
	Part C – State-Specific Forms – ***Name of Responding Company***	Single, Scanned PDF	**New Jersey Only Requirement.** Signatures Required.
	Part D - Questionnaire – ***Name of Responding Company*** Includes: ● Company Information ● Service Questionnaire ● Exceptions ● Deviations	Single, Scanned PDF	**Required.**
	Part E – Signature Forms – ***Name of Responding Company*** Includes: ● Uniform Guidance "EDGAR" Certification ● Solicitation Affidavit ● Acceptance of Solicitation & Contract	Single, Scanned PDF	**Required.** Signatures required.
	Part F – Pricing Schedule – ***Name of Responding Company***	Excel Workbook	**Required.**
	Price List and/or Catalog – ***Name of Responding Company***	Upload PDF	**Required.**
	Exhibit A – Marketing Plan – ***Name of Responding Company***	Scanned PDF	**Optional.** Form not provided by AEPA, Respondent Created

[redacted]

Association of Educational PURCHASING AGENCIES

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	ResolvteGuard, LLC	**Date**	9/16/2024
Address	417 Crescent Pkwy	**City, State Zip**	Sea Girt NJ 08750
Contact Person	Jeffrey Schobel	**Title**	Chief Executive Officer
Authorized Signature	Jeffrey A. Schobel	**Title**	Chief Executive Officer
Email	jschobel@resolvteguard.com	**Phone**	888-728-6030

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein. Respondent Certification (By Item)	Respondent Certification: YES, I agree	Initial
1. Violation of Contract Terms and Conditions	YES, I agree	JS
2. Termination for Cause of Convenience	YES, I Agree	JS
3. Equal Employment Opportunity	YES, I Agree	JS
4. Davis-Bacon Act	YES, I Agree	JS
5. Contract Work Hours and Safety Standards Act	YES, I Agree	JS
6. Right to Inventions Made Under a Contract or Agreement	YES, I Agree	JS
7. Clean Air Act and Federal Water Pollution Control Act	YES, I Agree	JS
8. Debarment and Suspension	YES, I Agree	JS
9. Byrd Anti-Lobbying Amendment	YES, I Agree	JS
10. Procurement of Recovered Materials	YES, I Agree	JS
11. Profit as a Separate Element of Price	YES, I Agree	JS
12. General Compliance with Participating Agencies	YES, I Agree	JS
13. Governing Law; Forum Selection.	YES, I Agree	JS

ResoluteGuard, LLC
Name of Business

Jeffrey R. Schobel
Signature of Authorized Representative

Jeffrey R. Schobel
Printed Name

9/16/2024
Date

[redacted]

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

Jeffrey R. Schobel	417 Crescent PKWY
Authorized Representative (Please print or type)	Mailing Address
Chief Executive Officer	Sea Girt NJ 08750
Title (Please print or type)	City, State, Zip
David Burns	9/16/2024
Signature of Authorized Representative	Date

Contents

1-Exhibit A – Marketing – SHI 1
Enhance the AEPA contract through SHI 2
1-Part C – State-Specific Forms-SHI 13
2-NJ Business Registration Certificate-SHI 74
3-Equal Employment Opportunity Affirmative Action Plan-SHI 76
4-Equal Opportunity Consolidated Report-SHI 77
5-W-9 -SHI 92
6-Intl Corp Signature Authorization-SHI 93
7-Certificate of Employee Information Report-SHI 95
1-Supporting Information Document-SHI 96
Table of Contents 98
Question Set 1: Company Information 1 98
Question Set 2: Service Questionnaire 52 98
Question Set 1: Company Information 99
Sales History 104
Key Contacts 104
SHI Public Sector Account Team Org Chart 105
Customer Support 106
SHI Standard Procedure and Issue Resolution 107
Sales Training 108
Products and Services 113
Distribution 117
Marketing 130
Environmental Initiatives 141
Value Add 145
Disclosures 148
References 148
Question Set 2: Service Questionnaire 150
Sales Data 150
Customer Support 154
Pricing 158
Cooperative Contracts 158
Fees 159
2-Catalog –SHI 162
3-Part C- AEPA Terms and Condition Exception-SHI 163

4-Part B - AEPA Terms and Conditions Exceptions - SHI 165
5-Sustainability and Action Report 2023-SHI 168
1-Part E – Signature Forms–SHI 216



Exhibit A-Marketing Plan-SHI

RFP #025 – Cyber Security & Training

9/17/2024

ENHANCE THE AEPA CONTRACT THROUGH SHI

SHI International Corp. (SHI) is excited by the opportunity provided by the Association of Educational Purchasing Agencies (AEPA) through this RFP to serve as a trusted partner to the agencies you serve.

As part of our practice, we work with market-leading and technology-emergent cybersecurity technology providers to help customers defend against cyberattacks' growing threat and navigate complex regulatory requirements. We offer people, technology, and process-focused solutions in data center and cloud security, application security, data-centric security, identity and access management, threat and vulnerability management, and program strategy and operations.

Our ability to support AEPA and your member agencies is demonstrated by our capabilities in supporting the public sector—services which we have significantly expanded since our inception in 1989. today we provide comprehensive support to 12,000 government and educational entities, including state and local governments, K-12 and higher education institutions, as well as public healthcare organizations and federal agencies throughout the United States. We also hold contracts with numerous large public sector cooperative and group purchasing organizations such as NASPO, OMNIA Partners, Sourcewell, and Vizient.

We have more than 250 salespeople, including field account executives who live and work throughout the United States. We have a dedicated Public Sector leadership team to oversee our operations and support these professionals, along with a Core Solutions Engineering team to assist customers in choosing exactly the right technology solutions.

We understand the critical importance of promoting this contract to both internal and external stakeholders and are deeply committed to accomplishing this through a strategic marketing plan.



Figure 1: SHI Public Sector Highlights

Upon award, our dedicated team supporting this contract will work in concert with AEPA to develop and execute a marketing plan. This plan will include various agreed-upon elements, including the creation of co-branded marketing materials and the release of contract information to agencies and the wider public. We can also establish mutual opportunities to promote our partnership in a variety of venues such as trade shows, conferences, and other meetings. This also includes the internal training of our own sales team around the elements of the contract to ensure we deliver the highest level of service to AEPA member agencies. The plan will be designed to be adaptable, ensuring we can quickly respond to the needs of AEPA and member agencies along with market changes. We will establish regular communication with AEPA representatives to evaluate the effectiveness of the current strategy, discuss new marketing ideas, and gauge the overall success of the contract rollout.

We thank AEPA for the opportunity to allow us to participate in this bidding process. Should you have any questions regarding this marketing plan, our response, or our cybersecurity practice, please reach out to members of our team supporting this RFP. This includes:

- Aimee Ballenger, Sr. Director of Contract Capture and Development, Aimee_Ballenger@SHI.com
- Amelia Jakubczyk, Director SLED Contract Capture and Development, Amelia_Jakubczyk@SHI.com
- Chris Dickman, Capture and Business Development Manager, Chris_Dickman@SHI.com

On the following pages, we have responded to each of the items you provided for additional information around key points regarding our plan to collaborate with and reach out to AEPA member agencies.

Process on how the contract will be launched to current and potential agencies.

SHI Response

Understanding the vital importance of marketing contracts and reaching all eligible agencies, SHI is excited at the opportunity to promote and market an AEPA partnership. We are committed to applying our tangible, demonstrated experience in supporting the unique requirements of procurement organizations to ensure a successful launch of this contract to current and potential AEPA agencies.

Throughout the contract, we will continue marketing this contract not only to AEPA agencies but also internally within SHI. Our SLED Contract Capture & Business Development Director, Amelia Jakubczyk, along with her team, is experienced in developing comprehensive internal training for our sales teams responsible for supporting similar contracts. These trainings cover the who, what, why, and when to break down the talk tracks that will be helpful to sales and potential AEPA agencies alike.

SHI has also committed in recent years to the expansion of our marketing team devoted to the public sector. Led by our Director of Growth Marketing Programs, Rob Fass, this team takes an innovative approach to expanding initiatives that are focused on public sector customers and the real IT obstacles they face. Through purposeful customer-directed emails about solutions specific to our customer base, social media, and supporting our customer-facing events, this team will be critical to our support of AEPA agencies.

Our dedicated Contract Capture and Strategy team, Public Sector leadership, and Public Sector Marketing teams will collaborate with AEPA to create and roll out our marketing plan for this contract.

Upon award of the contract, we will take the following steps at the launch of this new contract to your agencies:

- Create contract announcement materials for electronic distribution to customers via email, on SHI.com, and the SHI Resource HUB blog, and posts on LinkedIn along with other social media.
- Create co-branded marketing outlining the features of the new contract.
- Create internal sales training for new contract compliance, pricing, terms, etc.
- Design a dedicated website on SHI.com, including the AEPA awarded-vendor logo, a copy of contract documents, a summary of products and pricing, marketing materials, a link to AEPA's website, and all relevant contact information.

Our history of success with similar contracts and marketing them will be invaluable to a strong launch for AEPA. Below is our contract implementation plan:

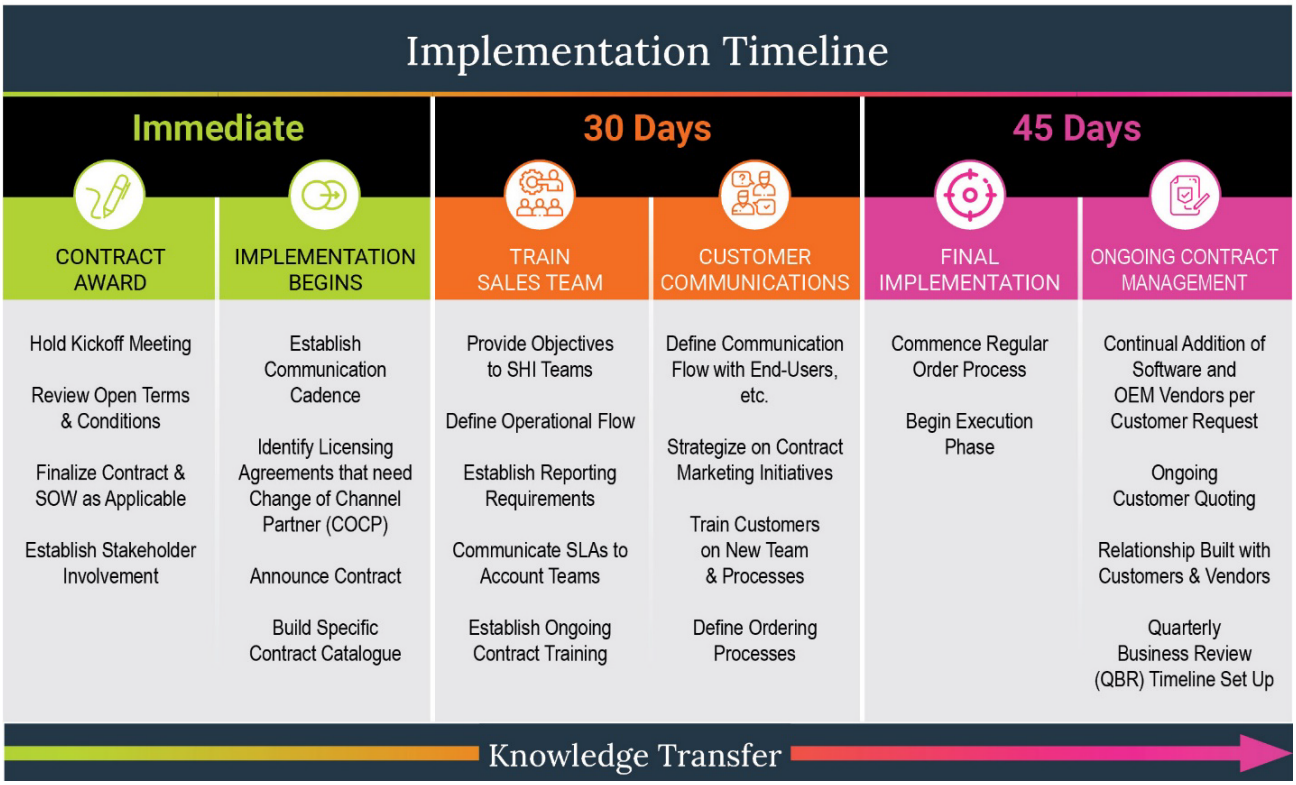


Figure 2: Sample Contract Implementation Timeline

Our account team can also use various other methods to market and sell the products that we represent to AEPA agencies, including customer meetings, vendor presentations, trade shows, web seminars, printed marketing materials, our website, and a monthly electronic newsletter. We also host strategic events with many of the SHI and manufacturer representatives to provide our mutual customers with new product information, product changes, and industry direction. Additionally, we participate in vendor exhibits at numerous monthly events, including technology trade shows.

Some of the marketing-related items that contract customers can expect to continue receiving and accessing include:

Newsletters

SHI creates various informative, monthly newsletters containing information regarding important contract dates, product releases or changes, Q&A, and upcoming events. Thousands of our customers currently receive these newsletters, and we will continue to make them available as a subscription to anyone who is interested.

Web Seminars

SHI hosts a series of web seminars covering a variety of topics including new product announcements, changes to licensing programs for major software OEMs, procurement and technology trends, and foundational IT information. Webinar schedules are published quarterly; please check the events page on our website https://www.publicsector.shidirect.com/ for the current schedule.

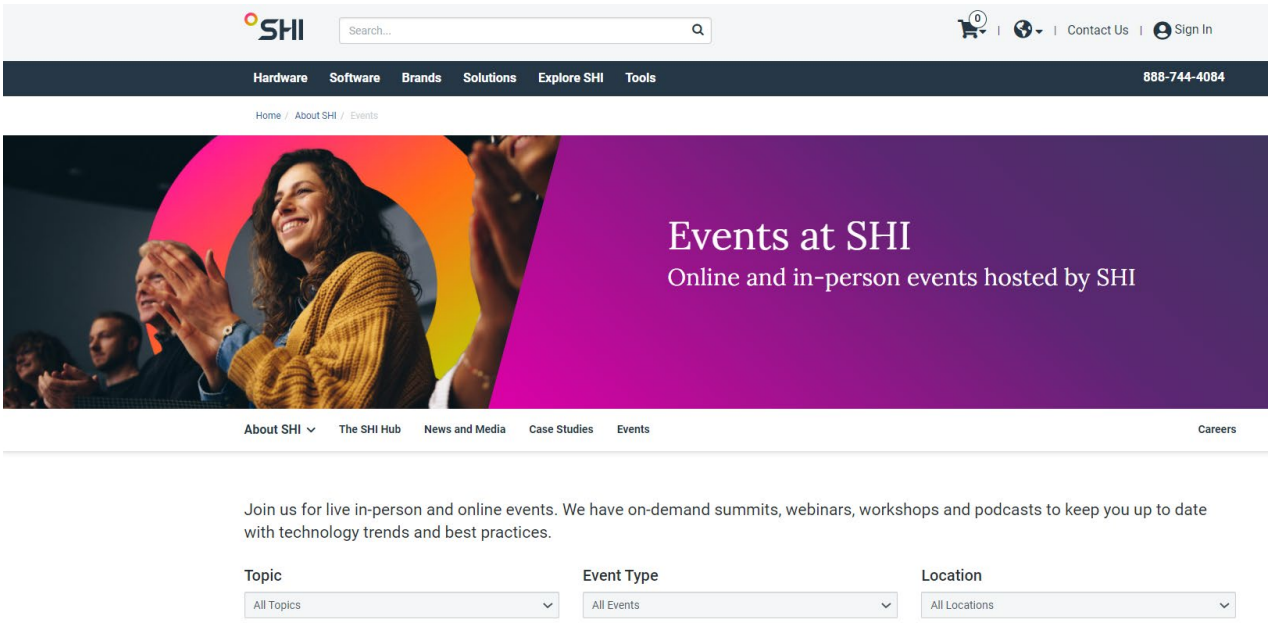


Figure 3: Events at SHI

Marketing Documents

SHI creates hundreds of marketing texts for our major manufacturer partners and SHI core services offerings, all of which are made available to customers through in-person meetings, trade shows, email delivery, and mail-outs. Marketing documents will include those that we receive from the manufacturers, those that SHI creates for a general audience, and those that SHI creates specific to AEPA. An example is included on the following page.



Overview

The Association of Educational Purchasing Agencies (AEPA) works on behalf of members to secure multi-state volume purchasing contracts that have benefits that are measurable, cost-effective and continuously exceed expectations. As a recipient of the Cyber Security & Training contract, SHI International Corp. (SHI) is available to provide comprehensive cyber security solutions and services to AEPA member agencies, including PK-12 educational, Higher Education Institutions, and other public institutions.

SHI offers people, technology, and process-focused solutions in data center and cloud security, application security, data-centric security, identity and access management, threat and vulnerability management, and program strategy and operations. The SHI Lab supports vendor comparisons with integration validation for your organization. Our data-supported use case analysis enables you to deliver your cybersecurity strategic objectives, achieve cross-departmental consensus, and secure your budget.

Key Benefits:

- A local agency in your state that manages the contract
- Avoid duplication and expense of the bid process
- Volume contracts based on 30 state participation
- Attract and leverage national vendors
- Save time and money

Contract Details

AEPA agencies can benefit from SHI's Cyber Security & Training contract award:

Contract Number: AEPA RFP#025 – F, Cyber Security & Training

Scope: SHI is approved to acquire, deliver and perform the required services, supplies, materials, equipment and labor to all participating member states (up to 30) in the category of Cyber Security & Training.

Contract Term: Indefinite Delivery, Indefinity Quantity (IDIQ) contract

Pricing Mode: Discount off MSRP

How to take advantage of AEPA Cybersecurity Contract:



Why SHI?

SHI helps government organizations take a smarter approach to technology deployment, provision applications faster, and run efficient and effective IT operations across data centers, end-user devices, and in the cloud. Contracts play an important role in public sector procurement and SHI offers hundreds of cooperative and statewide contract options across the country.

For more information contact:
PS_Contracts@shi.com

SHI | PUBLIC SECTOR

SHI International Corp. \\ SHI.com \\ 888-764-8888

Figure 4: SHI-AEPA Sample Marketing Flyer

SHI HUB

The SHI HUB is home to eBooks, on-demand articles, and podcasts to keep our customers updated on the latest changes and trends impacting the IT industry. Showcasing short news and informational articles, the SHI HUB keeps our customers up to date on our services and support as well as on emerging trends in technology. Written by SHI's subject matter experts who leverage their knowledge and insight to speak to SHI's broad customer base, SHI is committed to keeping our customers informed. The screenshot below exemplifies the easy navigation of the SHI HUB website. Customers can browse by IT category, recent articles, or popular posts.

The following articles relative to cooperative contracts are examples of resources that will be available to AEPA members through the SHI HUB:

- Reduce procurement costs with cooperative contracts
- Tired of expensive bid processes? You will love cooperative contracting!

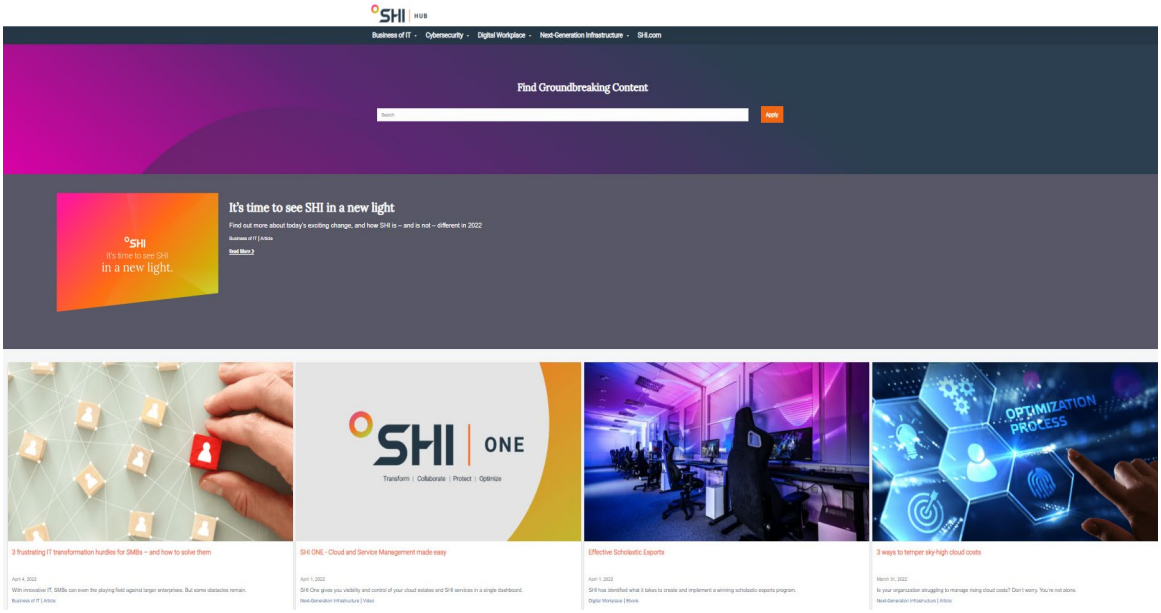


Figure 5: SHI HUB Website

SHI Summits Executive Forums

SHI extends invitations to our customers to attend our annual SHI Summits, which focus on reviewing current industry trends. These forums include keynotes and breakout sessions led by industry experts from both SHI and top OEMs sharing the best practices they use to support digital workspace, hybrid cloud, data center, and security initiatives. Your teams will also be able to attend deep-dive workshops focusing on IT asset management, next-generation data center architectures, and cloud services.

Social Media

In addition to the SHI HUB, SHI utilizes social media applications to keep our customers informed. Customers can get up-to-date information on demand by following SHI on X (formerly Twitter), LinkedIn, Facebook, and YouTube.

Process for ongoing communications with AEPA State lead agencies regarding marketing.

SHI Response

SHI has a dedicated Capture and Business Development Manager aligned to AEPA, Chris Dickman, who is available to support regular reviews with AEPA representatives as the contract kicks off. A healthy contract review will allow us to stay focused, analyze results for plans and strategies currently in place, discuss new campaign and marketing ideas, and review the overall success of the contract.

Chris, working in concert with our Public Sector Sales, Marketing, and Capture teams, will continue to be in close contact with AEPA State lead agencies regarding marketing initiatives and will be available to respond to any questions or feedback.

Additionally, SHI will have a dedicated AEPA contract website on SHI.com that will provide updated marketing materials for agencies to reference.

The ability to produce and maintain in full color advertisements in camera-ready electronic format including company logos and contact information.

SHI Response

SHI has a fully staffed and in-house graphics department that can be utilized to produce and maintain full-color advertisements–in camera-ready electronic format, including company logos and contact information–for use in support of this contract.

Anticipated contract announcements, planned advertisements, industry periodicals, other direct or indirect marketing activities promoting the AEPA awarded contract.

SHI Response

With decades of experience onboarding similar contracts, SHI has developed a team and process to ensure a successful launch and will have dedicated resources across the country to market and grow our new AEPA contract.

Since its inception in 1994, our Public Sector division has successfully supported contracts representing a broad portfolio of services and products for a range of public entities. Today, we hold contracts in all 50 states and have seven national and nine regional procurement consortia. For more information on our public sector contracts and how we assist in simplifying procurement while offering the best technology solutions for participating organizations, please visit https://www.shi.com/Contract/PSContract/ContractHome.

Our dedicated Contract Capture and Strategy, Public Sector leadership, and Public Sector Marketing teams will collaborate along with AEPA in the creation and rollout of our marketing plan for this contract. Below we have prepared a sample marketing plan for your review but will remain flexible and open to collaboration with AEPA upon award, including any contract announcements, industry periodicals, or other direct or indirect marketing activities agreed upon.

First week

- Post announcement along with contract details and contact information to https://www.SHI.com.
- Begin design of co-branded marketing materials, including print, electronic, email, and presentations.
- Discuss publication and distribution plans, as well as a plan to distribute and follow up on leads.
- Design and implement the AEPA secured-website on https://www.SHI.com including the AEPA logos, copy of original RFP, copy of contract and amendments, summary of products and pricing, marketing materials, a link to AEPA's website, and all relevant contact information.

First month

- Complete design of co-branded marketing materials.
- Finalize plans to publish and distribute.
- Begin distribution to current and prospective AEPA agencies.

First 90 days

- Complete training and enablement for SHI sales force.
- Complete publishing and distribution of initial marketing materials.
- Analyze initial activity.
- Discuss the next 90-day plan for marketing.

Ongoing

- Design and publish national and regional advertising in trade publications.
- Market and promote the Master Agreement, including case studies, presentations, campaigns, and blog posts.

How the contract award will be displayed/linked on the Respondent's website.

SHI Response

Upon award, SHI will design and create a dedicated AEPA website on SHI.com to display the contract award. This will include the AEPA awarded-vendor logo, a copy of any contract documents, a summary of products and pricing, marketing materials, a link to AEPA's website, and all relevant contact information. Please see below:

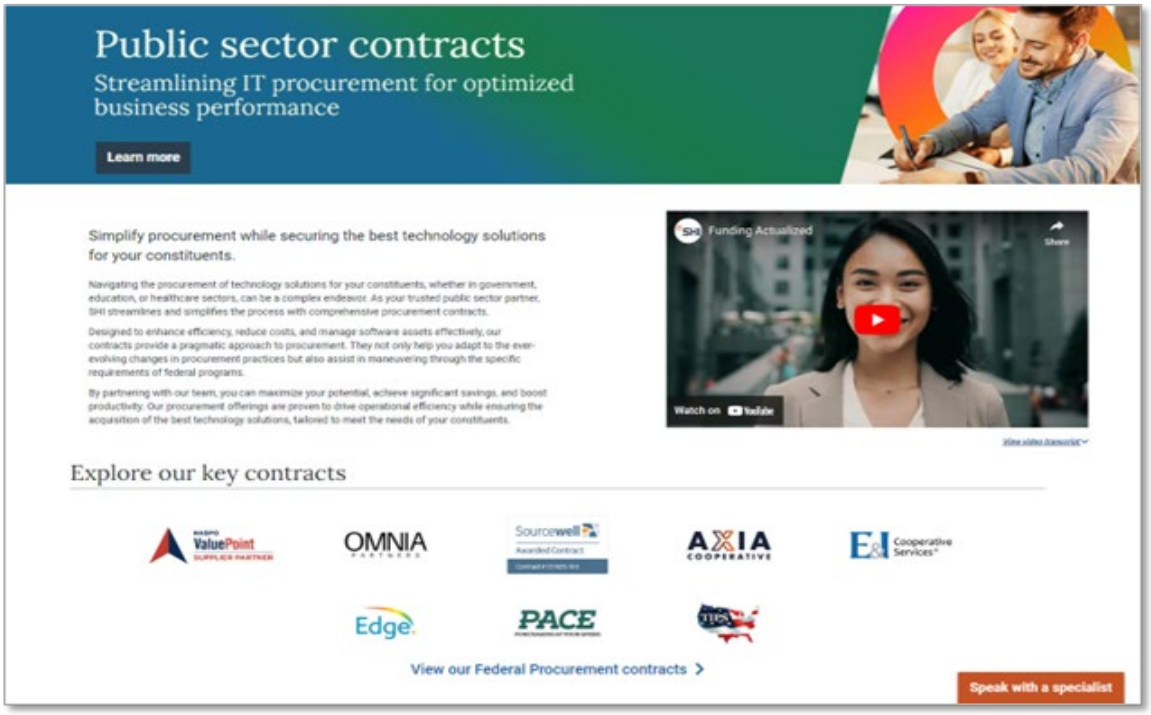


Figure 6: SHI Public Sector Contracts

Continuous outreach efforts, including attendance at national or state conferences, email and social media campaigns, etc.

SHI Response

SHI participates in many trade shows, conferences, and meetings across the country, and welcomes any opportunity to work with AEPA on advertising at events. AEPA has our commitment to participate at specified shows as well as additional opportunities to broadcast and promote our partnership.

SHI collaborates with many public sector-focused organizations to host educational seminars and workshops nationwide to educate ourselves and our customers. Representatives from SHI sit on the Partner Advisory Board for GMIS International and participate in many of the local chapters across the country. To better serve our customers and understand the common challenges and trends impacting the vertical they reside, SHI actively works with organizations such as:

- **Education:** To support our education customers in adopting innovative technologies, SHI is a member of EDUCAUSE and is connected to organizations such as the International Society for Technology in Education, Texas Computer Education Association, and Future of Education Technology, as well as numerous school board associations such as the New Jersey School Boards Association.
- **Government:** We are associated with the Center for Digital Government, Texas Association of State Systems for Computing and Communications Advisory Board, and through nationwide participation and sponsorship of state and local government events. As a member of both the National Association of State Chief Information Officers and the National Associate of State Technology Directors, we connect and collaborate with C-level public sector IT professionals.

Through these collaborations, we gain insight into the needs of education and government entities of all sizes. We also provide seminars and workshops to our public sector customers across the country and are eager to have AEPA members attend. These include.

- **Summits**: SHI holds technology summits at our corporate headquarters in Somerset, NJ. Our next summit, scheduled for Oct. 8-9, is titled *Infrastructure, Hybrid Cloud and Cybersecurity Foundations for AI Success*. The summit is aimed for Leaders in IT infrastructure (including CIOs, CTOs, CISOs, Directors of IT, and more) who are eager to learn from industry experts how to best address the forces impacting today's infrastructure, cloud, and security environments. SHI can coordinate participation with AEPA members for these events.
- **Custom Events**: SHI has previously hosted a series of roadshow events, focusing on topics such as cybersecurity and infrastructure at large event spaces around the country with solution partners and special guest speakers.

SHI can also be an invaluable resource for AEPA agencies to find reliable and relevant information about the latest trends, or threats, to their IT through the following digital mediums:

Webinar Series

AEPA agencies can access our regular schedule of webinars and workshops covering a variety of topics relevant to today's public sector customer. This includes, among other topics, grants and funding to modernize your network and streamline multivendor support for IT purchases. Agencies can visit our website for upcoming events and on-demand recordings: https://www.publicsector.shidirect.com/about/events.

SHI Resource Hub

The SHI Resource HUB is home to eBooks and short news articles that can keep AEPA agencies updated on the latest changes and trends impacting the IT industry. Displaying short news and informational articles, the HUB keeps our customers up to date on our services and support as well as on emerging trends in technology. Written by SHI's subject matter experts who leverage their knowledge and insight to speak to SHI's broad customer base, SHI is committed to keeping our customers informed. Customers can browse by IT category, recent articles, or popular posts. AEPA agencies can visit the SHI HUB website (https://blog.shi.com) for on-demand articles, eBooks, and podcasts.

Social Media

In addition to the SHI Resource Hub, SHI is active on social media applications and has dedicated public sector pages to help keep our public sector customers, such as AEPA agencies, informed. Up-to-date information is available on demand by following SHI on X, LinkedIn, Instagram, Advocacy, and YouTube. Upon award of a new contract with AEPA, we will create an announcement for LinkedIn for SHI to share with AEPA and our partner community. We also have podcasts—“We’ve Got Your Mac” and “Innovation Heroes” are available wherever you listen to podcasts. They are also available on our SHI Resource HUB at https://blog.shi.com.

E-Newsletters

SHI creates various informative, monthly newsletters containing information regarding important contract dates, product releases or changes, Q&A, and upcoming events. Thousands of our customers currently receive these newsletters, and we will continue to make them available as a subscription to anyone who is interested. SHI also creates hundreds of marketing texts for our major manufacturer partners and SHI core services offerings, which are shared with customers through in-person meetings, trade shows, and email.



We Are SHI

We bring together
IT and Procurement
like never before

NEW JERSEY REQUIRED DOCUMENTS FOR GOODS AND SERVICES BIDS

BUSINESS REGISTRATION CERTIFICATE (N.J.S.A. 52:32-44)

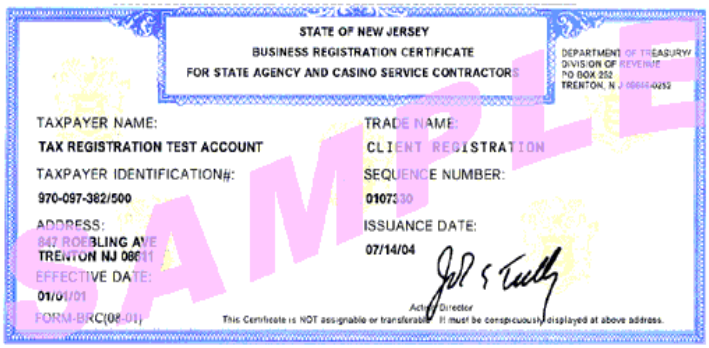
Pursuant to N.J.S.A. 52:32-44, all respondents shall submit prior to award of bid, a copy of their "New Jersey Business Registration Certificate" as issued by the Department of Treasury of the State of New Jersey. The ESCNJ requests that all respondents for this bid/proposal submit a current New Jersey Business Registration Certificate with the bid/proposal but no later than the bid award.

Goods and Services Contracts

N.J.S.A. 52:32-44 imposes the following requirements on contractors and all subcontractors that knowingly provide goods or perform services for a contractor fulfilling this contract:

1. The contractor shall not enter into a contract with a subcontractor unless the subcontractor first provides the contractor with a valid proof of business registration.
2. The contractor shall maintain and submit to the Contracting Agency a list of subcontractors and their addresses that may be updated from time to time.
3. Prior to receipt of final payment from a contracting agency, a contractor must submit to the contracting agency an accurate list of all subcontractors or attest that none was used.
4. The contractor and any subcontractor providing goods or performing services under the contract, and each of their affiliates, shall collect and remit to the Director of the Division of Taxation in the Department of the Treasury, the use tax due pursuant to the Sales and Use Tax Act, (N.J.S.A. 54:32B-1 et seq.) on all sales of tangible personal property delivered into the State. Any questions in this regard can be directed to the Division of Taxation at (609) 292-6400.

For more information on how to obtain a Business Registration Certificate, please visit the State of New Jersey, Department of Treasury, Division of Revenue and Enterprise Services website at:
http://www.state.nj.us/treasury/revenue/busregcert.shtml


STATE OF NEW JERSEY
BUSINESS REGISTRATION CERTIFICATE
FOR STATE AGENCY AND CASINO SERVICE CONTRACTORS

DEPARTMENT OF TREASURY
DIVISION OF REVENUE
PO BOX 252
TRENTON, NJ 08646-0252

TAXPAYER NAME:
TAX REGISTRATION TEST ACCOUNT

TRADE NAME:
CLIENT REGISTRATION

TAXPAYER IDENTIFICATION#:
970-097-362/500

SEQUENCE NUMBER:
0107330

ADDRESS:
847 ROEBLING AVE
TRENTON NJ 08611

ISSUANCE DATE:
07/14/04

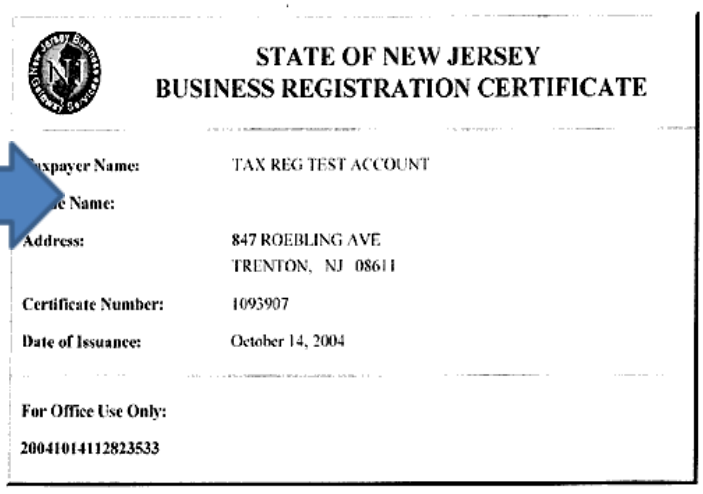
EFFECTIVE DATE:
01/01/01

Acting Director

FORM BRC(08-01)

This Certificate is NOT assignable or transferable. It must be conspicuously displayed at above address.

SAMPLE


STATE OF NEW JERSEY
BUSINESS REGISTRATION CERTIFICATE

Taxpayer Name: TAX REG TEST ACCOUNT

Trade Name:

Address: 847 ROEBLING AVE
TRENTON, NJ 08611

Certificate Number: 1093907

Date of Issuance: October 14, 2004

For Office Use Only:

20041014112823533

N.J.S.A. 54:49-4.1: Violations of Registration Requirements; Penalties.

A business organization that fails to provide a copy of a business registration as required pursuant to section 1 of P.L.2001, c.134 (C.52:32-44 et al.) or subsection e. or f. of section 92 of P.L.1977, c.110 (C.5:12-92), or that provides false information of business registration under the requirements of either of those sections, shall be liable for a penalty of $25 for each day of violation, not to exceed $50,000 for each business registration copy not properly provided under a contract with a contracting agency.

All respondents are urged to submit with their response, a copy of their firm's New Jersey Business Registration Certificate. Failure to submit the Certificate to the ESCNJ prior to the award of contract will result in the rejection of the entire bid or proposal.

CONTRACTOR/VENDOR REQUIREMENTS—OFFICE OF THE NEW JERSEY STATE COMPTROLLER

Contractors/vendors doing business with the ESCNJ are reminded of the following legal requirements pertaining to the Office of the New Jersey State Comptroller:

A. Access to Relevant Documents and Information—N.J.S.A. 52:15C-14 (d)

Private vendors or other persons contracting with or receiving funds from a unit in the Executive branch of State government, including an entity exercising executive branch authority, independent State authority, public institution of higher education, or unit of local government or board of education shall upon request by the State Comptroller provide the State Comptroller with prompt access to all relevant documents and information as a condition of the contract and receipt of public monies. The State Comptroller shall not disclose any document or information to which access is provided that is confidential or proprietary. If the State Comptroller finds that any person receiving funds from a unit in the Executive branch of State government, including an entity exercising executive branch authority, independent State authority, public institution of higher education, or unit of local government or board of education refuses to provide information upon the request of the State Comptroller, or otherwise impedes or fails to cooperate with any audit or performance review, the State Comptroller may recommend to the contracting unit that the person be subject to termination of their contract, or temporarily or permanently debarred from contracting with the contracting unit.

B. Maintenance of Contract Records—N.J.A.C. 17:44-2.2

Relevant records of private vendors or other persons entering into contracts with covered entities are subject to audit or review by OSC pursuant to N.J.S.A. 52:15C-14(d).

The contractor/vendor to whom a contract has been awarded shall maintain all documentation related to products, transactions or services under this contract for a period of five years from the date of final payment. Such records shall be made available to the New Jersey Office of the State Comptroller upon request.

D. Renewal of Contract; Services

The ESCNJ may, at its discretion, request that a contract for services be renewed in full accordance with N.J.S.A. 18A:18A-42. The ESCNJ may negotiate terms for a renewal of contract proposal and present such negotiated proposal to the Board. All multi-year contracts and renewals are subject to the availability and appropriation annually of sufficient funds as may be needed to meet the extended obligation.

The ESCNJ is the final authority in awarding renewals of contracts.

DEBARMENT, SUSPENSION, OR DISQUALIFICATION

The ESCNJ will not enter into a contract for work with any person, company or firm that is on the State Department of Labor and Workforce Development; Prevailing Wage Debarment List, or the State of New Jersey Consolidated Debarment Report (https://www.state.nj.us/treasury/revenue/debarment/index.shtml).

All bidders are required to submit a sworn statement indicating whether or not the bidder is, at the time of the bid, included on the State Department of Labor and Workforce Development; Prevailing Wage Debarment List or

the State of New Jersey Consolidated Debarment Report, or the Federal Debarred Vendor List—Excluded Parties List System—System for Award Management—SAM.gov

PROHIBITED ACTIVITIES IN RUSSIA AND BELARUS & INVESTMENT ACTIVITIES IN IRAN N.J.S.A. (18A:18A-49.4)

The ESCNJ, pursuant to N.J.S.A. 18A:18A-49.4, shall implement and comply with Public Law 2012, c.25, Disclosure of Investment Activities in Iran and Public Law 2022, c.3, Prohibited Russia-Belarus Activities —N.J.S.A. 52:32-55 et seq.

Pursuant to N.J.S.A. 52:32-57, et seq. (P.L. 2012, c.25, P.L. 2021, c.4 and P.L. 2022, c.3), any person or entity that is a successful bidder or proposer, or otherwise proposes to enter into or renew a contract, for goods or services must complete the certification below prior to contract award to attest, under penalty of perjury, that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list or Chapter 25 list as a person or entity engaging in prohibited activities in Russia, Belarus or Iran. Before a contract for goods or services can be amended or extended, a person or entity must certify that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list. Both lists are found on Treasury's website at the following web addresses:
https://www.nj.gov/treasury/administration/pdf/RussiaBelarusEntityList.pdf
www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf . Bidders must review this list prior to completing the certification. If the Director of the Division of Purchase and Property finds a person or entity to be in violation of the law, s/he shall take action as may be appropriate and provided by law, rule or contract, including but not limited to, imposing sanctions, seeking compliance, recovering damages, declaring the party in default and seeking debarment or suspension of the party.

In addition, bidders must provide a detailed, accurate and precise description of the activities of the bidding person/entity, or one of its parents, subsidiaries or affiliates, engaging in Russia or Belarus and/or investment activities in Iran outlined above by completing the boxes on the lower portion of the enclosed form. The person or entity must cease engaging in any prohibited activities and provide an updated certification before the contract can be entered into. If a vendor or contractor is found to be in violation of law, action may be taken as appropriate and as may be provided by law, rule, or contract, including but not limited to imposing sanctions, seeking compliance, recovering damages, declaring the party in default, and seeking debarment or suspension of the party.

The ESCNJ has provided within these specifications, a Prohibited Russia-Belarus Activities & Iran Investment Activities certification form for all persons or entities, that plan to submit a bid, respond to a proposal, or renew a contract with the ESCNJ, to complete, sign and submit with the proposal. The Prohibited Russia-Belarus Activities & Iran Investment Activities Form is to be completed, certified and submitted prior to the award of contract, preferably with the bid submittal.
Please sign and submit the Disclosure of Investment Activities in Iran form and include with your bid package. This form must be submitted no later than the time of the award of a contact.

POLITICAL CONTRIBUTIONS DISCLOSURE – AWARD OF CONTRACTS

Pursuant to N.J.A.C. 6A:23A-6.3 (a) (1-4) please note the following:

Award of Contract – Reportable Contributions – N.J.A.C. 6A:23A-6.3 (a) (1)
"No board of education will vote upon or award any contract in the amount of $17,500 or greater to any business entity which has made a contribution reportable by the recipient under P.L. 1973, c83 (codified at N.J.S.A. 19:44A-1 et. seq.) to a member of the board of education during the preceding one-year period."

Contributions During Term of Contract – Prohibited – N.J.A.C. 6A:23A-6.3 (a) (2, 3)

"Contributions reportable by the recipient under P.L. 1973, c83 (codified at N.J.S.A. 19:44A-1 et. seq.) to any member of the school board from any business entity doing business with the school district are prohibited during the term of the contract."

"When a business entity referred in 4.1(e) is a natural person, contribution by that person's spouse or child that resides therewith, shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by any person or other business entity having an interest therein shall be deemed to be a contribution by the business entity."

Chapter 271 Political Contribution Disclosure Form – Required – N.J.A.C. 6A:23A-6.3 (a) (4)

All respondents shall submit with their bid package a completed and signed Chapter 271 Political Contribution Disclosure Form. The Chapter 271 form will be reviewed by the district to determine whether the vendor is in compliance with the aforementioned N.J.A.C. 6A:23A-6.3 (a) (2) Award of Contract.

The Chapter 271 Political Contribution Disclosure form shall be submitted with the response to the bid/proposal or no later than ten (10) days prior to the award of contract. Failure to provide the completed and signed form shall be cause for disqualification of the bid/proposal.

POLITICAL CONTRIBUTION DISCLOSURE STATEMENT – PAY TO PLAY

Annual Disclosure

A business entity as defined by law is advised of its responsibility to file an annual disclosure statement on political contributions with the **New Jersey Election Law Enforcement Commission** pursuant to N.J.S.A. 19:44A-20.13 (P.L. 2005 Chapter 271 section 3) if the business entity receives contracts in excess of $50,000 from public entities in a calendar year. It is the business entity's responsibility to determine if filing is necessary. Additional information on this requirement is available from the New Jersey Election Law Enforcement Commission at 1-888-313-3532 or at www.elec.state.nj.us.

Chapter 271 Political Contribution Disclosure Form

Business entities (contractors) receiving contracts from a public agency that are NOT awarded pursuant to a "fair and open" process (defined at N.J.S.A. 19:44A-20.7) are subject to the provisions of P.L. 2005, c. 271, s.2 (N.J.S.A. 19:44A-20.26). This law provides that 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

- any State, county, or municipal committee of a political party
- any legislative leadership committee*
- any continuing political committee (a.k.a., political action committee)
- any candidate committee of a candidate for, or holder of, an elective office:
  - of the public entity awarding the contract
  - of that county in which that public entity is located
  - of another public entity within that county
  - or of a legislative district in which that public entity is located or, when the public entity is a county,
  - of any legislative district which includes all or part of the county.

The disclosure must list reportable contributions to any of the committees that exceed $300 per election cycle that were made during the 12 months prior to award of the contract. See N.J.S.A. 19:44A-8 and 19:44A-16 for more details on reportable contributions.

The ESCNJ has provided a Chapter 271 Political Contribution Disclosure Form within the specifications package for use by the business entity. The ESCNJ has also provided a list of agencies to assist the contractor. The enclosed list of agencies is provided to assist the contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor's responsibility to identify the specific committees to which contributions may have been made and need to be disclosed. The disclosed information may exceed the minimum requirement.

STATEMENT OF OWNERSHIP N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)
No business organization, regardless of form of ownership, shall be awarded any contract for the performance of any work or the furnishing of any goods and services, unless, prior to the receipt of the bid or accompanying the bid of said business organization, bidders shall submit a statement setting forth the names and addresses of all persons and entities that own ten percent or more of its stock or interest of any type at all levels of ownership.

The included Statement of Ownership shall be completed and attached to the bid proposal. This requirement applies to all forms of business organizations, including, but not limited to, corporations and partnerships, publicly-owned corporations, limited partnerships, limited liability corporations, limited liability partnerships, sole proprietorship, and Subchapter S corporations. **Failure to submit a disclosure document shall result in rejection of the bid as it cannot be remedied after bids have been opened.**

Not-for-profit entities should fill in their name, check the not-for-profit box, and certify the form. No other information is required.

AFFIRMATIVE ACTION QUESTIONNAIRE

1. Our company has a federal Affirmative Action Plan approval. ☑ Yes □ No

   If yes, please attach a copy of the plan to this questionnaire.

2. Our company has a New Jersey State Certificate of Employee Information Report. ☑ Yes □ No

   If yes, please attach a copy of the certificate to this questionnaire.

3. If you answered "***NO"*** to both questions above, No. 1 and 2, you must apply for an Affirmative Action Employee Information Report – Form AA302.

Please visit the New Jersey Department of Treasury website for the Division of Public Contracts Equal Employment Opportunity Compliance:

https://www.nj.gov/treasury/contract_compliance/

a. Click on "Employee Information Report"
b. Complete and submit the form with the *appropriate payment* to:

Department of Treasury
Division of Purchase and Property
Contract Compliance and Audit Unit
EEO Monitoring P.O. Box 206
Trenton, New Jersey 08625-0206

All fees for this application are to be paid directly to the State of New Jersey. A copy shall be submitted to the ESCNJ prior to the execution or award of contract.

I certify that the above information is correct to the best of my knowledge.

Name of Company/Firm SHI International Corp.

Address 290 Davidson Ave.
City, State, Zip Somerset, NJ 08873

Name of Authorized Agent Moitrayee Majumdar Title Senior Proposal Specialist
SIGNATURE Moitrayee Majumdar Date 09/05/2024

APPENDIX A
AMERICANS WITH DISABILITIES ACT OF 1990
Equal Opportunity for Individuals with Disability

The contractor and the Educational Services Commission of New Jersey (hereafter "owner") do hereby agree that the provisions of Title 11 of the Americans with Disabilities Act of 1990 (the "Act") (42 U.S.C. S121 01 et seq.), which prohibits discrimination on the basis of disability by public entities in all services, programs, and activities provided or made available by public entities, and the rules and regulations promulgated pursuant there unto, are made a part of this contract. In providing any aid, benefit, or service on behalf of the owner pursuant to this contract, the contractor agrees that the performance shall be in strict compliance with the Act. In the event that the contractor, its agents, servants, employees, or subcontractors violate or are alleged to have violated the Act during the performance of this contract, the contractor shall defend the owner in any action or administrative proceeding commenced pursuant to this Act. The contractor shall indemnify, protect, and save harmless the owner, its agents, servants, and employees from and against any and all suits, claims, losses, demands, or damages, of whatever kind or nature arising out of or claimed to arise out of the alleged violation. The contractor shall, at its own expense, appear, defend, and pay any and all charges for legal services and any and all costs and other expenses arising from such action or administrative proceeding or incurred in connection therewith. In any and all complaints brought pursuant to the owner's grievance procedure, the contractor agrees to abide by any decision of the owner which is rendered pursuant to said grievance procedure. If any action or administrative proceeding results in an award of damages against the owner, or if the owner incurs any expense to cure a violation of the ADA which has been brought pursuant to its grievance procedure, the contractor shall satisfy and discharge the same at its own expense.

The owner shall, as soon as practicable after a claim has been made against it, give written notice thereof to the contractor along with full and complete particulars of the claim, If any action or administrative proceeding is brought against the owner or any of its agents, servants, and employees, the *owner shall* expeditiously forward or have forwarded to the contractor every demand, complaint, notice, summons, pleading, or other process received by the owner or its representatives.

It is expressly agreed and understood that any approval by the owner of the services provided by the contractor pursuant to this contract will not relieve the contractor of the obligation to comply with the Act and to defend, indemnify, protect, and save harmless the owner pursuant to this paragraph.

It is further agreed and understood that the owner assumes no obligation to indemnify or save harmless the contractor, its agents, servants, employees and subcontractors for any claim which may arise out of their performance of this Agreement. Furthermore, the contractor expressly understands and agrees that the provisions of this indemnification clause shall in no way limit the contractor's obligations assumed in this Agreement, nor shall they be construed to relieve the contractor from any liability, nor preclude the owner from taking any other actions available to it under any other provisions of the Agreement or otherwise at law.

Company SHI International Corp. Name Moitrayee Majumdar

Signature Moitrayee Majumdar Title Senior Proposal Specialist

Date: 09/05/2024

ASSURANCE OF COMPLIANCE

Contact with Students

There may be times during the performance of this contract, where a contracted service provider may come in contact with students of the school district. The district fully understands it obligation to provide to all students and staff members, a safe educational environment. To this end, the district is requiring all bidders to sign a statement of Assurance of Compliance, acknowledging the bidder's understanding of the below listed requirements and further acknowledging the bidder's assurance of compliance with those listed requirements.

Anti-Bullying Reporting--Requirement

When applicable, the contracted service provider shall comply with all applicable provisions of the New Jersey Anti-Bullying Bill of Rights Act—N.J.S.A. 18A:37-13.1 et seq., all applicable code and regulations, and the Anti-Bullying Policy of the Board of Education. In accordance with N.J.A.C. 6A:16-7.7 (c), a contracted service provider, who has witnessed, or has reliable information that a student has been subject to harassment, intimidation, or bullying shall immediately report the incident to any school administrator or safe schools resource officer, or the School Business Administrator/Board Secretary.

Criminal History Background Checks—N.J.S.A. 18A:6-7.1--Requirement

When applicable, the contracted service provider, shall provide to the school district prior to commencement of contract, evidence or proof that each employee assigned to provide services and that comes in **regular contact** with students, has had a criminal history background check, and furthermore, that said background check indicates that no criminal history record information exists on file for that worker. Failure to provide a proof of criminal history background check for any employee coming in regular contact with students, prior to commencement of contact, may be cause for breach of contract. See NJDOE Broadcast 9/9/19.

Pre-Employment Requirements

When applicable, all contracted service providers, whose employees have **regular contact with students**, shall comply with the Pre-Employment Requirements in accordance with New Jersey P.L. 2018 c.5, N.J.S.A. 18A:6-7.6 et seq. Contracted service providers are to review the following New Jersey Department of Education Office of Student Protection—Pre-Employment Resource P.L. 2018 c.5 link below for guidance and compliance procedures.

https://www.nj.gov/education/crimhist/preemployment/

Name of Company SHI International Corp.

Name of Authorized Representative Moitrayee Majumdar

Signature Moitrayee Majumdar Date 09/05/2024

(Revised: January, 2016)

EXHIBIT A
MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE
N.J.S.A. 10:5-31 et seq. (P.L. 1975, C. 127)
N.J.A.C. 17:27
GOODS, PROFESSIONAL SERVICE AND GENERAL SERVICE CONTRACTS

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Except with respect to affectional or sexual orientation and gender identity or expression, the contractor will ensure that equal employment opportunity is afforded to such applicants in recruitment and employment, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Such equal employment opportunity shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this nondiscrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex.

The contractor or subcontractor will send to each labor union, with which it has a collective bargaining agreement, a notice, to be provided by the agency contracting officer, advising the labor union of the contractor's commitments under this chapter and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to N.J.S.A. 10:5-31 et seq., as amended and supplemented from time to time and the Americans with Disabilities Act.

The contractor or subcontractor agrees to make good faith efforts to meet targeted county employment goals established in accordance with N.J.A.C. 17:27-5.2.

The contractor or subcontractor agrees to inform in writing its appropriate recruitment agencies including, but not limited to, employment agencies, placement bureaus, colleges, universities, and labor unions, that it does not discriminate on the basis of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job related testing, as established by the statutes and court decisions of the State of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

In conforming with the targeted employment goals, the contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and layoff to ensure that all such actions are taken without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The contractor shall submit to the public agency, after notification of award but prior to execution of a goods and services contract, one of the following three documents:

- Letter of Federal Affirmative Action Plan Approval
- Certificate of Employee Information Report
- Employee Information Report Form AA302 (electronically provided by the Division and distributed to the public agency through the Division's website at https://www.nj.gov/treasury/contract_compliance/

The contractor and its subcontractors shall furnish such reports or other documents to the Division of Purchase & Property, CCAU, EEO Monitoring Program as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Division of Purchase & Property, CCAU, EEO Monitoring Program for conducting an investigation pursuant to N.J.A.C. 17:27-1.1 et seq.

Company SHI International Corp. Name Moitrayee Majumdar

Signature Moitrayee Majumdar Title Senior Proposal Specialist

Date: _____

Form AA302
Rev. 11/11

STATE OF NEW JERSEY

Division of Purchase & Property
Contract Compliance Audit Unit
EEO Monitoring Program

EMPLOYEE INFORMATION REPORT

IMPORTANT-READ INSTRUCTIONS CAREFULLY BEFORE COMPLETING FORM. FAILURE TO PROPERLY COMPLETE THE ENTIRE FORM AND TO SUBMIT THE REQUIRED $150.00 FEE MAY DELAY ISSUANCE OF YOUR CERTIFICATE. DO NOT SUBMIT EEO-1 REPORT FOR SECTION B, ITEM 11. For Instructions on completing the form, go to: http://www.state.nj.us/treasury/contract_compliance/pdf/aa302ins.pdf

SECTION A - COMPANY IDENTIFICATION

1. FID. NO. OR SOCIAL SECURITY
2. TYPE OF BUSINESS ☐ 1. MFG ☐ 2. SERVICE ☐ 3. WHOLESALE ☐ 4. RETAIL ☐ 5. OTHER
3. TOTAL NO. EMPLOYEES IN THE ENTIRE COMPANY
4. COMPANY NAME
5. STREET CITY COUNTY STATE ZIP CODE
6. NAME OF PARENT OR AFFILIATED COMPANY (IF NONE, SO INDICATE) CITY STATE ZIP CODE
7. CHECK ONE: IS THE COMPANY: ☐ SINGLE-ESTABLISHMENT EMPLOYER ☐ MULTI-ESTABLISHMENT EMPLOYER
8. IF MULTI-ESTABLISHMENT EMPLOYER, STATE THE NUMBER OF ESTABLISHMENTS IN NJ
9. TOTAL NUMBER OF EMPLOYEES AT ESTABLISHMENT WHICH HAS BEEN AWARDED THE CONTRACT
10. PUBLIC AGENCY AWARDING CONTRACT CITY COUNTY STATE ZIP CODE

Official Use Only	DATE RECEIVED	INAUG DATE	ASSIGNED CERTIFICATION NUMBER

SECTION B - EMPLOYMENT DATA

11. Report all permanent, temporary and part-time employees ON YOUR OWN PAYROLL. Enter the appropriate figures on all lines and in all columns. Where there are no employees in a particular category, enter a zero. Include ALL employees, not just those in minority/non-minority categories, in columns 1, 2, & 3. *DO NOT SUBMIT AN EEO-1 REPORT.*

JOB CATEGORIES	ALL EMPLOYEES COL. 1 TOTAL (Cols.2 &3)	COL. 2 MALE	COL. 3 FEMALE	PERMANENT MINORITY/NON-MINORITY EMPLOYEE BREAKDOWN MALE: BLACK	HISPANIC	AMER. INDIAN	ASIAN	NON MIN.	FEMALE: BLACK	HISPANIC	AMER. INDIAN	ASIAN	NON MIN.
Officials/ Managers													
Professionals													
Technicians													
Sales Workers													
Office & Clerical													
Craftworkers (Skilled)													
Operatives (Semi-skilled)													
Laborers (Unskilled)													
Service Workers													
TOTAL													
Total employment From previous Report (if any)													
Temporary & Part-Time Employees	The data below shall NOT be included in the figures for the appropriate categories above.												

SAMPLE

12. HOW WAS INFORMATION AS TO RACE OR ETHNIC GROUP IN SECTION B OBTAINED? ☐ 1. Visual Survey ☐ 2. Employment Record ☐ 3. Other (Specify)
13. DATES OF PAYROLL PERIOD USED From: To:
14. IS THIS THE FIRST Employee Information Report Submitted? 1. YES ☐ 2. NO ☐
15. IF NO, DATE LAST REPORT SUBMITTED MO. DAY YEAR

SECTION C - SIGNATURE AND IDENTIFICATION

16. NAME OF PERSON COMPLETING FORM (Print or Type) SIGNATURE TITLE DATE MO DAY YEAR
17. ADDRESS NO. & STREET CITY COUNTY STATE ZIP CODE PHONE (AREA CODE, NO., EXTENSION) - -

To download the AA-302 form, click this link:
https://www.nj.gov/treasury/contract_compliance/documents/pdf/forms/aa302.pdf

INSTRUCTIONS FOR COMPLETING THE EMPLOYEE INFORMATION REPORT (FORM AA302)

IMPORTANT: READ THE FOLLOWING INSTRUCTIONS CAREFULLY BEFORE COMPLETING THE FORM. PRINT OR TYPE ALL INFORMATION. FAILURE TO PROPERLY COMPLETE THE ENTIRE FORM **AND TO SUBMIT THE REQUIRED $150.00 NON-REFUNDABLE FEE MAY DELAY ISSUANCE OF YOUR CERTIFICATE**. **IF YOU HAVE A CURRENT CERTIFICATE OF EMPLOYEE INFORMATION REPORT, DO NOT COMPLETE THIS FORM UNLESS YOUR ARE RENEWING A CERTIFICATE THAT IS DUE FOR EXPIRATION. DO NOT COMPLETE THIS FORM FOR CONSTRUCTION CONTRACT AWARDS.**

ITEM 1 - Enter the Federal Identification Number assigned

by the Internal Revenue Service, or if a Federal Employer Identification Number has been applied for, or if your business is such that you have not or will not receive a Federal Employer Identification Number, enter the Social Security Number of the owner or of one partner, in the case of a partnership.

ITEM 2 - Check the box appropriate to your TYPE OF BUSINESS. If you are engaged in more than one type of business check the predominate one. If you are a manufacturer deriving more than 50% of your receipts from your own retail outlets, check “Retail”.

ITEM 3 - Enter the total “number” of employees in the entire company, including part-time employees. This number shall include all facilities in the entire firm or corporation.

ITEM 4 - Enter the name by which the company is identified. If there is more than one company name, enter the predominate one.

ITEM 5 - Enter the physical location of the company. Include City, County, State and Zip Code.

ITEM 6 - Enter the name of any parent or affiliated company including the City, County, State and Zip Code. If there is none, so indicate by entering “None” or N/A.

ITEM 7 - Check the box appropriate to your type of company establishment. “Single-establishment Employer” shall include an employer whose business is conducted at only one physical location. “Multi-establishment Employer” shall include an employer whose business is conducted at more than one location.

ITEM 8 - If “Multi-establishment” was entered in item 8, enter the number of establishments within the State of New Jersey.

ITEM 9 - Enter the total number of employees at the establishment being awarded the contract.

ITEM 10 - Enter the name of the Public Agency awarding the Include City, County, State and Zip Code. This is Number. not applicable if you are renewing a current certificate.

ITEM 11 - Enter the appropriate figures on all lines and in all

columns. THIS SHALL ONLY INCLUDE EMPLOYMENT DATA FROM THE FACILITY THAT IS BEING AWARDED THE CONTRACT. DO NOT list the same employee in more than one job category. **DO NOT attach an EEO-1 Report.**

Racial/Ethnic Groups will be defined:
Black: Not of Hispanic origin. Persons having origin in any of the Black racial groups of Africa.
Hispanic: Persons of Mexican, Puerto Rican, Cuban, or Central or South American or other Spanish culture or origin, regardless of race.
American Indian or Alaskan Native: Persons having origins in any of the original peoples of North America, and who maintain cultural identification through tribal affiliation or community recognition.
Asian or Pacific Islander: Persons having origin in any of the original peoples of the Far East, Southeast Asia, the Indian Sub-continent or the Pacific Islands. This area includes for example, China, Japan, Korea, the Philippines Islands and Samoa.
Non-Minority: Any Persons not identified in any of the aforementioned Racial/Ethnic Groups.

ITEM 12 - Check the appropriate box. If the race or ethnic group information was not obtained by 1 or 2, specify by what other means this was done in 3.

ITEM 13 - Enter the dates of the payroll period used to prepare the employment data presented in Item 12.

ITEM 14 - If this is the first time an Employee Information Report has been submitted for this company, check block “Yes”.

ITEM 15 - If the answer to Item 15 is “No”, enter the date when the last Employee Information Report was submitted by this company.

ITEM 16 - Print or type the name of the person completing the form. Include the signature, title and date.

ITEM 17 - Enter the physical location where the form is being completed. Include City, State, Zip Code and Phone contact.

TYPE OR PRINT IN SHARP BALL POINT PEN

THE VENDOR IS TO COMPLETE THE EMPLOYEE INFORMATION REPORT FORM (AA302) AND RETAIN A COPY FOR THE VENDOR’S OWN FILES. THE VENDOR SHOULD ALSO SUBMIT A COPY TO THE PUBLIC AGENCY AWARDING THE CONTRACT IF THIS IS YOUR FIRST REPORT; AND FORWARD ONE COPY **WITH A CHECK IN THE AMOUNT OF $150.00 PAYABLE TO THE TREASURER, STATE OF NEW JERSEY(FEE IS NON-REFUNDABLE)** TO:

NJ Department of the Treasury
Division of Public Contracts Equal Employment Opportunity Compliance

P.O. Box 206

Trenton, New Jersey 08625-0206 Telephone No. (609) 292-5473

Educational Services Commission of New Jersey

Business Office

1660 Stelton Road, Floor 2
Piscataway, New Jersey 08854

Chapter 271
Political Contribution Disclosure Form

(Contracts that Exceed $17,500.00)
Ref. N.J.S.A. 19:44A-20.26

The undersigned, being authorized and knowledgeable of the circumstances, does hereby certify that SHI International Corp. (Business Entity) has made the following **reportable** political contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26 during the twelve (12) months preceding this award of contract:

Reportable Contributions

Date of Contribution	Amount of Contribution	Name of Recipient Elected Official/ Committee/Candidate	Name of Contributor
Not Applicable	Not Applicable	Not Applicable	Not Applicable

The Business Entity may attach additional pages if needed.

☑ **No Reportable Contributions** (Please check (✔) if applicable.)

I certify that SHI International Corp. (Business Entity) made no reportable contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26.

Certification

I certify that the information provided above is in full compliance with Public law 2005 – Chapter 271.

Name of Authorized Agent Moitrayee Majumdar

Signature Moitrayee Majumdar Title Senior Proposal Specialist

Business Entity SHI International Corp.

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

Contractor Instructions

Business entities (contractors) receiving contracts from a public agency that are NOT awarded pursuant to a "fair and open" process (defined at N.J.S.A. 19:44A-20.7) are subject to the provisions of P.L. 2005, c. 271, s. 2 (N.J.S.A. 19:44A-20.26). This law provides that 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

- any State, county, or municipal committee of a political party
- any legislative leadership committee*[1]
- any continuing political committee (a.k.a., political action committee)
- any candidate committee of a candidate for, or holder of, an elective office:
    - of the public entity awarding the contract
    - of that county in which that public entity is located
    - of another public entity within that county
    - or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county

The disclosure must list reportable contributions to any of the committees that exceed $300 per election cycle that were made during the 12 months prior to award of the contract. See N.J.S.A. 19:44A-8 and 19:44A-16 for more details on reportable contributions.

N.J.S.A. 19:44A-20.26 itemizes the parties from whom contributions must be disclosed when a business entity is not a natural person. This includes the following:

- individuals with an "interest" ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit
- all principals, partners, officers, or directors of the business entity or their spouses
- any subsidiaries directly or indirectly controlled by the business entity
- IRS Code Section 527 New Jersey based organizations, directly or indirectly controlled by the business entity and filing as continuing political committees, (PACs)

When the business entity is a natural person, "a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity." [N.J.S.A. 19:44A-20.26(b)]. The contributor must be listed on the disclosure.

Any business entity that fails to comply with the disclosure provisions shall be subject to a fine imposed by ELEC in an amount to be determined by the Commission which may be based upon the amount that the business entity failed to report.

The enclosed list of agencies is provided to assist the contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor's responsibility to identify the specific committees to which contributions may have been made and need to be disclosed. The disclosed information may exceed the minimum requirement.

The enclosed form, a content-consistent facsimile, or an electronic data file containing the required details (along with a signed over sheet) may be used as the contractor's submission and is disclosable to the public under the Open Public Records Act.

The contractor must also complete the attached Stockholder Disclosure Certification. This will assist the agency in meeting its obligations under the law. **NOTE: This section does not apply to Board of Education contracts.**

P.L. 2005, c. 271

[1] N.J.S.A. 19:44A-3(s): "The term "legislative leadership committee" means a committee established, authorized to be established, or designated by the President of the Senate, the Minority Leader of the Senate, the Speaker of the General Assembly or the Minority Leader of the General Assembly pursuant to section 16 of P.L. 1993, c. 65 (C. 19:44A-10.1) for the purpose of receiving contributions and making expenditures."

(Unofficial version, Assembly Committee Substitute to A-3013, First Reprint*)

AN ACT authorizing units of local government to impose limits on political contributions by contractors and supplementing Title 40A of the New Jersey Statutes and Title 19 of the Revised Statutes.

BE IT ENACTED by the Senate and General Assembly of the State of New Jersey:

40A:11-51 1. a. A county, municipality, independent authority, board of education, or fire district is hereby authorized to establish by ordinance, resolution or regulation, as may be appropriate, measures limiting the awarding of public contracts there from to business entities that have made a contribution pursuant to P.L. 1973, c. 83 (C. 19:44A-1 et seq.) and limiting the contributions that the holders of a contract can make during the term of a contract, notwithstanding the provisions and parameters of sections 1 through 12 of P.L. 2004, c. 19 (C. 19:44A-20.2 et al.) and section 22 of P.L. 1973, c. 83 (C. 19:44A-22).

b. The provisions of P.L. 2004, c. 19 shall not be construed to supersede or preempt any ordinance, resolution or regulation of a unit of local government that limits political contributions by business entities performing or seeking to perform government contracts. Any ordinance, resolution or regulation in effect on the effective date of P.L. 2004, c. 19 shall remain in effect and those adopted after that effective date shall be valid and enforceable.

c. An ordinance, resolution or regulation adopted or promulgated as provided in this section shall be filed with the Secretary of State.

19:44A-20.26 2. a. Not later than 10 days prior to entering into any contract having an anticipated value in excess of $17,500, except for a contract that is required by law to be publicly advertised for bids, a State agency, county, municipality, independent authority, board of education, or fire district shall require any business entity bidding thereon or negotiating therefor, to submit along with its bid or price quote, a list of political contributions as set forth in this subsection that are reportable by the recipient pursuant to the provisions of P.L. 1973, c. 83 (C.19:44A-1 et seq.) and that were made by the business entity during the preceding 12 month period, along with the date and amount of each contribution and the name of the recipient of each contribution. A business entity contracting with a State agency shall disclose contributions to any State, county, or municipal committee of a political party, legislative leadership committee, candidate committee of a candidate for, or holder of, a State elective office, or any continuing political committee. A business entity contracting with a county, municipality, independent authority, other than an independent authority that is a State agency, board of education, or fire district shall disclose contributions to: any State, county, or municipal committee of a political party; any legislative leadership committee; or any candidate committee of a candidate for, or holder of, and elective office of that public entity, of that county in which that public entity is located, of another public entity within that county, or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county, or any continuing political committee.

The provisions of this section shall not apply to a contract when a public emergency requires the immediate delivery of goods or services.

b. When a business entity is a natural person, a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by any person or other business entity having an interest therein shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by: all principals, partners, officers, or directors of the business entity or their spouses; any subsidiaries directly or indirectly controlled by the business entity; or any political organization organized under section 527 of the Internal Revenue Code that is directly or indirectly controlled by the business entity, other than a candidate committee, election fund, or political party committee, shall be deemed to be a contribution by the business entity.

c. As used in this section:
"business entity" means a natural or legal person, business corporation, professional services corporation, limited liability company, partnership, limited partnership, business trust, association or any other legal commercial entity organized under the laws of this State or of any other state or foreign jurisdiction;

"interest" means the ownership or control of more than 10% of the profits or assets of a business entity of 10% of the stock in the case of a business entity that is a corporation for profit, as appropriate; and

P.L. 2005, c. 271

"State agency" means any of the principal departments in the Executive Branch of the State Government, and any division, board, bureau, office, commission or other instrumentality within or created by such department, the Legislature of the State and any

office, board, bureau or commission within or created by the Legislative Branch, and any independent State authority, commission, instrumentality or agency.

d. Any business entity that fails to comply with the provisions of this section shall be subject to a fine imposed by the New Jersey Election Law Enforcement Commission in an amount to be determined by the commission which may be based upon the amount that the business entity failed to report.

19:44A-20.13 3. a. Any business entity making a contribution of money or any other thing of value, including an in-kind contribution, or pledge to make a contribution of any kind to a candidate for or the holder of any public office having ultimate responsibility for the awarding of public contracts, or to a political party committee, legislative leadership committee, political committee or continuing political committee, which has received in any calendar year $50,000 or more in the aggregate through agreements or contracts with a public entity, shall file an annual disclosure statement with the New Jersey Election Law Enforcement Commission, established pursuant to section 5 of P.L. 1973, c. 83 (C. 19:44A-5), setting forth all such contributions made by the business entity during the 12 months prior to the reporting deadline.

b. The commission shall prescribe forms and procedures for the reporting required in subsection a. of this section which shall include,
but not be limited to:

(1) the name and mailing address of the business entity making the contribution, and the amount contributed during the 12 months prior to the reporting deadline;

(2) the name of the candidate for or the holder of any public office having ultimate responsibility for the awarding of public contracts, candidate committee, joint candidates committee, political party committee, legislative leadership committee, political committee or continuing political committee receiving the contribution; and

(3) the amount of money the business entity received from the public entity through contract or agreement, the dates, and information identifying each contract or agreement and describing the goods, services or equipment provided or property sold.

c. The commission shall maintain a list of such reports for public inspection both at its office and through its Internet site.

d. When a business entity is a natural person, a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by any person or other business entity having an interest therein shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by: all principals, partners, officers, or directors of the business entity, or their spouses; any subsidiaries directly or indirectly controlled by the business entity; or any political organization organized under section 527 of the Internal Revenue Code that is directly or indirectly controlled by the business entity, other than a candidate committee, election fund, or political party committee, shall be deemed to be a contribution by the business entity.

As used in this section:

"Business entity" means a natural or legal person, business corporation, professional services corporation, limited liability company, partnership, limited partnership, business trust, association or any other legal commercial entity organized under the laws of this State or of any other state or foreign jurisdiction; and

"Interest" means the ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit, as appropriate.

e. Any business entity that fails to comply with the provisions of this section shall be subject to a fine imposed by the New Jersey Election Law Enforcement Commission in an amount to be determined by the commission which may be based upon the amount that the business entity failed to report.

4. This act shall take effect immediately.

*Note: Bold italicized statutory references of new sections are anticipated and not final as of the time this document was prepared. Statutory compilations of N.J.S.A. 18A:18A-51 is anticipated to show a reference to N.J.S.A. 40:11-51 and to N.J.S.A. 19:44A-20.26.

Prohibited Russia-Belarus Activities & Iran Investment Activities

Person or Entity	SHI International Corp.

Part 1: Certification

COMPLETE PART 1 BY CHECKING **ONE OF THE THREE BOXES BELOW**

Pursuant to law, any person or entity that is a successful bidder or proposer, or otherwise proposes to enter into or renew a contract, for goods or services must complete the certification below prior to contract award to attest, under penalty of perjury, that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list or Chapter 25 list as a person or entity engaging in prohibited activities in Russia, Belarus or Iran. Before a contract for goods or services can be amended or extended, a person or entity must certify that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list. Both lists are found on Treasury's website at the following web addresses:

https://www.nj.gov/treasury/administration/pdf/RussiaBelarusEntityList.pdf
www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf.

As applicable to the type of contract, the above-referenced lists must be reviewed prior to completing the below certification.

A person or entity unable to make the certification must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran. The person or entity must cease engaging in any prohibited activities and provide an updated certification before the contract can be entered into.

If a vendor or contractor is found to be in violation of law, action may be taken as appropriate and as may be provided by law, rule, or contract, including but not limited to imposing sanctions, seeking compliance, recovering damages, declaring the party in default, and seeking debarment or suspension of the party.

CONTRACT AWARDS AND RENEWALS

☑	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate appears on the N.J. Department of Treasury's lists of entities engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3 or in investment activities in Iran pursuant to P.L. 2012, c. 25 ("Chapter 25 List"). I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf.* (Skip Part 2 and sign and complete the Certification below.)
CONTRACT AMENDMENTS AND EXTENSIONS	
☐	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate is listed on the N.J. Department of the Treasury's lists of entities determined to be engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3. I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf.* (Skip Part 2 and sign and complete the Certification below.)
IF UNABLE TO CERTIFY	
☐	*I am unable to certify as above because the person or entity and/or a parent entity, subsidiary, or affiliate is listed on the Department's Russia-Belarus list and/or Chapter 25 Iran list. I will provide a detailed, accurate, and precise description of the activities as directed in Part 2 below, and sign and complete the Certification below. Failure to provide such will prevent the award of the contract to the person or entity, and appropriate penalties, fines, and/or sanctions will be assessed as provided by law.*

Part 2: Additional Information

PLEASE PROVIDE FURTHER INFORMATION RELATED TO PROHIBITED ACTIVITIES IN RUSSIA OR BELARUS AND/OR INVESTMENT ACTIVITIES IN IRAN.

You must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran in the space below and, if needed, on additional sheets provided by you.

Not Applicable

Part 3: Certification of True and Complete Information

I, being duly sworn upon my oath, hereby represent and state that the foregoing information and any attachments there, to the best of my knowledge, are true and complete. I attest that I am authorized to execute this certification on behalf of the above-referenced person or entity.

*I acknowledge that the <**Name of Contracting Unit**> is relying on the information contained herein and hereby acknowledge that I am under a continuing obligation from the date of this certification through the completion of any contracts with the <**Name of Contracting Unit**> to notify the <**Name of Contracting Unit**> in writing of any changes to the answers of information contained herein.*

*I acknowledge that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I recognize that I am subject to criminal prosecution under the law and that it will also constitute a material breach of my agreement(s) with the <**Name of Contracting Unit**> and that the <**Name of Contracting Unit**> at its option may declare any contract(s) resulting from this certification void and unenforceable.*

Full Name (Print)	Moitrayee Majumdar	**Title**	Senior Proposal Specialist
Signature	Moitrayee Majumdar	**Date**	09/05/2024

Statement of Suspension or Debarment

STATE OF NEW JERSEY/ State of California
Specify, of other

COUNTY OF San Diego, CA

I, Moitrayee Majumdar **of the (City, Town, Borough)**

of San Diego **State of** California **of full age,**

being duly sworn according to law on my oath depose and say that:

I am authorized representative **of the firm**

of SHI International Corp. **the Bidder**

making the Proposal for the above named projects, and that I executed the said Proposal with full authority to do so; that said Bidder is not at the time of the making this bid included on the New Jersey State Treasurer's or the Federal Government's List of Debarred, Suspended or Disqualified Bidders or the State Department of Labor and Workforce Development; Prevailing Wage Debarment List as a result of action taken by any State or Federal Agency.

Name of Contractor: SHI International Corp.
(Company Name)

By: Moitrayee Majumdar
(Signature of authorized representative)

Subscribed and sworn to before me

This 05 **day of** September **, 20** 24

(Seal) Notary Public of New Jersey/
Specify Other State

MAYA LYNCH
Commission # 50211505
Notary Public, State of New Jersey
My Commission Expires
June 28, 2028

My Commission expires June 28 **20** 28

STATEMENT OF OWNERSHIP DISCLOSURE

N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

Name of Organization: SHI International Corp.
Organization Address: 290 Davidson Ave.
City, State, ZIP: Somerset, NJ 08873

Part I Check the box that represents the type of business organization:

☐ Sole Proprietorship (skip Parts II and III, execute certification in Part IV)

☐ Non-Profit Corporation (skip Parts II and III, execute certification in Part IV)

☑ For-Profit Corporation (any type) S Corporation ☐ Limited Liability Company (LLC)

☐ Partnership ☐ Limited Partnership ☐ Limited Liability Partnership (LLP)

☐ Other (be specific): _____

Part II Check the appropriate box

☑ The list below contains the names and addresses of all stockholders in the corporation who own 10 percent or more of its stock, of any class, or of all individual partners in the partnership who own a 10 percent or greater interest therein, or of all members in the limited liability company who own a 10 percent or greater interest therein, as the case may be. (**COMPLETE THE LIST BELOW IN THIS SECTION**)

OR

☐ No one stockholder in the corporation owns 10 percent or more of its stock, of any class, or no individual partner in the partnership owns a 10 percent or greater interest therein, or no member in the limited liability company owns a 10 percent or greater interest therein, as the case may be. (**SKIP TO PART IV**)

(Please attach additional sheets if more space is needed):

Name of Individual or Business Entity	Home Address (for Individuals) or Business Address
Thai Lee (President and CEO)	Texas, SHI does not provide personal information, such as home addresses, as we deem this information confidential. However, we have provided the state of residence for our President/CEO and Chairman of the Board. Further, SHI's business address is 290 Davidson Ave., Somerset, NJ 08873.
KoGuan Leo (Chairman of the Board)	

Part III DISCLOSURE OF 10% OR GREATER OWNERSHIP IN THE STOCKHOLDERS, PARTNERS OR LLC MEMBERS LISTED IN PART II

If a bidder has a direct or indirect parent entity which is publicly traded, and any person holds a 10 percent or greater beneficial interest in the publicly traded parent entity as of the last annual federal Security and Exchange Commission (SEC) or foreign equivalent filing, ownership disclosure can be met by providing links to the website(s) containing the last annual filing(s) with the federal Securities and Exchange Commission (or foreign equivalent) that contain the name and address of each person holding a 10% or greater beneficial interest in the publicly traded parent entity, along with the relevant page numbers of the filing(s) that contain the information on each such person. **Attach additional sheets if more space is needed**.

Website (URL) containing the last annual SEC (or foreign equivalent) filing	Page #'s
SHI is S corporation, SHI's co-founders, Thai Lee and KoGuan Leo remain the majority and minority	
shareholders, respectively, and also constitute SHI's Board of Director. SHI is not a publicly traded company.	

Please list the names and addresses of each stockholder, partner or member owning a 10 percent or greater interest in any corresponding corporation, partnership and/or limited liability company (LLC) listed in Part II **other than for any publicly traded parent entities referenced above**. The disclosure shall be continued until names and addresses of every non-corporate stockholder, and individual partner, and member exceeding the 10 percent ownership criteria established pursuant to N.J.S.A. 52:25-24.2 has been listed. **Attach additional sheets if more space is needed.**

Stockholder/Partner/Member and Corresponding Entity Listed in Part II	Home Address (for Individuals) or Business Address
Not Applicable	

Part IV Certification

I, being duly sworn upon my oath, hereby represent that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I acknowledge: that I am authorized to execute this certification on behalf of the bidder/proposer; that the ***ESCNJ and/or its members*** is relying on the information contained herein and that I am under a continuing obligation from the date of this certification through the completion of any contracts with the ***ESCNJ and/or its members*** to notify the ***ESCNJ and/or its members*** in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the, permitting the ***ESCNJ and/or its members*** to declare any contract(s) resulting from this certification void and unenforceable.

Full Name (Print):	Moitrayee Majumdar	Title:	Senior Proposal Specialist
Signature:	Moitrayee Majumdar	Date:	09/05/2024

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

NEW JERSEY REQUIRED DOCUMENTS FOR PUBLIC WORKS BIDS

SHI is not proposing to provide any Public Works related services and hence this part of the form is Not Applicable to SHI.

BUSINESS REGISTRATION CERTIFICATE (N.J.S.A. 52:32-44)

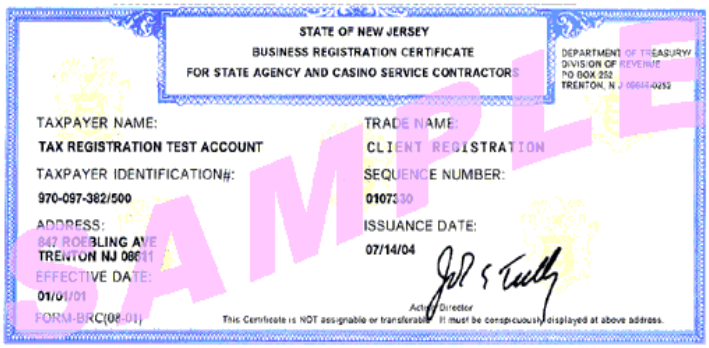
Pursuant to N.J.S.A. 52:32-44, all respondents shall submit prior to award of bid, a copy of their "New Jersey Business Registration Certificate" as issued by the Department of Treasury of the State of New Jersey. The ESCNJ requests that all respondents for this bid/proposal submit a current New Jersey Business Registration Certificate with the bid/proposal but no later than date of award.

Goods and Services Contracts

N.J.S.A. 52:32-44 imposes the following requirements on contractors and all subcontractors that knowingly provide goods or perform services for a contractor fulfilling this contract:

3. The contractor shall not enter into a contract with a subcontractor unless the subcontractor first provides the contractor with a valid proof of business registration.
4. The contractor shall maintain and submit to the Contracting Agency a list of subcontractors and their addresses that may be updated from time to time.
3. Prior to receipt of final payment from a contracting agency, a contractor must submit to the contracting agency an accurate list of all subcontractors or attest that none was used.
4. The contractor and any subcontractor providing goods or performing services under the contract, and each of their affiliates, shall collect and remit to the Director of the Division of Taxation in the Department of the Treasury, the use tax due pursuant to the Sales and Use Tax Act, (N.J.S.A. 54:32B-1 et seq.) on all sales of tangible personal property delivered into the State. Any questions in this regard can be directed to the Division of Taxation at (609) 292-6400.

For more information on how to obtain a Business Registration Certificate, please visit the State of New Jersey, Department of Treasury, Division of Revenue and Enterprise Services website at:
http://www.state.nj.us/treasury/revenue/busregcert.shtml


STATE OF NEW JERSEY
BUSINESS REGISTRATION CERTIFICATE
FOR STATE AGENCY AND CASINO SERVICE CONTRACTORS

DEPARTMENT OF TREASURY
DIVISION OF REVENUE
PO BOX 252
TRENTON, NJ 08646-0252

TAXPAYER NAME:
TAX REGISTRATION TEST ACCOUNT

TRADE NAME:
CLIENT REGISTRATION

TAXPAYER IDENTIFICATION#:
970-097-362/500

SEQUENCE NUMBER:
0107330

ADDRESS:
847 ROEBLING AVE
TRENTON NJ 08611

ISSUANCE DATE:
07/14/04

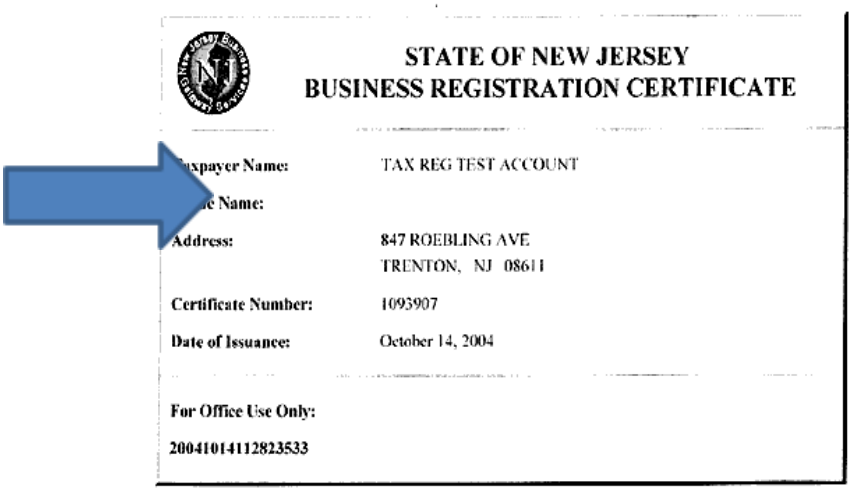
EFFECTIVE DATE:
01/01/01

Acting Director

FORM BRC(08-01)

This Certificate is NOT assignable or transferable. It must be conspicuously displayed at above address.

SAMPLE


STATE OF NEW JERSEY
BUSINESS REGISTRATION CERTIFICATE

Taxpayer Name: TAX REG TEST ACCOUNT

Trade Name:

Address: 847 ROEBLING AVE
TRENTON, NJ 08611

Certificate Number: 1093907

Date of Issuance: October 14, 2004

For Office Use Only:

20041014112823533

Not Applicable

RETURN PRIOR TO BID AWARD

N.J.S.A. 54:49-4.1: Violations of Registration Requirements; Penalties.

A business organization that fails to provide a copy of a business registration as required pursuant to section 1 of P.L.2001, c.134 (C.52:32-44 et al.) or subsection e. or f. of section 92 of P.L.1977, c.110 (C.5:12-92), or that provides false information of business registration under the requirements of either of those sections, shall be liable for a penalty of $25 for each day of violation, not to exceed $50,000 for each business registration copy not properly provided under a contract with a contracting agency.

All respondents are urged to submit with their response, a copy of their firm's New Jersey Business Registration Certificate. Failure to submit the Certificate to the ESCNJ prior to the award of contract will result in the rejection of the entire bid or proposal.

Not Applicable

CONTRACTOR/VENDOR REQUIREMENTS—OFFICE OF THE NEW JERSEY STATE COMPTROLLER

Contractors/vendors doing business with the ESCNJ are reminded of the following legal requirements pertaining to the Office of the New Jersey State Comptroller:

C. Access to Relevant Documents and Information—N.J.S.A. 52:15C-14 (d)

Private vendors or other persons contracting with or receiving funds from a unit in the Executive branch of State government, including an entity exercising executive branch authority, independent State authority, public institution of higher education, or unit of local government or board of education shall upon request by the State Comptroller provide the State Comptroller with prompt access to all relevant documents and information as a condition of the contract and

receipt of public monies. The State Comptroller shall not disclose any document or information to which access is provided that is confidential or proprietary. If the State Comptroller finds that any person receiving funds from a unit in the Executive branch of State government, including an entity exercising executive branch authority, independent State authority, public institution of higher education, or unit of local government or board of education refuses to provide information upon the request of the State Comptroller, or otherwise impedes or fails to cooperate with any audit or performance review, the State Comptroller may recommend to the contracting unit that the person be subject to termination of their contract, or temporarily or permanently debarred from contracting with the contracting unit.

D. Maintenance of Contract Records—N.J.A.C. 17:44-2.2

Relevant records of private vendors or other persons entering into contracts with covered entities are subject to audit or review by OSC pursuant to N.J.S.A. 52:15C-14(d).

The contractor/vendor to whom a contract has been awarded shall maintain all documentation related to products, transactions or services under this contract for a period of five years from the date of final payment. Such records shall be made available to the New Jersey Office of the State Comptroller upon request.

D. <u>Renewal of Contract; Services</u>

The ESCNJ may, at its discretion, request that a contract for services be renewed in full accordance with N.J.S.A. 18A:18A-42. The ESCNJ may negotiate terms for a renewal of contract proposal and present such negotiated proposal to the Board. All multi-year contracts and renewals are subject to the availability and appropriation annually of sufficient funds as may be needed to meet the extended obligation.

The ESCNJ is the final authority in awarding renewals of contracts.

Not Applicable

DEBARMENT, SUSPENSION, OR DISQUALIFICATION

The ESCNJ will not enter into a contract for work with any person, company or firm that is on the State Department of Labor and Workforce Development; Prevailing Wage Debarment List, or the State of New Jersey Consolidated Debarment Report (https://www.state.nj.us/treasury/revenue/debarment/index.shtml).

All bidders are required to submit a sworn statement indicating whether or not the bidder is, at the time of the bid, included on the State Department of Labor and Workforce Development; Prevailing Wage Debarment List or the State of New Jersey Consolidated Debarment Report, or the Federal Debarred Vendor List—Excluded Parties List System—System for Award Management—SAM.gov

PROHIBITED ACTIVITIES IN RUSSIA AND BELARUS & INVESTMENT ACTIVITIES IN IRAN N.J.S.A. (18A:18A-49.4)

The ESCNJ, pursuant to N.J.S.A. 18A:18A-49.4, shall implement and comply with Public Law 2012, c.25, Disclosure of Investment Activities in Iran and Public Law 2022, c.3, Prohibited Russia-Belarus Activities —N.J.S.A. 52:32-55 et seq.

Pursuant to N.J.S.A. 52:32-57, et seq. (P.L. 2012, c.25, P.L. 2021, c.4 and P.L. 2022, c.3), any person or entity that is a successful bidder or proposer, or otherwise proposes to enter into or renew a contract, for goods or services must complete the certification below prior to contract award to attest, under penalty of perjury, that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list or Chapter 25 list as a person or entity engaging in prohibited activities in Russia, Belarus or Iran. Before a contract for goods or services can be amended or extended, a person or entity must certify that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list. Both lists are found on Treasury's website at the following web addresses:
https://www.nj.gov/treasury/administration/pdf/RussiaBelarusEntityList.pdf
www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf . Bidders must review this list prior to completing the certification. If the Director of the Division of Purchase and Property finds a person or entity to be in violation of the law, s/he shall take action as may be appropriate and provided by law, rule or contract, including but not limited to, imposing sanctions, seeking compliance, recovering damages, declaring the party in default and seeking debarment or suspension of the party.

In addition, bidders must provide a detailed, accurate and precise description of the activities of the bidding person/entity, or one of its parents, subsidiaries or affiliates, engaging in Russia or Belarus and/or investment activities in Iran outlined above by completing the boxes on the lower portion of the enclosed form. The person or entity must cease engaging in any prohibited activities and provide an updated certification before the contract can be entered into. If a vendor or contractor is found to be in violation of law, action may be taken as appropriate and as may be provided by law, rule, or contract, including but not limited to imposing sanctions, seeking compliance, recovering damages, declaring the party in default, and seeking debarment or suspension of the party.

The ESCNJ has provided within these specifications, a Prohibited Russia-Belarus Activities & Iran Investment Activities certification form for all persons or entities, that plan to submit a bid, respond to a proposal, or renew a contract with the ESCNJ, to complete, sign and submit with the proposal. The Prohibited Russia-Belarus Activities & Iran Investment Activities Form is to be completed, certified and submitted prior to the award of contract, preferably with the bid submittal.
Please sign and submit the Disclosure of Investment Activities in Iran form and include with your bid package. This form must be submitted no later than the time of the award of a contact.

Not Applicable

PREVAILING WAGES

Where applicable, all vendors must adhere to NJ State Prevailing Wage laws; All subcontractors named in this bid understand the requirements of the subcontractor to pay prevailing wages in full accordance with the law, where applicable**.**

STATEMENT OF OWNERSHIP N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)

No business organization, regardless of form of ownership, shall be awarded any contract for the performance of any work or the furnishing of any goods and services, unless, prior to the receipt of the bid or accompanying the bid of said business organization, bidders shall submit a statement setting forth the names and addresses of all persons and entities that own ten percent or more of its stock or interest of any type at all levels of ownership.

The included Statement of Ownership shall be completed and attached to the bid proposal. This requirement applies to all forms of business organizations, including, but not limited to, corporations and partnerships, publicly-owned corporations, limited partnerships, limited liability corporations, limited liability partnerships, sole proprietorship, and Subchapter S corporations. **Failure to submit a disclosure document shall result in rejection of the bid as it cannot be remedied after bids have been opened.**

Not-for-profit entities should fill in their name, check the not-for-profit box, and certify the form. No other information is required.

Not Applicable

APPENDIX A RETURN WITH BID
AMERICANS WITH DISABILITIES ACT OF 1990
Equal Opportunity for Individuals with Disability

The contractor and the Educational Services Commission of New Jersey (hereafter "owner") do hereby agree that the provisions of Title 11 of the Americans with Disabilities Act of 1990 (the "Act") (42 U.S.C. S121 01 et seq.), which prohibits discrimination on the basis of disability by public entities in all services, programs, and activities provided or made available by public entities, and the rules and regulations promulgated pursuant there unto, are made a part of this contract. In providing any aid, benefit, or service on behalf of the owner pursuant to this contract, the contractor agrees that the performance shall be in strict compliance with the Act. In the event that the contractor, its agents, servants, employees, or subcontractors violate or are alleged to have violated the Act during the performance of this contract, the contractor shall defend the owner in any action or administrative proceeding commenced pursuant to this Act. The contractor shall indemnify, protect, and save harmless the owner, its agents, servants, and employees from and against any and all suits, claims, losses, demands, or damages, of whatever kind or nature arising out of or claimed to arise out of the alleged violation. The contractor shall, at its own expense, appear, defend, and pay any and all charges for legal services and any and all costs and other expenses arising from such action or administrative proceeding or incurred in connection therewith. In any and all complaints brought pursuant to the owner's grievance procedure, the contractor agrees to abide by any decision of the owner which is rendered pursuant to said grievance procedure. If any action or administrative proceeding results in an award of damages against the owner, or if the owner incurs any expense to cure a violation of the ADA which has been brought pursuant to its grievance procedure, the contractor shall satisfy and discharge the same at its own expense.

The owner shall, as soon as practicable after a claim has been made against it, give written notice thereof to the contractor along with full and complete particulars of the claim, If any action or administrative proceeding is brought against the owner or any of its agents, servants, and employees, the *owner shall* expeditiously forward or have forwarded to the contractor every demand, complaint, notice, summons, pleading, or other process received by the owner or its representatives.

It is expressly agreed and understood that any approval by the owner of the services provided by the contractor pursuant to this contract will not relieve the contractor of the obligation to comply with the Act and to defend, indemnify, protect, and save harmless the owner pursuant to this paragraph.

It is further agreed and understood that the owner assumes no obligation to indemnify or save harmless the contractor, its agents, servants, employees and subcontractors for any claim which may arise out of their performance of this Agreement. Furthermore, the contractor expressly understands and agrees that the provisions of this indemnification clause shall in no way limit the contractor's obligations assumed in this Agreement, nor shall they be construed to relieve the contractor from any liability, nor preclude the owner from taking any other actions available to it under any other provisions of the Agreement or otherwise at law.

Company _____ Name _____

Signature _____ Title _____

Not Applicable, Please see signed form above.

ASSURANCE OF COMPLIANCE – RETURN WITH BID

Contact with Students
There may be times during the performance of this contract, where a contracted service provider may come in contact with students of the school district. The district fully understands it obligation to provide to all students and staff members, a safe educational environment. To this end, the district is requiring all bidders to sign a statement of Assurance of Compliance, acknowledging the bidder's understanding of the below listed requirements and further acknowledging the bidder's assurance of compliance with those listed requirements.

Anti-Bullying Reporting--Requirement
When applicable, the contracted service provider shall comply with all applicable provisions of the New Jersey Anti-Bullying Bill of Rights Act—N.J.S.A. 18A:37-13.1 et seq., all applicable code and regulations, and the Anti-Bullying Policy of the Board of Education. In accordance with N.J.A.C. 6A:16-7.7 (c), a contracted service provider, who has witnessed, or has reliable information that a student has been subject to harassment, intimidation, or bullying shall immediately report the incident to any school administrator or safe schools resource officer, or the School Business Administrator/Board Secretary.

Criminal History Background Checks—N.J.S.A. 18A:6-7.1--Requirement
When applicable, the contracted service provider, shall provide to the school district prior to commencement of contract, evidence or proof that each employee assigned to provide services and that comes in **regular contact** with students, has had a criminal history background check, and furthermore, that said background check indicates that no criminal history record information exists on file for that worker. Failure to provide a proof of criminal history background check for any employee coming in regular contact with students, prior to commencement of contact, may be cause for breach of contract. See NJDOE Broadcast 9/9/19.

Pre-Employment Requirements
When applicable, all contracted service providers, whose employees have **regular contact with students**, shall comply with the Pre-Employment Requirements in accordance with New Jersey P.L. 2018 c.5, N.J.S.A. 18A:6-7.6 et seq. Contracted service providers are to review the following New Jersey Department of Education Office of Student Protection—Pre-Employment Resource P.L. 2018 c.5 link below for guidance and compliance procedures.

https://www.nj.gov/education/crimhist/preemployment/

Name of Company _____

Name of Authorized Representative _____
Signature _____ Date _____

Not Applicable, Please see signed form above.

RETURN WITH BID

Educational Services Commission of New Jersey
Business Office
1660 Stelton Road, Floor 2
Piscataway, New Jersey 08854

Chapter 271
Political Contribution Disclosure Form

(Contracts that Exceed $17,500.00)
Ref. N.J.S.A. 19:44A-20.26

The undersigned, being authorized and knowledgeable of the circumstances, does hereby certify that _____(Business Entity) has made the following **reportable** political contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26 during the twelve (12) months preceding this award of contract:

Reportable Contributions

Date of Contribution	Amount of Contribution	Name of Recipient Elected Official/ Committee/Candidate	Name of Contributor

The Business Entity may attach additional pages if needed.

_____

□ **No Reportable Contributions** (Please check (✔) if applicable.)

I certify that _____ (Business Entity) made no reportable contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26.

Certification

I certify that the information provided above is in full compliance with Public law 2005 – Chapter 271.

Name of Authorized Agent _____

Signature _____ Title _____

Business Entity _____

Not Applicable, Please see signed form above.

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

Contractor Instructions

Business entities (contractors) receiving contracts from a public agency that are NOT awarded pursuant to a "fair and open" process (defined at N.J.S.A. 19:44A-20.7) are subject to the provisions of P.L. 2005, c. 271, s. 2 (N.J.S.A. 19:44A-20.26). This law provides that 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

- any State, county, or municipal committee of a political party
- any legislative leadership committee*[2]
- any continuing political committee (a.k.a., political action committee)
- any candidate committee of a candidate for, or holder of, an elective office:
    - of the public entity awarding the contract
    - of that county in which that public entity is located
    - of another public entity within that county
    - or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county

The disclosure must list reportable contributions to any of the committees that exceed $300 per election cycle that were made during the 12 months prior to award of the contract. See N.J.S.A. 19:44A-8 and 19:44A-16 for more details on reportable contributions.

N.J.S.A. 19:44A-20.26 itemizes the parties from whom contributions must be disclosed when a business entity is not a natural person. This includes the following:

- individuals with an "interest" ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit
- all principals, partners, officers, or directors of the business entity or their spouses
- any subsidiaries directly or indirectly controlled by the business entity
- IRS Code Section 527 New Jersey based organizations, directly or indirectly controlled by the business entity and filing as continuing political committees, (PACs)

When the business entity is a natural person, "a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity." [N.J.S.A. 19:44A-20.26(b)]. The contributor must be listed on the disclosure.

Any business entity that fails to comply with the disclosure provisions shall be subject to a fine imposed by ELEC in an amount to be determined by the Commission which may be based upon the amount that the business entity failed to report.

The enclosed list of agencies is provided to assist the contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor's responsibility to identify the specific committees to which contributions may have been made and need to be disclosed. The disclosed information may exceed the minimum requirement.

The enclosed form, a content-consistent facsimile, or an electronic data file containing the required details (along with a signed over sheet) may be used as the contractor's submission and is disclosable to the public under the Open Public Records Act.

The contractor must also complete the attached Stockholder Disclosure Certification. This will assist the agency in meeting its obligations under the law. **NOTE: This section does not apply to Board of Education contracts.**

P.L. 2005, c. 271

[2] N.J.S.A. 19:44A-3(s): "The term "legislative leadership committee" means a committee established, authorized to be established, or designated by the President of the Senate, the Minority Leader of the Senate, the Speaker of the General Assembly or the Minority Leader of the General Assembly pursuant to section 16 of P.L. 1993, c. 65 (C. 19:44A-10.1) for the purpose of receiving contributions and making expenditures."

Not Applicable

AN ACT authorizing units of local government to impose limits on political contributions by contractors and supplementing Title 40A of the New Jersey Statutes and Title 19 of the Revised Statutes.

BE IT ENACTED by the Senate and General Assembly of the State of New Jersey:

40A:11-51 1. a. A county, municipality, independent authority, board of education, or fire district is hereby authorized to establish by ordinance, resolution or regulation, as may be appropriate, measures limiting the awarding of public contracts there from to business entities that have made a contribution pursuant to P.L. 1973, c. 83 (C. 19:44A-1 et seq.) and limiting the contributions that the holders of a contract can make during the term of a contract, notwithstanding the provisions and parameters of sections 1 through 12 of P.L. 2004, c. 19 (C. 19:44A-20.2 et al.) and section 22 of P.L. 1973, c. 83 (C. 19:44A-22).

b. The provisions of P.L. 2004, c. 19 shall not be construed to supersede or preempt any ordinance, resolution or regulation of a unit of local government that limits political contributions by business entities performing or seeking to perform government contracts. Any ordinance, resolution or regulation in effect on the effective date of P.L. 2004, c. 19 shall remain in effect and those adopted after that effective date shall be valid and enforceable.

c. An ordinance, resolution or regulation adopted or promulgated as provided in this section shall be filed with the Secretary of State.

19:44A-20.26 2. a. Not later than 10 days prior to entering into any contract having an anticipated value in excess of $17,500, except for a contract that is required by law to be publicly advertised for bids, a State agency, county, municipality, independent authority, board of education, or fire district shall require any business entity bidding thereon or negotiating therefor, to submit along with its bid or price quote, a list of political contributions as set forth in this subsection that are reportable by the recipient pursuant to the provisions of P.L. 1973, c. 83 (C.19:44A-1 et seq.) and that were made by the business entity during the preceding 12 month period, along with the date and amount of each contribution and the name of the recipient of each contribution. A business entity contracting with a State agency shall disclose contributions to any State, county, or municipal committee of a political party, legislative leadership committee, candidate committee of a candidate for, or holder of, a State elective office, or any continuing political committee. A business entity contracting with a county, municipality, independent authority, other than an independent authority that is a State agency, board of education, or fire district shall disclose contributions to: any State, county, or municipal committee of a political party; any legislative leadership committee; or any candidate committee of a candidate for, or holder of, and elective office of that public entity, of that county in which that public entity is located, of another public entity within that county, or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county, or any continuing political committee.

The provisions of this section shall not apply to a contract when a public emergency requires the immediate delivery of goods or services.

b. When a business entity is a natural person, a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by any person or other business entity having an interest therein shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by: all principals, partners, officers, or directors of the business entity or their spouses; any subsidiaries directly or indirectly controlled by the business entity; or any political organization organized under section 527 of the Internal Revenue Code that is directly or indirectly controlled by the business entity, other than a candidate committee, election fund, or political party committee, shall be deemed to be a contribution by the business entity.

c. As used in this section:
"business entity" means a natural or legal person, business corporation, professional services corporation, limited liability company, partnership, limited partnership, business trust, association or any other legal commercial entity organized under the laws of this State or of any other state or foreign jurisdiction;

"interest" means the ownership or control of more than 10% of the profits or assets of a business entity of 10% of the stock in the case of a business entity that is a corporation for profit, as appropriate; and

P.L. 2005, c. 271

"State agency" means any of the principal departments in the Executive Branch of the State Government, and any division, board, bureau, office, commission or other instrumentality within or created by such department, the Legislature of the State and any

Not Applicable

office, board, bureau or commission within or created by the Legislative Branch, and any independent State authority, commission, instrumentality or agency.

d. Any business entity that fails to comply with the provisions of this section shall be subject to a fine imposed by the New Jersey Election Law Enforcement Commission in an amount to be determined by the commission which may be based upon the amount that the business entity failed to report.

19:44A-20.13 3. a. Any business entity making a contribution of money or any other thing of value, including an in-kind contribution, or pledge to make a contribution of any kind to a candidate for or the holder of any public office having ultimate responsibility for the awarding of public contracts, or to a political party committee, legislative leadership committee, political committee or continuing political committee, which has received in any calendar year $50,000 or more in the aggregate through agreements or contracts with a public entity, shall file an annual disclosure statement with the New Jersey Election Law Enforcement Commission, established pursuant to section 5 of P.L. 1973, c. 83 (C. 19:44A-5), setting forth all such contributions made by the business entity during the 12 months prior to the reporting deadline.

b. The commission shall prescribe forms and procedures for the reporting required in subsection a. of this section which shall include,
but not be limited to:

(3) the name and mailing address of the business entity making the contribution, and the amount contributed during the 12 months prior to the reporting deadline;

(4) the name of the candidate for or the holder of any public office having ultimate responsibility for the awarding of public contracts, candidate committee, joint candidates committee, political party committee, legislative leadership committee, political committee or continuing political committee receiving the contribution; and

(4) the amount of money the business entity received from the public entity through contract or agreement, the dates, and information identifying each contract or agreement and describing the goods, services or equipment provided or property sold.

c. The commission shall maintain a list of such reports for public inspection both at its office and through its Internet site.

d. When a business entity is a natural person, a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by any person or other business entity having an interest therein shall be deemed to be a contribution by the business entity. When a business entity is other than a natural person, a contribution by: all principals, partners, officers, or directors of the business entity, or their spouses; any subsidiaries directly or indirectly controlled by the business entity; or any political organization organized under section 527 of the Internal Revenue Code that is directly or indirectly controlled by the business entity, other than a candidate committee, election fund, or political party committee, shall be deemed to be a contribution by the business entity.

As used in this section:

"Business entity" means a natural or legal person, business corporation, professional services corporation, limited liability company, partnership, limited partnership, business trust, association or any other legal commercial entity organized under the laws of this State or of any other state or foreign jurisdiction; and

"Interest" means the ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit, as appropriate.

e. Any business entity that fails to comply with the provisions of this section shall be subject to a fine imposed by the New Jersey Election Law Enforcement Commission in an amount to be determined by the commission which may be based upon the amount that the business entity failed to report.

4. This act shall take effect immediately.

*Note: Bold italicized statutory references of new sections are anticipated and not final as of the time this document was prepared. Statutory compilations of N.J.S.A. 18A:18A-51 is anticipated to show a reference to N.J.S.A. 40:11-51 and to N.J.S.A. 19:44A-20.26.

Not Applicable

Prohibited Russia-Belarus Activities & Iran Investment Activities

Person or Entity	

Part 1: Certification

COMPLETE PART 1 BY CHECKING **ONE OF THE THREE BOXES BELOW**

Pursuant to law, any person or entity that is a successful bidder or proposer, or otherwise proposes to enter into or renew a contract, for goods or services must complete the certification below prior to contract award to attest, under penalty of perjury, that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list or Chapter 25 list as a person or entity engaging in prohibited activities in Russia, Belarus or Iran. Before a contract for goods or services can be amended or extended, a person or entity must certify that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list. Both lists are found on Treasury's website at the following web addresses:

https://www.nj.gov/treasury/administration/pdf/RussiaBelarusEntityList.pdf
www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf.

As applicable to the type of contract, the above-referenced lists must be reviewed prior to completing the below certification.

A person or entity unable to make the certification must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran. The person or entity must cease engaging in any prohibited activities and provide an updated certification before the contract can be entered into.

If a vendor or contractor is found to be in violation of law, action may be taken as appropriate and as may be provided by law, rule, or contract, including but not limited to imposing sanctions, seeking compliance, recovering damages, declaring the party in default, and seeking debarment or suspension of the party.

CONTRACT AWARDS AND RENEWALS

Not Applicable

☐	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate appears on the N.J. Department of Treasury's lists of entities engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3 or in investment activities in Iran pursuant to P.L. 2012, c. 25 ("Chapter 25 List"). I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf.* (Skip Part 2 and sign and complete the Certification below.)
CONTRACT AMENDMENTS AND EXTENSIONS	
☐	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate is listed on the N.J. Department of the Treasury's lists of entities determined to be engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3. I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf.* (Skip Part 2 and sign and complete the Certification below.)
IF UNABLE TO CERTIFY	
☐	*I am unable to certify as above because the person or entity and/or a parent entity, subsidiary, or affiliate is listed on the Department's Russia-Belarus list and/or Chapter 25 Iran list. I will provide a detailed, accurate, and precise description of the activities as directed in Part 2 below, and sign and complete the Certification below. Failure to provide such will prevent the award of the contract to the person or entity, and appropriate penalties, fines, and/or sanctions will be assessed as provided by law.*

Part 2: Additional Information

PLEASE PROVIDE FURTHER INFORMATION RELATED TO PROHIBITED ACTIVITIES IN RUSSIA OR BELARUS AND/OR INVESTMENT ACTIVITIES IN IRAN.

You must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran in the space below and, if needed, on additional sheets provided by you.

Not Applicable

Part 3: Certification of True and Complete Information

I, being duly sworn upon my oath, hereby represent and state that the foregoing information and any attachments there, to the best of my knowledge, are true and complete. I attest that I am authorized to execute this certification on behalf of the above-referenced person or entity.

*I acknowledge that the <**Name of Contracting Unit**> is relying on the information contained herein and hereby acknowledge that I am under a continuing obligation from the date of this certification through the completion of any contracts with the <**Name of Contracting Unit**> to notify the <**Name of Contracting Unit**> in writing of any changes to the answers of information contained herein.*

*I acknowledge that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I recognize that I am subject to criminal prosecution under the law and that it will also constitute a material breach of my agreement(s) with the <**Name of Contracting Unit**> and that the <**Name of Contracting Unit**> at its option may declare any contract(s) resulting from this certification void and unenforceable.*

Full Name (Print)		**Title**	
Signature		**Date**	

Not Applicable

Statement of Suspension or Debarment - RETURN WITH BID

Not Applicable

STATE OF NEW JERSEY/ _____
Specify, of other

COUNTY OF _____

I, _____ of the (City, Town, Borough)

of _____ State of _____ of full age,

being duly sworn according to law on my oath depose and say that:

I am _____ of the firm

of _____ the Bidder

making the Proposal for the above named projects, and that I executed the said Proposal with full authority to do so; that said Bidder is not at the time of the making this bid included on the New Jersey State Treasurer's or the Federal Government's List of Debarred, Suspended or Disqualified Bidders or the State Department of Labor and Workforce Development; Prevailing Wage Debarment List as a result of action taken by any State or Federal Agency.

Name of Contractor: _____
(Company Name)

By: _____
(Signature of authorized representative)

Subscribed and sworn to before me

This_____ day of _____, 20 ____

_____
(Seal) Notary Public of New Jersey/
Specify Other State

My Commission expires_____ 20 ___

Not Applicable, Please see signed form above.

STATEMENT OF OWNERSHIP DISCLOSURE - RETURN WITH BID

N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

Name of Organization: _____
Organization Address: _____
City, State, ZIP: _____

Part I Check the box that represents the type of business organization:

Sole Proprietorship (skip Parts II and III, execute certification in Part IV)

Non-Profit Corporation (skip Parts II and III, execute certification in Part IV)

For-Profit Corporation (any type) Limited Liability Company (LLC)

Partnership Limited Partnership Limited Liability Partnership (LLP)

Other (be specific): _____

Part II Check the appropriate box

The list below contains the names and addresses of all stockholders in the corporation who own 10 percent or more of its stock, of any class, or of all individual partners in the partnership who own a 10 percent or greater interest therein, or of all members in the limited liability company who own a 10 percent or greater interest therein, as the case may be. (**COMPLETE THE LIST BELOW IN THIS SECTION**)

OR

No one stockholder in the corporation owns 10 percent or more of its stock, of any class, or no individual partner in the partnership owns a 10 percent or greater interest therein, or no member in the limited liability company owns a 10 percent or greater interest therein, as the case may be. (**SKIP TO PART IV**)

(Please attach additional sheets if more space is needed):

Name of Individual or Business Entity	Home Address (for Individuals) or Business Address

Not Applicable, Please see signed form above.

Part III DISCLOSURE OF 10% OR GREATER OWNERSHIP IN THE STOCKHOLDERS, PARTNERS OR LLC MEMBERS LISTED IN PART II

If a bidder has a direct or indirect parent entity which is publicly traded, and any person holds a 10 percent or greater beneficial interest in the publicly traded parent entity as of the last annual federal Security and Exchange Commission (SEC) or foreign equivalent filing, ownership disclosure can be met by providing links to the website(s) containing the last annual filing(s) with the federal Securities and Exchange Commission (or foreign equivalent) that contain the name and address of each person holding a 10% or greater beneficial interest in the publicly traded parent entity, along with the relevant page numbers of the filing(s) that contain the information on each such person. **Attach additional sheets if more space is needed**.

Website (URL) containing the last annual SEC (or foreign equivalent) filing	Page #'s

Please list the names and addresses of each stockholder, partner or member owning a 10 percent or greater interest in any corresponding corporation, partnership and/or limited liability company (LLC) listed in Part II **other than for any publicly traded parent entities referenced above**. The disclosure shall be continued until names and addresses of every non-corporate stockholder, and individual partner, and member exceeding the 10 percent ownership criteria established pursuant to N.J.S.A. 52:25-24.2 has been listed. **Attach additional sheets if more space is needed.**

Stockholder/Partner/Member and Corresponding Entity Listed in Part II	Home Address (for Individuals) or Business Address

STATEMENT OF OWNERSHIP DISCLOSURE – continued - RETURN WITH BID

N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)

Part IV Certification

I, being duly sworn upon my oath, hereby represent that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I acknowledge: that I am authorized to execute this certification on behalf of the bidder/proposer; that the ***ESCNJ and/or its members*** is relying on the information contained herein and that I am under a continuing obligation from the date of this certification through the completion of any contracts with the ***ESCNJ and/or its members*** to notify the ***ESCNJ and/or its members*** in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the, permitting the ***ESCNJ and/or its members*** to declare any contract(s) resulting from this certification void and unenforceable.

Full Name (Print):		Title:	
Signature:		Date:	

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

Not Applicable, Please see signed form above.

CERTIFICATE OF AUTHORITY - RETURN WITH BID

All bidders are to submit their Sworn Contractor Certification, a current valid "Certificate of Authority" as issued by the New Jersey Department of Treasury. Reference—N.J.S.A. 18A:7G-37.

Sample Certificate of Authority



STATE OF NEW JERSEY
Certificate of Authority

DIVISION OF TAXATION
TRENTON, N J 08695

The person, partnership or corporation named below is hereby authorized to collect
NEW JERSEY SALES & USE TAX

pursuant to N.J.S.A. [redacted]

This authorization is good ONLY for the named person at the location specified herein
This authorization is null and void if any change of ownership or address is effected

Acting Director, Division of Taxation

[redacted]

Tax Registration No. [redacted]
Tax Effective Date 10-15-10
Document Locator No. [redacted]
Date Issued 10-14-10

This Certificate is NOT assignable or transferable. It must be conspicuously displayed at above address.

CHANGE ORDERS (N.J.A.C. 6A:26-4.9, 4.10 et seq.) (N.J.A.C. 5:30-11.1 et seq.)

Co-op member Approval Required; Prior to Issuance of Change Order (N.J.A.C. 5:30-11.2)

Change orders may be approved by the Co-op member in an amount up to twenty percent (20%) when necessitated by one of the following:

- Emergencies consistent with N.J.S.A. 18A:18A-7;
- Unforeseeable physical conditions; or
- Minor modifications to the project/scope that achieve cost savings, improve service or resolve construction conditions.

Division of Finance (NJDOE) Approval

All other change orders shall be approved by the Division of Finance (NJDOE) when extraordinary circumstances exist such as:

- Change order amounts greater than twenty percent (20%);
- Change orders that eliminate or affect the project scope; or
- Change orders that affect the number, size, configuration, location or use of co-op member spaces.

All contractors are prohibited to perform any change order unless so directed in writing by the Co-op member.

Not Applicable

CONTRACTOR TRADE LICENSES - RETURN WITH BID

All bidders are to submit with their proposal all current, valid contractor or trade licenses as issued by the New Jersey Division of Consumer Affairs, for any trade or specialty area the contractor seeks to perform work for this particular proposal.

Sample Contractor Trade License


THIS DOCUMENT IS PRINTED ON WATERMARKED PAPER, WITH A MULTI-COLORED BACKGROUND AND MULTIPLE SECURITY FEATURES. PLEASE VERIFY AUTHENTICITY.

NOT AN ELECTRICIAN'S OR PLUMBER'S LICENSE

State Of New Jersey
New Jersey Office of the Attorney General
Division of Consumer Affairs

THIS IS TO CERTIFY THAT THE
Division of Consumer Affairs

HAS REGISTERED

ABC CONSTRUCTION
123 YOUR BLOCK
ANYTOWN USA

FOR PRACTICE IN NEW JERSEY AS A(N): Home Improvement Contractor

11/01/2013 TO 12/31/2014
VALID

1234567890123
LICENSE/REGISTRATION/CERTIFICATION #

Signature of Licensee/Registrant/Certificate Holder

DIRECTOR

CONTRACTOR'S REGISTRATION EVIDENCE —"Public Works Contractor Registration Act"

A. Valid Certificate – Receipt of Bid

All Contractors must adhere to the provisions of the Public Works Contractor Registration Act - N.J.S.A. 34:11-56.48 et. seq. The PWCRA requires that *"No contractor shall bid on any contract for public work as defined in N.J.S.A.34:11-56.26 unless the contractor is registered pursuant to this act."* The law requires that all contractors and sub-contractors named in the proposal possess a valid certificate at the time the proposal is received by the contracting unit, in this case the ESCNJ.

B. Submission of Certificate – Receipt of Bid; Prior to Award--Mandatory

All bidders are requested to submit with the bid package or prior to the award of contract, a current Public Works Contractor Registration Certificate that was issued prior to the receipt of the bid.

The vendor(s) who is deemed to receive the contract award must submit a copy of the current New Jersey Department of Labor and Workforce Development Public Works Contractor Registration Certificate, and if applicable, copies of certifications of all listed subcontractors, prior to the award of contract. **If the successful vendor fails to provide copies of certificates prior to the award of contract, the bid shall be rejected as non-responsive.**

Not Applicable

For more information contact:

Contractor Registration Unit
Division of Wage and Hour Compliance
New Jersey Department of Labor & Workforce Development
PO Box 389
Trenton, New Jersey 08625-0389
Tel: 609-292-9464
Fax: 609-633-8591
E-mail: wage.hour@dol.nj.gov
Web site: lwd.dol.state.nj.us/labor/wagehour/content/contact_us.html

PRE-QUALIFICATION OF BIDDERS

A. **DPMC Prequalification--** Pursuant to N.J.S.A. 18A:18A-26, 27 et seq., all Bidders on any contract for public works which the entire cost of the contract exceeds $20,000, must be pre-qualified by the Department of Treasury, Division of Property Management and Construction, as to charter and amount of public work on which they may submit bids. No person shall be qualified to bid on any public work contract with the Commission if he has not submitted a statement to the Department of Treasury, Division of Property Management and Construction which fully develops the financial ability, adequacy of plant and equipment, organization and prior experience of the prospective bidder, and such other pertinent and material facts, within a period of one year preceding the date of opening of the bids for such contract.

NJSDA Prequalification---Pursuant to N.J.S.A. 18A:7G-33, all contractors bidding on any contract for a School Facilities Project as defined in N.J.A.C. 6A:26-1.2, shall be prequalified with the New Jersey School Development Authority in the major construction trades listed in N.J.S.A. 18A:7G-33. Bidders will have to submit a Sworn Contractor Certification attesting to the NJSDA prequalification. Named subcontractors shall also be pre-qualified with the NJSDA—N.J.A.C. 6A:26-4.7 (b) (3).

Maintenance Projects—Contractors are reminded that maintenance projects solely to achieve the design life of a school facility and routine maintenance do not constitute a school facility project and therefor NJSDA prequalification is not a requirement. Reference N.J.A.C. 6A:26-1.2002E

B. **Prequalification Affidavit--No Material Adverse Change**

Every pre-qualified Bidder must submit with his proposal, a notarized affidavit setting forth the type of work and the amount of work for which he has been qualified, that there has been no material adverse change in his qualification information, the total amount of completed work on contracts at the time and date of the classification. **Any bid not including a copy of this affidavit shall be rejected as being non-responsive to bid requirements.** (N.J.S.A. 18A:18A-32)

Not Applicable

C. Bidders shall furnish satisfactory evidence that he and his subcontractors have sufficient means and experience in the type of work to complete the project in accordance with the bid specifications. A subcontractor listing and bidder's personnel and experience sheet shall be submitted to the ESCNJ as part of the bidding documents. Where the Bidder intends to subcontract any portion of the project, the cost of which will exceed $20,000.00, the sub-contractor shall be pre-qualified to perform the work and the bidder shall submit the requisite documentation pertaining to the sub-contractor in accordance with Paragraphs A and B above. The ESCNJ may make such additional investigations as it deems necessary to determine the ability, competence and financial responsibility of the bidder to perform their work. The bidder shall furnish the ESCNJ with the information and data for this purpose upon request. The ESCNJ reserves the right to reject any bid if the information fails to establish to the ESCNJ's satisfaction that the bidder is properly qualified to carry out the obligations of the contract and to complete the work contemplated here.

D. **Notice of Classification--**(For Contracts Exceeding $20,000) N.J.S.A. 18A:18A-26 et seq., N.J.S.A. 52:35-1 et seq.
Each Bidder shall submit with his/her bid a copy of a valid and active Notice of Classification letter issued by the Department of Treasury, Division of Property Management and Construction as appropriate to the nature of the bid. **Any bid submitted to the ESCNJ under the terms of New Jersey Statutes not including a copy of a valid and active classification letter shall be rejected as being non-responsive to bid requirements.**

"The Co-op member, through its authorized agent, shall upon completion of the contract report to the State agency listed on the pre-qualification/classification letter as to the contractor's performance and shall furnish such report from time to time during performance if the contractor is then in default".

E. **Uncompleted Contracts--**(For Contracts Exceeding $20,000) - N.J.A.C. 17:19-2.13(a)
The ESCNJ also requires that each bidder submit with his bid a certified Total Amount of Uncompleted Contracts form as prescribed by code. (Form DPMC 701). **Failure to submit this document will result in the rejection of the bid as being non-responsive.**

PREVAILING WAGES: CONSTRUCTION, ALTERATIONS, REPAIRS
The State of New Jersey Prevailing Wage Act, Chapter 150 Laws of 1963 with applicable wage rates by County as published by the Department of Labor and Workforce Development in conformance with N.J.S.A. 34:11-56:25, is hereby made a part of these Contract Documents. Copies of these wage rates may be obtained from the State Department of Labor and Workforce Development, and/or viewed athttps://www.state.nj.us/labor/wagehour/wagerate/prevailing_wage_determinations.html
http://lwd.dol.state.nj.us/http://lwd.dol.state.nj.us/, the Prevailing Wages Determination Section.

Not Applicable

- **Compliance with New Jersey Prevailing Wage Act**

Every contractor and subcontractor performing services in connection with this project, shall pay all workers a wage rate not less than the published prevailing wage rates, for the locality the work is being performed, as designated by the New Jersey Department of Labor and Workforce Development.

- **Certified Payrolls**

Contractor agrees to submit to the Co-op member a certified payroll for each payroll period within ten (10) days of the payment of wages. Contractor further agrees that no payments will be made to the Contractor if certified payrolls are not received. It is the Contractor's responsibility to insure timely receipt by the district of certified payrolls.

- **Submission of Affidavit**

Before final payment, the contractor shall furnish the co-op member with an affidavit stating that all workers have been paid the prevailing rate of wages in accordance with State of New Jersey requirements. The contractor shall keep an accurate record showing the name, craft, or trade and actual hourly rate of wages paid to each workman employed by him in connection with this work. Upon request, the Contractor(s) and each Subcontractor shall file written statements certifying to the amounts then due and owing to any and all workmen for wages due on account of the work. The statements shall be verified by the oaths of the Contractor or Subcontractor, as the case may be.

- **Posting of Prevailing Wages**

The contractor shall post the prevailing wage rates for each craft and classification involved in the work, including the effective date of any changes thereof, in prominent and easily accessible places at the site of the work and in such place or places as used to pay workers their wages. (Reference 18A:7G-23 and N.J.S.A 34:11-56.32.)

- **Prevailing Wages Certification—Submission with Bid**

The bidder shall submit a Prevailing Wages Certification with its bid package.

- **Non-compliance Statement**

If it is found that any worker, employed by the contractor or any subcontractor covered by said contract, has been paid a rate of wages less than the prevailing wage required to be paid by such contract, the ESCNJ or co-op member may begin proceedings to terminate the contractor's or subcontractor's right to proceed with the work, or such part of the work as to which there has been a failure to pay required wages and to prosecute the work to completion or otherwise. The contractor and his sureties shall be liable for any excess costs occasioned thereby to the public body.

Not Applicable

EQUIPMENT CERTIFICATION (N.J.S.A. 18A:18A-23)

Each Bidder shall provide a certification showing that he/she owns, leases or controls all the necessary equipment required by the specifications. If the Bidder is not the actual owner or lessee of any such equipment, he/she shall submit a certificate stating the source from which the equipment will be obtained and shall obtain a certificate from the owner and person in control of the equipment, definitely granting to the bidder the control of the equipment required during such time as may be necessary for the completion of that portion of the contract for which it is necessary.

The certificates are to be submitted with the bid. If the contract involves the installation of a manufactured system which requires the contractor to have special knowledge or training, or to be specifically certified by the manufacturer to install their system, this form is used to submit such required evidence of the bidder's approval from the manufacturer.

SUBCONTRACTING: ASSIGNMENT OF CONTRACT - RETURN WITH BID

Contractors, services providers, and all vendors with whom the ESCNJ has an executed contract, may not subcontract any part of any work done or assign any part of the contract for goods or materials for ESCNJ and Co-op members without first receiving written permission from the ESCNJ. Awarded vendors may add additional subcontractors after submitting the proper paperwork and upon approval from the ESCNJ. Under no condition will any work specified be subcontracted without the ESCNJ's prior written approval. **Failure to adhere to this requirement may result in revocation of a contract.**

Contractors, service providers, and vendors using subcontractors assume all responsibility for work performed by subcontractors. The ESCNJ must approve all subcontractors and will require the following documents to be secured from all approved subcontractors:

-Affirmative Action Evidence – Construction type contracts
-Americans with Disabilities Act of 1990
-Assurance of Compliance
-Certificate of Authority
-Certifications and Licenses as applicable
-Contractor's Registration Certificate (Public Works)
-Disclosure of Investment Activities in Iran
-Equipment Certification
-Insurance Certificate as outlined in the bid specifications;
-New Jersey Business Registration Certificate
-New Jersey School Development Authority Prequalification
-Notice of Classification Form (DPMC)
-Political Contribution Disclosure Form
- Prequalification Affidavit--No Material Adverse Change
-Prevailing Wages Compliance Certification
-Statement of Ownership (Ownership Disclosure Certification)
-Statement of Suspension or Debarment
-Subcontracting Assignments
-Sworn Contractor's Disclosure
-Total Amount of Uncompleted Contractor's Form—Certified (Form DPMC 701)
-Written certification that the subcontractor shall adhere to prevailing wages as provided through New Jersey State Law.

Not Applicable

SUBCONTRACTING: ASSIGNMENT OF CONTRACT-continued

In cases of subcontracting, the Co-op member shall only pay the prime contractor. It is the sole responsibility of the prime contractor to ensure that all subcontractors are paid. The Co-op member shall not be responsible for payments to subcontractors and shall be held harmless against any or all claims generated against prime contractors for nonpayment to subcontractors. Transportation carriers hired by the vendor to deliver goods and materials are not considered to be subcontractors. All vendors are responsible for submitting subcontractor documentation.

Penalties – Unauthorized Subcontractors

The Co-op member may deduct the amount of $1,000.00 (one thousand dollars) per day as a penalty, for each day a prime contractor uses a subcontractor without first receiving **written** permission as required.

Subcontractor Disclosure Statement

If the bidder intends to subcontract any work, please submit the completed **Subcontractor Disclosure Statement found in this bid document.**

SWORN CONTRACTOR CERTIFICATION – (Bidder's Certification)

Pursuant to N.J.S.A. 18A:7G-37, a pre-qualified contractor seeking to bid school facilities projects, and any subcontractors, that are required to be named under N.J.S.A. 18A:7G-1 et seq. shall, as a condition of bidding, submit this Sworn Contractor Certification regarding qualifications and credentials. **Failure to complete, sign and submit the certification may lead to the bid being rejected.**

Not Applicable

AFFIRMATIVE ACTION—Construction Contracts—Acknowledgement – RETURN WITH BID

The undersigned acknowledges and agrees to comply with the following:

AFFIRMATIVE ACTION—EQUAL EMPLOYMENT OPPORTUNITY IN PUBLIC CONTRACTS—EEO

The construction contractor shall complete and submit an Initial Project Workforce Report, **Form AA-201** listing their entire work force and all employees that may be used for any jobs under this ESCNJ Co-op contract with their bid submission. Proper completion and submission of this Report shall constitute evidence of the contractor's compliance with the regulations. Failure to submit this form may result in the contract being terminated. The awarded contractor(s) shall also complete and submit an Initial Project Workforce Report, **Form AA-201** to the owner before the start of any job entered into under this contract. The contractor also agrees to submit a copy of the Monthly Project Workforce Report, Form AA-202 once a month thereafter for the duration of the contract to the Department of Labor Workforce and Development and to the owner's Public Agency Compliance Officer.

All bidders should familiarize themselves with N.J.S.A. 10:5-31 et seq. and N.J.A.C. 17:27-1.1 et seq. MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE—EXHIBIT B. If awarded a contract, your company/firm will be required to comply with the above requirements.

Contractors and vendors are to familiarize themselves with the following document:

Vendor/Contractor Guidelines for Awarded Public Contracts

The document may be obtained from the New Jersey Division of Purchase and Property, Contract Compliance and Audit Unit, Equal Employment Opportunity (EEO) Program website or by visiting the following link:

https://www.nj.gov/treasury/contract_compliance/https://www.state.nj.us/treasury/contract_compliance/pdf/vc.pdf

Name of Company _____

Address _____ P.O. Box _____

City, State, Zip Code _____

Name of Authorized Representative _____

Signature _____ Date _____

Not Applicable

EXHIBIT B - RETURN WITH BID
MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE
N.J.S.A. 10:5-31 et seq. (P.L.1975, c.127)
N.J.A.C. 17:27-1.1 et seq.
CONSTRUCTION CONTRACTS

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Except with respect to affectional or sexual orientation and gender identity or expression, the contractor will ensure that equal employment opportunity is afforded to such applicants in recruitment and employment, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Such equal employment opportunity shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this nondiscrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex.

The contractor or subcontractor will send to each labor union, with which it has a collective bargaining agreement, a notice, to be provided by the agency contracting officer, advising the labor union or workers' representative of the contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer, pursuant to N.J.S.A. 10:5-31et seq., as amended and supplemented from time to time and the Americans with Disabilities Act.

When hiring or scheduling workers in each construction trade, the contractor or subcontractor agrees to make good faith efforts to employ minority and women workers in each construction trade consistent with the targeted employment goal prescribed by N.J.A.C. I7:27-7.2; provided, however, that the Dept. of LWD, Construction EEO Monitoring Program, may, in its discretion, exempt a contractor or subcontractor from compliance with the good faith procedures prescribed by the following provisions, A, B, and C, as long as the Dept. of LWD, Construction EEO Monitoring Program is satisfied that the contractor or subcontractor is employing workers provided by a union which provides evidence, in accordance with standards prescribed by the Dept. of LWD, Construction EEO Monitoring Program, that its percentage of active "card carrying" members who are minority and women workers is equal to or greater than the targeted employment goal established in accordance with N.J.A.C. 17:27-7.2. The contractor or subcontractor agrees that a good faith effort shall include compliance with the following procedures:

(A) If the contractor or subcontractor has a referral agreement or arrangement with a union for a construction trade, the contractor or subcontractor shall, within three business days of the contract award, seek assurances from the union that it will cooperate with the contractor or subcontractor as it fulfills its affirmative action obligations under this contract and in accordance with the rules promulgated by the Treasurer pursuant to N.J.S.A. 10:5-31 et. seq., as supplemented and amended from time to time and the Americans with Disabilities Act. If the contractor or subcontractor is unable to obtain said assurances from the construction trade union at least five business days prior to the commencement of construction work, the contractor or subcontractor agrees to afford equal employment opportunities minority and women workers directly, consistent with this chapter. If the contractor's or subcontractor's prior experience with a construction trade union, regardless of whether the union has provided said assurances, indicates a significant possibility that the trade union will not refer sufficient minority and women workers consistent with affording equal employment opportunities as specified in this chapter, the contractor or subcontractor agrees to be prepared to provide such opportunities to minority and women workers directly, consistent with this chapter, by complying with the hiring or scheduling procedures prescribed under (B) below; and the contractor or subcontractor further agrees to take said action immediately if it determines that the union is not referring minority and women workers consistent with the equal employment opportunity goals set forth in this chapter.

Not Applicable

(B) EXHIBIT B - RETURN WITH BID
(C) MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE
(D) N.J.S.A. 10:5-31 et seq. (P.L.1975, c.127)
(E) N.J.A.C. 17:27-1.1 et seq.
(F) CONSTRUCTION CONTRACTS-continued

(B) If good faith efforts to meet targeted employment goals have not or cannot be met for each construction trade by adhering to the procedures of (A) above, or if the contractor does not have a referral agreement or arrangement with a union for a construction trade, the contractor or subcontractor agrees to take the following actions:

(1) To notify the public agency compliance officer, the Dept. of LWD, Construction EEO Monitoring Program, and minority and women referral organizations listed by the Division pursuant to N.J.A.C. 17:27-5.3, of its workforce needs, and request referral of minority and women workers;

(2) To notify any minority and women workers who have been listed with it as awaiting available vacancies;
EXHIBIT B (Continued)

(3) Prior to commencement of work, to request that the local construction trade union refer minority and women workers to fill job openings, provided the contractor or subcontractor has a referral agreement or arrangement with a union for the construction trade;

(4) To leave standing requests for additional referral to minority and women workers with the local construction trade union, provided the contractor or subcontractor has a referral agreement or arrangement with a union for the construction trade, the State Training and Employment Service and other approved referral sources in the area;

(5) If it is necessary to lay off some of the workers in a given trade on the construction site, layoffs shall be conducted in compliance with the equal employment opportunity and nondiscrimination standards set forth in this regulation, as well as with applicable Federal and State court decisions;

(6) To adhere to the following procedure when minority and women workers apply or are referred to the contractor or subcontractor:

(i) The contactor or subcontractor shall interview the referred minority or women worker.

(ii) If said individuals have never previously received any document or certification signifying a level of qualification lower than that required in order to perform the work of the construction trade, the contractor or subcontractor shall in good faith determine the qualifications of such individuals. The contractor or subcontractor shall hire or schedule those individuals who satisfy appropriate qualification standards in conformity with the equal employment opportunity and non-discrimination principles set forth in this chapter. However, a contractor or subcontractor shall determine that the individual at least possesses the requisite skills, and experience recognized by a union, apprentice program or a referral agency, provided the referral agency is acceptable to the Dept. of LWD, Construction EEO Monitoring Program. If necessary, the contractor or subcontractor shall hire or schedule minority and women workers who qualify as trainees pursuant to these rules. All of the requirements, however, are limited by the provisions of (C) below.

(iii) The name of any interested women or minority individual shall be maintained on a waiting list, and shall be considered for employment as described in above, whenever vacancies occur. At the request of the Dept. of LWD, Construction EEO Monitoring Program, the contractor or subcontractor shall provide evidence of its good faith efforts to employ women and minorities from the list to fill vacancies.

(iv) If, for any reason, said contractor or subcontractor determines that a minority individual or a woman is not qualified or if the individual qualifies as an advanced trainee or apprentice, the contractor or subcontractor shall inform the individual in writing of the reasons for the determination, maintain a copy of the determination in its files, and send a copy to the public agency compliance officer and to the Dept. of LWD, Construction EEO Monitoring Program.

(7) To keep a complete and accurate record of all requests made for the referral of workers in any trade covered by the contract, on forms made available by the Dept. of LWD, Construction EEO Monitoring Program and submitted promptly to the Dept. of LWD, Construction EEO Monitoring Program upon request.

(C) The contractor or subcontractor agrees that nothing contained in (B) above shall preclude the contractor or subcontractor from complying with the union hiring hall or apprenticeship policies in any applicable collective bargaining agreement or union hiring hall arrangement, and, where required by custom or agreement, it shall send journeymen and

Not Applicable

EXHIBIT B - RETURN WITH BID
MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE
N.J.S.A. 10:5-31 et seq. (P.L.1975, c.127)
N.J.A.C. 17:27-1.1 et seq.
CONSTRUCTION CONTRACTS-continued

trainees to the union for referral, or to the apprenticeship program for admission, pursuant to such agreement or arrangement. However, where the practices of a union or apprenticeship program will result in the exclusion of minorities and women or the failure to refer minorities and women consistent with the targeted county employment goal, the contractor or subcontractor shall consider for employment persons referred pursuant to (B) above without regard to such agreement or arrangement; provided further, however, that the contractor or subcontractor shall not be required to employ women and minority advanced trainees and trainees in numbers which result in the employment of advanced trainees and trainees as a percentage of the total workforce for the construction trade, which percentage significantly exceeds the apprentice to journey worker ratio specified in the applicable collective bargaining agreement, or in the absence of a collective bargaining agreement, exceeds the ratio established by practice in the area for said construction trade. Also, the contractor or subcontractor agrees that, in implementing the procedures of (B) above, it shall, where applicable, employ minority and women workers residing within the geographical jurisdiction of the union.

After notification of award, but prior to signing a construction contract, the contractor shall submit to the public agency compliance officer and the Dept. of LWD, Construction EEO Monitoring Program an initial project workforce report (Form AA-201) electronically provided to the public agency by the Dept. of LWD, Construction EEO Monitoring Program, through its website, for distribution to and completion by the contractor, in accordance with N.J.A.C. 17:27-7. The contractor also agrees to submit a copy of the Monthly Project Workforce Report once a month thereafter for the duration of this contract to the Dept. of LWD, Construction EEO Monitoring Program, and to the public agency compliance officer. The contractor agrees to cooperate with the public agency in the payment of budgeted funds, as is necessary, for on-the-job and/or off-the job programs for outreach and training of minorities and women.

(D) The contractor and its subcontractors shall furnish such reports or other documents to the Dept. of LWD, Construction EEO Monitoring Program as may be requested by the Dept. of LWD, Construction EEO Monitoring Program from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Dept. of LWD, Construction EEO Monitoring Program for conducting a compliance investigation pursuant to N.J.A.C. 17:27-1.1 et seq. (Revised: January, 2016)

Company _____

Signature _____

Name _____
Title _____

Not Applicable

Sample-AA201

Official Use Only

Assignment

Code

STATE OF NEW JERSEY

DEPARTMENT OF LABOR & WORKFORCE DEVELOPMENT
CONSTRUCTION EEO COMPLIANCE MONITORING PROGRAM

FORM AA-201
Revised 11/11

INITIAL PROJECT WORKFORCE REPORT CONSTRUCTION

For instructions on completing the form, go to: http://www.state.nj.us/treasury/contract_compliance/pdf/aa201ins.pdf

1. FID NUMBER

2. CONTRACTOR ID NUMBER

3. NAME AND ADDRESS OF PRIME CONTRACTOR

(Name)

(Street Address)

(City) (State) (Zip Code)

4. IS THIS COMPANY MINORITY OWNED [ ] OR WOMAN OWNED [ ]

5. NAME AND ADDRESS OF PUBLIC AGENCY AWARDING CONTRACT

Name:
Address:

CONTRACT NUMBER **DATE OF AWARD** **DOLLAR AMOUNT OF AWARD**

6. NAME AND ADDRESS OF PROJECT

Name:
Address:

7. PROJECT NUMBER

COUNTY

8. IS THIS PROJECT COVERED BY A PROJEC
LABOR AGREEMENT (PLA)? YES

9. TRADE OR CRAFT	PROJECTED TOTAL EMPLOYEES				PROJECTED MINORITY EMPLOYEES				PROJECTED PHASE - IN DATE	PROJECTED COMPLETION DATE
	MALE		FEMALE		MALE		FEMALE			
	J	AP	J	AP	J	AP	J	AP		
1. ASBESTOS WORKER										
2. BRICKLAYER OR MASON										
3. CARPENTER										
4. ELECTRICIAN										
5. GLAZIER										
6. HVAC MECHANIC										
7. IRONWORKER										
8. OPERATING ENGINEER										
9. PAINTER										
10. PLUMBER										
11. ROOFER										
12. SHEET METAL WORKER										
13. SPRINKLER FITTER										
14. STEAMFITTER										
15. SURVEYOR										
16. TILER										
17. TRUCK DRIVER										
18. LABORER										
19. OTHER										
20. OTHER										

I hereby certify that the foregoing statements made by me are true. I am aware that if any of the foregoing statements are willfully false, I am subject to punishment.

(Signature)

10. (Please Print Your Name) (Title)

(Area Code) (Telephone Number) (Ext.) (Date)

INSTRUCTIONS FOR COMPLETING THE INITIAL PROJECT WORKFORCE REPORT – CONSTRUCTION (AA201)

DO NOT COMPLETE THIS FORM FOR GOODS AND/OR SERVICE CONTRACTS

1. **Enter the Federal Identification Number assigned to the contractor by the Internal Revenue Service, or if a Federal Employer Identification Number has been applied for but not yet issued, or if your business is such that you have not or will not receive a Federal Identification Number, enter the social security number assigned to the single owner or one partner, in the case of a partnership.**

2. **Note: The Department of Labor & Workforce Development, Construction EEO Monitoring Program will assign a contractor ID number to your company. This number will be your permanently assigned contractor ID number that must be on all correspondence and reports submitted to this office.**

3. **Enter the prime contractor's name, address and zip code number.**

4. **Check box if Company is Minority Owned or Woman Owned**

5. **Enter the complete name and address of the Public Agency awarding the contract. Include the contract number, date of award and dollar amount of the contract.**

6. **Enter the name and address of the project, including the county in which the project is located.**

7. **Note: A project contract ID number will be assigned to your firm upon receipt of the completed Initial Project Workforce Report (AA201) for this contract. This number must be indicated on all correspondence and reports submitted to this office relating to this contract.**

8. **Check "Yes" or "No" to indicate whether a Project Labor Agreement (PLA) was established with the labor organization(s) for this project.**

9. **Under the Projected Total Number of Employees in each trade or craft and at each level of classification, enter the total composite workforce of the prime contractor and all subcontractors projected to work on the project. Under Projected Employees enter total minority and female employees of the prime contractor and all subcontractors projected to work on the project. Minority employees include Black, Hispanic, American Indian and Asian, (J=Journey worker, AP=Apprentice). Include projected phase-in and completion dates.**

10. **Print or type the name of the company official or authorized Equal Employment Opportunity (EEO) official include signature and title, phone number and date the report is submitted.**

This report must be submitted to the Public Agency that awards the contract and the Department of Labor & Workforce Development, Construction EEO Compliance Monitoring Program after notification of award, but prior to signing the contract.

THE CONTRACTOR IS TO RETAIN A COPY AND SUBMIT COPY TO THE PUBLIC AGENCY AWARDING THE CONTRACT AND FORWARD A COPY TO:

NEW JERSEY DEPARTMENT OF LABOR & WORKFORCE DEVELOPMENT
CONSTRUCTION EEO COMPLIANCE MONITORING UNIT
P.O. BOX 209
TRENTON, NJ 08625-0209
(609) 292-9550

Not Applicable

EQUIPMENT CERTIFICATION - RETURN WITH BID

In accordance with N.J.S.A. 18A:18A-23, I hereby certify that

A) _____owns all the necessary equipment as required by the
Name of Company
specifications and to complete the specified public work project.

or

B) _____leases or controls all the necessary equipment as required
Name of Company
by the specifications and to complete the specified public work project.

PLEASE NOTE: If your company is not the actual owner of the equipment, **you shall submit with the bid:**

1. A certificate stating the source from which the equipment will be obtained and

2. Obtain and submit with the bid a certificate from the owner and person in control of the equipment, definitely granting to the bidder the control of the equipment required during such time it may be necessary for the completion of that portion of the contract for which said equipment will be necessary.

Name of Company_____

Authorized Agent

Title_____

Authorized Signature_____

Not Applicable

PRE-QUALIFICATION AFFIDAVIT—NO MATERIAL ADVERSE CHANGE - RETURN WITH BID

The below affidavit must be submitted with your bid for projects over $20,000.00 pursuant to N.J.S.A. 18A:18A-32:

I, _____ of the City of _____
in the County of _____ and the State of _____

of full age, being duly sworn according to law on my oath depose and say that:

No Material Adverse Change in Qualification

I am_____ *(Position in Company)*, and the bidder for the above named project. The answers to the following statements are true and correct and that there has been no material adverse change in the qualification information subsequent to the latest statement submitted as required (N.J.S.A. 18A:18A-32 et seq.) as amended, except as set forth herewith. I further certify that there is not now pending any litigation or other action that may jeopardize my rating, status or contract limits from their current limits.

Notice of Classification (DPMC 27)

_____ *(Name of Company)* is classified by the State of New Jersey pursuant to N.J.S.A. 52:35-1 et seq. This Classification became effective (Date).
Type of Contract/Trade Classified: _____

_____

Classification Approved Amount $_____
A copy of my valid and active prequalification/classification certificate from the Department of Treasury, Division of Property Management and Construction has been submitted with this bid.

Total Amount of Uncompleted Contracts (DPMC 701)

The total amount of uncompleted work is $_____ as of _____(Date).
A copy of the company's Total Amount of Uncompleted Contracts form is required to be submitted with the bid.

NJSDA Prequalification

The _____ (Name of Company), pursuant to N.J.S.A.18A:7G-33, is prequalified with the NJSDA on contracts for "school facilities" projects as defined by code. NJSDA prequalification is not a requirement for maintenance projects.

_____ _____
Signature of Authorized Representative **Date**

Sworn and subscribed to before me this _____ day of _____ in the Year __

_____ _____Notary Public of _____
Signature of Notary **Print Name of Notary**

My Commission Expires:_____ _____ _____ **SEAL**
Month Day Year

Not Applicable

PREVAILING WAGES COMPLIANCE CERTIFICATION - RETURN WITH BID

It is the determination of the ESCNJ that this is a public works project that in total will exceed $2,000.00 (two thousand dollars), therefore prevailing wages rules and regulations apply as promulgated by the New Jersey Prevailing Wage Act and in conformance with N.J.S.A. 34:11-56:25 et seq.

CERTIFICATION

1. I certify that our company understands that this project of the ESCNJ or its Co-op members requires prevailing wages to be paid in full accordance with the law.

2. I further certify that all subcontractors named in this bid understand that this project requires the subcontractor to pay prevailing wages in full accordance with the law.

Non-compliance Statement

If it is found that any worker, employed by the contractor or any subcontractor covered by said contract, has been paid a rate of wages less than the prevailing wage required to be paid by such contract, the ESCNJ or its members may begin proceedings to terminate the contractor's or subcontractor's right to proceed with the work, or such part of the work as to which there has been a failure to pay required wages and to prosecute the work to completion or otherwise. The contractor and his sureties shall be liable for any excess costs occasioned thereby to the public body.

NOTIFICATION OF VIOLATIONS – New Jersey Department of Labor and Workforce Development

Has the bidder or any person having an "interest" with the bidder, been notified by the New Jersey Department of Labor and Workforce Development by notice issued pursuant to N.J.S.A. 34:11-56:37 that he/she has been in violation for failure to pay prevailing wages as required by the New Jersey Prevailing Wage Act within the last five (5) years?

* Yes _____ No _____

*If yes, please attach a signed document explaining any/or all administrative proceedings with the Department within the last five (5) years. Please include any pending administrative proceedings with the Department if any.

Submission of Certified Payroll Records

All certified payroll records are to be submitted to the member/person who is coordinating the activities for the project.

Name of Company: _____

Authorized Agent: _____

Title of Authorized Agent: _____

Authorized Signature: _____

Not Applicable

SUBCONTRACTOR'S DISCLOSURE FORM - RETURN WITH BID

If the bidder **will** subcontract any part of their services /installation award, the bidder ***must*** do the following:

Provide the name, address and other pertinent information about the subcontractor;*

Please list subcontractor(s) here.

**Failure to identify the names and addresses of any subcontractors required to be named in the bid, or to submit the appropriate documents for each such subcontractor, may be cause for the bid to be rejected as being non-responsive.*

SHI acknowledges this requirement and will comply. SHI is submitting this response as a MBE/WBE certified prime bidder and will update this form with the AEPA before signing any customer SOW requiring a subcontractor.

1. Sub-Contractor for _____

Name of Subcontracting Company_____

Address_____

City, State, Zip_____

Telephone_____Fax_____

E-Mail _____FEIN No_____

Authorized Agent _____ Title _____

Certification of Equipment

The_____hereby certifies the above named
Name of Bidding Company

subcontractor has the personnel, equipment, experience, financial and sufficient means to complete their portion of the contract in full accordance with the bid specifications.

Moitrayee Majumdar _____ Moitrayee Majumdar _____

Authorized Agent (Print)—Bidder ***Signature of Authorized Agent—Bidder***

Bidders may make extra copies of this page to list additional subcontractors and subcontractors may be added throughout the life of the bid after receiving approval from the ESCNJ.

SUBCONTRACTOR'S DISCLOSURE FORM *(Continued)* - **RETURN WITH BID**

If the bidder **will** subcontract any part of their services /installation award, the bidder ***must*** do the following:

Provide the name, address and other pertinent information about the subcontractor;*

Please list subcontractor(s) here.

**Failure to identify the names and addresses of any subcontractors required to be named in the bid, or to submit the appropriate documents for each such subcontractor, may be cause for the bid to be rejected as being non-responsive.*

SHI acknowledges this requirement and will comply. SHI is submitting this response as a MBE/WBE certified prime bidder and will update this form with the AEPA before signing any customer SOW requiring a subcontractor.

1. Sub-Contractor for Other _____

Name of Subcontracting Company_____

Address_____

City, State, Zip_____

Telephone_____Fax_____

E-Mail _____FEIN No_____

Authorized Agent _____ Title _____

Certification of Equipment

The_____hereby certifies the above named

Name of Bidding Company

subcontractor has the personnel, equipment, experience, financial and sufficient means to complete their portion of the contract in full accordance with the bid specifications.

Moitrayee Majumdar _____ Moitrayee Majumdar _____

Authorized Agent (Print)—Bidder ***Signature of Authorized Agent—Bidder***

Bidders may make extra copies of this page to list additional subcontractors and subcontractors may be added throughout the life of the bid after receiving approval from the ESCNJ.

Type text here

Sworn Contractor Certification; Qualifications and Credentials (Bidder's Certification) - RETURN WITH BID

Pursuant to N.J.S.A. 18A:7G-37, a pre-qualified contractor seeking to bid school facilities projects, and any subcontractors, that are required to be named under N.J.S.A. 18A:7G-1 et seq. shall, as a condition of bidding, submit this Sworn Contractor Certification regarding qualifications and credentials.

I_____ the principal owner or officer of the company certify that the forgoing statements are true and our firm has the following qualifications and credentials:

1. A current, valid certificate of registration issued pursuant to "The Public Works Contractor Registration Act," N.J.S.A. 34:11-56:48 et seq. A copy of which is submitted with its bid;

2. A current, valid Certificate of Authority to perform work in New Jersey issued by the Department of Treasury, a copy of which is submitted with its bid;

3. A current valid contractor trade license required under applicable New Jersey Law for any specialty trade or specialty area in which the firm seeks to perform work, a copy of which is submitted with its bid;

4. During the term of the project, I as principal owner or officer of the company or corporation, as contractor, will have in place a suitable quality control and quality assurance program and appropriate safety and health plan.

5. Certify that, at the time of bidding, the amount of the bid proposal and value of all of its outstanding incomplete contracts does not exceed the firm's existing aggregate rating limit.

Name of Company_____

Name of Owner or Officer_____

Signature of Owner or Officer_____

Notarized before me this _____ day of _____, _____
Month Year

_____ _____
NOTARY PUBLIC SIGNATURE **Print Name of Notary Public**

My commission expires _____ _____, _____
Month Day Year

-SEAL-

Not Applicable

RETURN WITH BID

State of New Jersey

DEPARTMENT OF THE TREASURY
DIVISION OF PROPERTY MANAGEMENT AND CONSTRUCTION
33 W. STATE STREET
PO BOX 034
TRENTON, NEW JERSEY 08625-0034

REPLY TO:
TEL: (609) 943-3400
FAX: (609) 292-7651

TOTAL AMOUNT OF UNCOMPLETED CONTRACTS

(This form is to be used with the NOTICE OF CLASSIFICATION when submitting bids to the ESCNJ.) I certify that the amount of uncompleted work on contracts is $_____.

The amount claimed includes uncompleted portions of all currently held contracts from all sources (public and private) in accordance with N.J.A.C. 1 7:19-2.13.

I further certify that the amount of this bid proposal, including all outstanding incomplete contracts does not exceed my prequalification dollar limit.

Affix corporate seal here

_____
Name of Firm

_____
Signature

_____
Title

_____
_____
Address

_____
Phone

Sworn to and Subscribed before me

This day ____ of _____ 20___
Notary Public

DPMC 701 (3/15)

Not Applicable

Vendor Contact Form - RETURN WITH BID

This page should be included in your electronic file in Word format
so that we can copy and paste into our website.
Please do not handwrite the information; type it in.

If you are awarded a contract with the ESCNJ, we will post this contact sheet on our website for members to contact. Please complete and include with your bid package. List the individual(s) who will be best equipped to handle calls from our 1,300+ members and have knowledge of your award.

Bid	**Title of Bid:** RFP AEPA RFP#025 - F CYBER SECURITY & TRAINING **Bid #** AEPA RFP#025
Vendor	SHI International Corp.
Representative	PS_Contracts
Address	290 Davidson Ave. Somerset, NJ 08873
Telephone #	888-764-8888
Fax #	888-764-8889
Email	PS_Contracts@shi.com
Website	https://www.shi.com/

NEW JERSEY REQUIRED DOCUMENTS CHECKLIST – RETURN WITH BID			
1.	Affirmative Action Construction Contracts Acknowledgement **and** Total Work Force/Employee AA201 (for Public Works contracts) Not Applicable	16.	NJ School Development Authority Prequalification (for Public Works contracts) Not Applicable
2.	Affirmative Action Questionnaire and supported documentation (current CEIR) ✓	17.	Non-Collusion Affidavit **Notarized and Sealed**
3.	Americans with Disabilities Act of 1990 ✓	18.	Pre-Qualification Affidavit (Projects over $20,000 in accordance with N.J.S.A. 18A:18A-26 et. seq.) Not Applicable
4.	Assurance of Compliance ✓	19.	Prevailing Wage Certification (for Public Works contracts) Not Applicable
5.	Certificate of Authority ✓	20.	Request for Clarifications Form Not Applicable
6.	Certificate of Insurance with the Educational Services Commission of New Jersey named as the certificate holder with Bid Title and Bid # **(Upon award)**	21.	Respondent Comment Form – Optional Not Applicable
7.	Chapter 271 Political Contribution Disclosure Form ✓	22.	Statement of Ownership (Ownership Disclosure Certification) ✓
8.	Dealer/Subcontractor Documents if applicable Not Applicable	23.	Statement of Suspension or Debarment **Notarized & Sealed** ✓
9.	Disclosure of Investment Activities in Iran Form (for Public Works contracts) Not Applicable	24.	Sub-contractor's Disclosure Form(s) ✓
10.	DPMC Notice of Classification Form Not Applicable	25.	Sworn Contractor Certification; Qualifications and Credentials (for Public Works contracts) Not Applicable
11.	Equipment Certification Not Applicable	26.	Total Amount of Uncompleted Contracts Form-Certified (DPMC Form 701) (for Public Works contracts) Not Applicable
12.	Exhibit B Mandatory Equal Employment Opportunity Language Construction Contracts Not Applicable	27.	Vendor Contact Form ✓
13.	Licenses	28.	W-9 Form ✓
14.	New Jersey Business Registration Certificate **(Received no later than the time of award) ✓		
15.	New Jersey Public Works Contractor Certificate (for Public Works contracts) Not Applicable		

Signature: Moitrayee Majumdar

Please sign above indicating that you have included all of the required New Jersey documents on this checklist and return this checklist with your bid package.

STATE OF NEW JERSEY
BUSINESS REGISTRATION CERTIFICATE

Taxpayer Name:	SHI INTERNATIONAL CORP.
Trade Name:	
Address:	290 DAVIDSON AVENUE SOMERSET, NJ 08873-3135
Certificate Number:	0078008
Effective Date:	December 11, 1989
Date of Issuance:	October 25, 2021

For Office Use Only:

20211025173135067

12/20/11

Taxpayer Identification# **223-009-648/000**

Dear Business Representative:

Congratulations! You are now registered with the New Jersey Division of Revenue.

Use the Taxpayer Identification Number listed above on all correspondence with the Divisions of Revenue and Taxation, as well as with the Department of Labor (if the business is subject to unemployment withholdings). Your tax returns and payments will be filed under this number, and you will be able to access information about your account by referencing it.

Additionally, please note that State law requires all contractors and subcontractors with Public agencies to provide proof of their registration with the Division of Revenue. The law also amended Section 92 of the Casino Control Act, which deals with the casino service industry.

We have attached a Proof of Registration Certificate for your use. To comply with the law, if you are currently under contract or entering into a contract with a State agency, you must provide a copy of the certificate to the contracting agency.

If you have any questions or require more information, feel free to call our Registration Hotline at (609)292-9292.

I wish you continued success in your business endeavors.

Sincerely,

James J. Fruscione

James J. Fruscione
Director
New Jersey Division of Revenue

STATE OF NEW JERSEY

BUSINESS REGISTRATION CERTIFICATE

DEPARTMENT OF TREASURY/
DIVISION OF REVENUE
PO BOX 252
TRENTON, N J 08646-0252

TAXPAYER NAME:

SHI INTERNATIONAL CORP.

ADDRESS:

290 DAVIDSON AVENUE
SOMERSET NJ 08873

EFFECTIVE DATE:

12/11/89

TRADE NAME:

SOFTWARE HOUSE

SEQUENCE NUMBER:

0078008

ISSUANCE DATE:

12/20/11

James J. Fruscione

Director
New Jersey Division of Revenue

FORM-BRC
[illegible]

This Certificate is NOT assignable or transferable. It must be conspicuously displayed at above address.

SHI's Affirmative/EEO Plan

To comply with governmental regulations and the company's Affirmative Action Policy and obligations to employ, retain, promote, terminate, and otherwise treat all employees and job applicants on the basis of merit, qualifications, and competence.

1. A complete up-to-date Personnel Profile of all employees classified by race, sex, and job classification will be maintained, and annual reports will be submitted to the EEOC.
2. All employees will be advised at the time of employment and during the HR orientation that SHI is an equal opportunity/affirmative action employer and that all personnel decisions are based on an individual's qualifications and ability to perform the work.
3. A company policy statement outlining SHI's commitment to equal employment opportunity will be posted on SHI's intranet site, MySHI, as well as within the Handbook. A detailed policy outlining SHI's commitment to affirmative action will be accessible upon request within the Human Resources department.
4. The company has appointed Ellen Mass to serve as the Equal Employment Opportunity/Affirmative Action officer. The EEO/AA officer is authorized to supply reports and represent this company in all matters referenced in this document and regarding the Company's Affirmative Action Plans.
5. The EEO/AA officer will be responsible for the following:
    a. Implementing all phases and requirements of the plan
    b. Conducting quarterly audits of employment practices to ensure nondiscrimination
    c. Providing yearly instruction to supervisors regarding their responsibilities of compliance with Affirmative Action and Equal Employment obligations, ensuring no type of discriminatory practices or harassment are present and all requirements are implemented.
    d. Notification via Job posting (MySHI), SHI newsletter, recruiters to all eligible employees regarding promotions or vacancies to ensure equal employment opportunity.
6. All applicants or employees seeking promotion are reviewed fairly. HR reviews applicant and promotion records with the CEO of SHI to monitor job availability and the recruitment labor area.
7. Training is provided without regard to race, gender, disability status, veteran status, or any other prohibited factor ensuring job opportunities are equally available to all.

Ellen Mass

Ellen Mass, Vice President of Human Resources

5-15-24

Date

These goals are established company-wide and reach each department. They are established for women, minorities, individuals with disabilities, and veterans and are designed to increase availability for greater utilization.

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
CONSOLIDATED REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME
R608600	SHI INTERNATIONAL CORP.

ADDRESS	CITY/TOWN	STATE	ZIP CODE
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME

HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	CITY/TOWN	STATE	ZIP CODE

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
[X] **YES** (Employer Is Eligible to File) [ ] **NO** (Employer Is Not Eligible to File) [ ] **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

[ ] **YES** (Single-Establishment Employer is Federal Contractor) [X] **YES** (Multi-Establishment Employer is Federal Contractor)

[X] **YES** (Headquarters is Federal Contractor) [ ] **YES** (Non-Headquarters Establishment is Federal Contractor)

[X] **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	1	0	22	1	3	0	0	0	6	0	2	0	0	0	35
First/Mid-Level Officials and Managers	45	32	482	45	27	2	1	13	217	19	20	0	0	9	912
Professionals	135	89	889	109	119	2	2	39	433	88	100	1	2	25	2033
Technicians	39	6	69	46	17	0	0	8	1	2	4	0	0	0	192
Sales Workers	151	91	1001	56	52	1	4	32	424	31	49	0	3	20	1915
Administrative Support Workers	35	38	77	35	33	1	1	7	78	28	30	0	2	8	373
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	8	0	1	7	0	0	0	0	0	0	0	0	0	0	16
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	414	256	2541	299	251	6	8	99	1159	168	205	1	7	62	5476
PRIOR 2022 REPORTING YEAR TOTAL	407	259	2562	339	264	7	9	96	1165	195	201	1	5	59	5569

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
Not Applicable

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION K – OFFICIAL CERTIFICATION OF SUBMISSION

EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME
R608600	SHI INTERNATIONAL CORP.

ADDRESS	CITY/TOWN	STATE	ZIP CODE
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

CERTIFICATION COMMENTS (optional)

No Certification Comments Provided

CERTIFICATION STATEMENT

"I certify that the information, including any workforce demographic data, provided in this report is correct and true to the best of my knowledge and was prepared in conformity with the directions set forth in the form and accompanying instructions."

Knowingly and willfully false statements on this report are punishable by law, US Code, Title 18, Section 1001.

DATE OF CERTIFICATION

5/28/2024 1:34 PM [EST]

EMPLOYER'S CERTIFYING OFFICIAL

Name of Employer's Certifying Official	Title of Certifying Official
Dorothy L. Clinton	Ethics and Compliance Officer
Email Address of Certifying Official	**Telephone Number of Certifying Official**
dorothy_clinton@shi.com	732-537-7279

PRIMARY POINT OF CONTACT (POC) FOR EEO-1 COMPONENT 1 REPORTING

Name of Primary POC	Title and Employer of Primary POC
Dorothy L. Clinton	Ethics and Compliance Officer SHI International Corp
Email Address of Primary POC	**Telephone Number of Primary POC**
dorothy_clinton@shi.com	732-537-7279

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
HEADQUARTERS REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME		
R608600	SHI INTERNATIONAL CORP.		
ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME		
R608600	SHI INTERNATIONAL CORP.		
HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
☒ **YES** (Employer Is Eligible to File) ☐ **NO** (Employer Is Not Eligible to File) ☐ **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

☐ **YES** (Single-Establishment Employer is Federal Contractor) ☒ **YES** (Multi-Establishment Employer is Federal Contractor)

☒ **YES** (Headquarters is Federal Contractor) ☐ **YES** (Non-Headquarters Establishment is Federal Contractor)

☒ **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	1	0	13	1	3	0	0	0	5	0	1	0	0	0	24
First/Mid-Level Officials and Managers	23	14	362	22	18	0	1	10	170	15	15	0	0	7	657
Professionals	90	59	740	83	98	2	0	31	349	76	92	1	2	21	1644
Technicians	8	1	24	9	2	0	0	2	0	0	0	0	0	0	46
Sales Workers	68	45	693	36	37	0	4	19	286	23	34	0	2	15	1262
Administrative Support Workers	17	25	61	24	26	0	0	6	69	21	23	0	1	8	281
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	207	144	1893	175	184	2	5	68	879	135	165	1	5	51	3914
PRIOR 2022 REPORTING YEAR TOTAL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME		
R608600	SHI INTERNATIONAL CORP.		
ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME		
JG53885	SHI COLUMBUS		
HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
425 METRO PLACE, STE 220	DUBLIN	OH	43017

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
[X] **YES** (Employer Is Eligible to File) [ ] **NO** (Employer Is Not Eligible to File) [ ] **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): Not Applicable

[ ] **YES** (Single-Establishment Employer is Federal Contractor) [X] **YES** (Multi-Establishment Employer is Federal Contractor)

[X] **YES** (Headquarters is Federal Contractor) [ ] **YES** (Non-Headquarters Establishment is Federal Contractor)

[X] **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First/Mid-Level Officials and Managers	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Professionals	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Technicians	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sales Workers	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Administrative Support Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	0	0	2	0	0	0	0	0	0	0	0	0	0	0	2
PRIOR 2022 REPORTING YEAR TOTAL	0	0	4	0	0	0	0	0	0	0	0	0	0	0	4

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME		
R608600	SHI INTERNATIONAL CORP.		
ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME		
GM89122	SHI GOVERNMENT SOLUTIONS INC.		
HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
3828 Pecana Trail	AUSTIN	TX	78749

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
☒ **YES** (Employer Is Eligible to File) ☐ **NO** (Employer Is Not Eligible to File) ☐ **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

☐ **YES** (Single-Establishment Employer is Federal Contractor) ☒ **YES** (Multi-Establishment Employer is Federal Contractor)

☒ **YES** (Headquarters is Federal Contractor) ☒ **YES** (Non-Headquarters Establishment is Federal Contractor)

☒ **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
First/Mid-Level Officials and Managers	0	1	2	1	0	0	0	0	1	0	0	0	0	0	5
Professionals	1	0	2	0	0	0	0	0	2	0	0	0	0	0	5
Technicians	4	1	9	0	1	0	0	1	0	0	0	0	0	0	16
Sales Workers	4	1	6	0	0	0	0	0	6	1	0	0	0	0	18
Administrative Support Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	9	3	19	1	1	0	0	1	9	1	1	0	0	0	45
PRIOR 2022 REPORTING YEAR TOTAL	10	2	25	2	0	0	0	1	10	1	1	0	0	0	52

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME
R608600	SHI INTERNATIONAL CORP.

ADDRESS	CITY/TOWN	STATE	ZIP CODE
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME
JG53896	SHI HOUSTON TX

HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	CITY/TOWN	STATE	ZIP CODE
2000 WEST SAM HOUSTON PARKWAY SOUTH, SUITE 800	HOUSTON	TX	77042

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
[X] **YES** (Employer Is Eligible to File) [ ] **NO** (Employer Is Not Eligible to File) [ ] **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): Not Applicable

[ ] **YES** (Single-Establishment Employer is Federal Contractor) [X] **YES** (Multi-Establishment Employer is Federal Contractor)

[X] **YES** (Headquarters is Federal Contractor) [ ] **YES** (Non-Headquarters Establishment is Federal Contractor)

[X] **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First/Mid-Level Officials and Managers	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2
Professionals	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Technicians	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sales Workers	0	0	4	0	0	0	0	0	4	0	1	0	0	0	9
Administrative Support Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	0	0	5	0	0	0	0	0	6	0	1	0	0	0	12
PRIOR 2022 REPORTING YEAR TOTAL	0	0	8	0	0	0	0	0	7	0	1	0	0	0	16

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME		
R608600	SHI INTERNATIONAL CORP.		
ADDRESS	CITY/TOWN	STATE	ZIP CODE
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME		
JG53803	SHI FORT LAUDERDALE		
HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	CITY/TOWN	STATE	ZIP CODE
101 NE 3RD AVE, STE 420	FT. LAUDERDALE	FL	33301

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
[X] **YES** (Employer Is Eligible to File) [ ] **NO** (Employer Is Not Eligible to File) [ ] **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

[ ] **YES** (Single-Establishment Employer is Federal Contractor) [X] **YES** (Multi-Establishment Employer is Federal Contractor)

[X] **YES** (Headquarters is Federal Contractor) [X] **YES** (Non-Headquarters Establishment is Federal Contractor)

[X] **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity: Hispanic or Latino: Male	Hispanic or Latino: Female	Not Hispanic or Latino: Male: White	Male: Black or African American	Male: Asian	Male: Native Hawaiian or Other Pacific Islander	Male: American Indian or Alaska Native	Male: Two or More Races	Not Hispanic or Latino: Female: White	Female: Black or African American	Female: Asian	Female: Native Hawaiian or Other Pacific Islander	Female: American Indian or Alaska Native	Female: Two or More Races	Row Total
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First/Mid-Level Officials and Managers	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Professionals	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Technicians	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sales Workers	1	1	1	0	0	0	0	0	2	0	0	0	0	0	5
Administrative Support Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	1	1	3	0	0	0	0	0	2	0	0	0	0	0	7
PRIOR 2022 REPORTING YEAR TOTAL	1	2	3	0	0	0	0	0	3	0	0	0	0	0	9

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME		
R608600	SHI INTERNATIONAL CORP.		
ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME		
JG55315	SHI MANHATTAN		
HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
ONE PENN PLAZA, SUITE 1020	NEW YORK	NY	10119

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
[X] **YES** (Employer Is Eligible to File) [ ] **NO** (Employer Is Not Eligible to File) [ ] **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

[ ] **YES** (Single-Establishment Employer is Federal Contractor) [X] **YES** (Multi-Establishment Employer is Federal Contractor)

[X] **YES** (Headquarters is Federal Contractor) [X] **YES** (Non-Headquarters Establishment is Federal Contractor)

[X] **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First/Mid-Level Officials and Managers	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Professionals	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Technicians	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sales Workers	1	0	14	1	0	0	0	1	6	0	0	0	0	0	23
Administrative Support Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	1	0	14	1	0	0	0	1	8	0	0	0	0	0	25
PRIOR 2022 REPORTING YEAR TOTAL	2	1	15	1	1	0	0	1	7	0	0	0	0	0	28

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME		
R608600	SHI INTERNATIONAL CORP.		
ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME		
DQ71535	SHI INTERNATIONAL CORP.		
HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
3828 Pecana Trail	AUSTIN	TX	78749

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
☒ **YES** (Employer Is Eligible to File) ☐ **NO** (Employer Is Not Eligible to File) ☐ **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

☐ **YES** (Single-Establishment Employer is Federal Contractor) ☒ **YES** (Multi-Establishment Employer is Federal Contractor)

☒ **YES** (Headquarters is Federal Contractor) ☒ **YES** (Non-Headquarters Establishment is Federal Contractor)

☒ **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	9	0	0	0	0	0	0	0	0	0	0	0	9
First/Mid-Level Officials and Managers	14	10	76	3	1	2	0	3	34	0	1	0	0	1	145
Professionals	27	25	88	14	9	0	1	4	53	7	5	0	0	4	237
Technicians	0	0	1	1	0	0	0	0	0	0	0	0	0	0	2
Sales Workers	76	44	266	18	15	1	0	11	110	7	14	0	1	5	568
Administrative Support Workers	3	4	3	3	1	0	1	0	5	1	1	0	0	0	22
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	120	83	443	39	26	3	2	18	202	15	21	0	1	10	983
PRIOR 2022 REPORTING YEAR TOTAL	117	82	463	39	27	3	3	20	217	20	21	0	0	8	1020

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME
R608600	SHI INTERNATIONAL CORP.

ADDRESS	CITY/TOWN	STATE	ZIP CODE
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME
JG55240	SHI RALEIGH

HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	CITY/TOWN	STATE	ZIP CODE
4819 EMPEROR BLOULEVARD, SUITE 210	DURHAM	NC	27703

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
[X] **YES** (Employer Is Eligible to File) [ ] **NO** (Employer Is Not Eligible to File) [ ] **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

[ ] **YES** (Single-Establishment Employer is Federal Contractor) [X] **YES** (Multi-Establishment Employer is Federal Contractor)

[X] **YES** (Headquarters is Federal Contractor) [X] **YES** (Non-Headquarters Establishment is Federal Contractor)

[X] **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First/Mid-Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Professionals	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Technicians	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sales Workers	0	0	4	1	0	0	0	0	1	0	0	0	0	0	6
Administrative Support Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	0	0	5	1	0	0	0	0	1	0	0	0	0	0	7
PRIOR 2022 REPORTING YEAR TOTAL	0	0	7	1	0	0	0	0	0	0	0	0	0	0	8

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME
R608600	SHI INTERNATIONAL CORP.

ADDRESS	CITY/TOWN	STATE	ZIP CODE
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME
PD09700	SHI Bethlehem

HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	CITY/TOWN	STATE	ZIP CODE
1605 Valley Center Parkway	BETHLEHEM	PA	18017

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
☒ **YES** (Employer Is Eligible to File) ☐ **NO** (Employer Is Not Eligible to File) ☐ **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

☐ **YES** (Single-Establishment Employer is Federal Contractor) ☒ **YES** (Multi-Establishment Employer is Federal Contractor)

☒ **YES** (Headquarters is Federal Contractor) ☒ **YES** (Non-Headquarters Establishment is Federal Contractor)

☒ **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First/Mid-Level Officials and Managers	0	0	2	0	0	0	0	0	2	0	1	0	0	1	6
Professionals	2	2	22	4	1	0	0	1	15	2	0	0	0	0	49
Technicians	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Sales Workers	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Administrative Support Workers	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	3	3	25	4	1	0	0	1	17	2	1	0	0	1	58
PRIOR 2022 REPORTING YEAR TOTAL	1	2	12	1	2	0	0	0	10	0	2	0	0	0	30

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME
R608600	SHI INTERNATIONAL CORP.

ADDRESS	CITY/TOWN	STATE	ZIP CODE
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME
JG53841	SHI CHARLOTTE NC

HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	CITY/TOWN	STATE	ZIP CODE
1520 SOUTH BLVD, STE 210	CHARLOTTE	NC	28203

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY

[X] **YES** (Employer Is Eligible to File) [ ] **NO** (Employer Is Not Eligible to File) [ ] **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

[ ] **YES** (Single-Establishment Employer is Federal Contractor) [X] **YES** (Multi-Establishment Employer is Federal Contractor)

[X] **YES** (Headquarters is Federal Contractor) [X] **YES** (Non-Headquarters Establishment is Federal Contractor)

[X] **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First/Mid-Level Officials and Managers	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Professionals	0	0	2	1	0	0	0	0	2	0	0	0	0	0	5
Technicians	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sales Workers	0	0	2	0	0	0	0	1	2	0	0	0	0	0	5
Administrative Support Workers	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	0	0	6	1	0	0	0	1	4	0	0	0	0	0	12
PRIOR 2022 REPORTING YEAR TOTAL	0	0	3	0	0	0	0	1	2	0	0	0	0	0	6

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME
R608600	SHI INTERNATIONAL CORP.

ADDRESS	CITY/TOWN	STATE	ZIP CODE
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME
QE95410	SHI Ridge

HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	CITY/TOWN	STATE	ZIP CODE
400 Ridge Road	PISCATAWAY	NJ	08854

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
☒ **YES** (Employer Is Eligible to File) ☐ **NO** (Employer Is Not Eligible to File) ☐ **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): Not Applicable

☐ **YES** (Single-Establishment Employer is Federal Contractor) ☒ **YES** (Multi-Establishment Employer is Federal Contractor)

☒ **YES** (Headquarters is Federal Contractor) ☐ **YES** (Non-Headquarters Establishment is Federal Contractor)

☒ **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
First/Mid-Level Officials and Managers	2	2	16	7	3	0	0	0	2	1	1	0	0	0	34
Professionals	5	0	17	1	6	0	1	1	5	2	1	0	0	0	39
Technicians	11	0	18	14	6	0	0	0	0	2	0	0	0	0	51
Sales Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Administrative Support Workers	2	3	4	1	0	1	0	1	1	3	2	0	1	0	19
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	4	0	0	1	0	0	0	0	0	0	0	0	0	0	5
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	24	5	55	24	15	1	1	2	9	8	4	0	1	0	149
PRIOR 2022 REPORTING YEAR TOTAL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME
R608600	SHI INTERNATIONAL CORP.

ADDRESS	CITY/TOWN	STATE	ZIP CODE
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME
JG53863	SHI CHICAGO

HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	CITY/TOWN	STATE	ZIP CODE
150 NORTH MICHIGAN AVENUE, SUITE 500	CHICAGO	IL	60601

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
[X] **YES** (Employer Is Eligible to File) [ ] **NO** (Employer Is Not Eligible to File) [ ] **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): Not Applicable

[ ] **YES** (Single-Establishment Employer is Federal Contractor) [X] **YES** (Multi-Establishment Employer is Federal Contractor)

[X] **YES** (Headquarters is Federal Contractor) [ ] **YES** (Non-Headquarters Establishment is Federal Contractor)

[X] **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First/Mid-Level Officials and Managers	0	0	2	0	0	0	0	0	0	0	0	0	0	0	2
Professionals	0	0	5	0	0	0	0	0	0	0	0	0	0	0	5
Technicians	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sales Workers	1	0	9	0	0	0	0	0	7	0	0	0	0	0	17
Administrative Support Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	1	0	16	0	0	0	0	0	7	0	0	0	0	0	24
PRIOR 2022 REPORTING YEAR TOTAL	1	0	22	0	0	0	0	0	11	0	0	0	0	0	34

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC)
2023 EMPLOYER INFORMATION REPORT (EEO-1 COMPONENT 1)

EEOC Standard Form 100 (SF 100)
Revised 08/2023
OMB Control Number: 3046-0049
Expiration Date: 11/30/2026

SECTION A – TYPE OF REPORT
ESTABLISHMENT-LEVEL REPORT

SECTION B – EMPLOYER IDENTIFICATION

OFS COMPANY ID	EMPLOYER NAME		
R608600	SHI INTERNATIONAL CORP.		
ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
290 DAVIDSON AVENUE	SOMERSET	NJ	08873

SECTION C – HEADQUARTERS OR ESTABLISHMENT-LEVEL IDENTIFICATION (if applicable)

HQ/ESTABLISHMENT-LEVEL UNIT ID	HEADQUARTERS OR ESTABLISHMENT-LEVEL NAME		
QB04735	SHI Knox Integration Center		
HEADQUARTERS OR ESTABLISHMENT-LEVEL ADDRESS	**CITY/TOWN**	**STATE**	**ZIP CODE**
10 Knox Drive	PISCATAWAY	NJ	08854

SECTION D – EMPLOYER IDENTIFICATION NUMBER (EIN)
223009648

SECTION E – EMPLOYER FILING ELIGIBILITY
[X] **YES** (Employer Is Eligible to File) [ ] **NO** (Employer Is Not Eligible to File) [ ] **EMPLOYER NO LONGER IN BUSINESS**

SECTION F – FEDERAL CONTRACTOR DESIGNATION (if applicable)
Unique Entity ID (UEI): UNAVAILABLE

[ ] **YES** (Single-Establishment Employer is Federal Contractor) [X] **YES** (Multi-Establishment Employer is Federal Contractor)

[X] **YES** (Headquarters is Federal Contractor) [X] **YES** (Non-Headquarters Establishment is Federal Contractor)

[X] **YES** (One or More Non-Headquarters Establishments is Federal Contractor)

SECTION G – NAICS INFORMATION
541511 - Custom Computer Programming Services

SECTION H – WORKFORCE DEMOGRAPHIC DATA

JOB CATEGORIES	Race/Ethnicity														Row Total
	Hispanic or Latino		Not Hispanic or Latino												
			Male						Female						
	Male	Female	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	White	Black or African American	Asian	Native Hawaiian or Other Pacific Islander	American Indian or Alaska Native	Two or More Races	
Executive/Senior Level Officials and Managers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First/Mid-Level Officials and Managers	6	5	19	12	5	0	0	0	5	3	2	0	0	0	57
Professionals	10	3	10	6	5	0	0	2	6	1	2	0	0	0	45
Technicians	15	4	17	22	8	0	0	5	1	0	4	0	0	0	76
Sales Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Administrative Support Workers	13	5	8	7	6	0	0	0	3	3	4	0	0	0	49
Craft Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operatives	4	0	1	6	0	0	0	0	0	0	0	0	0	0	11
Laborers and Helpers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CURRENT 2023 REPORTING YEAR TOTAL	48	17	55	53	24	0	0	7	15	7	12	0	0	0	238
PRIOR 2022 REPORTING YEAR TOTAL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

SECTION I – WORKFORCE SNAPSHOT PERIOD
12/9/2023 - 12/22/2023

SECTION J – HEADQUARTERS OR ESTABLISHMENT-LEVEL COMMENTS (optional)
No Comments Provided

Form **W-9**
(Rev. October 2018)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

▶ **Go to *www.irs.gov/FormW9* for instructions and the latest information.**

Give Form to the requester. Do not send to the IRS.

Print or type. See **Specific Instructions** on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.

SHI International Corp.

2 Business name/disregarded entity name, if different from above

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor or single-member LLC ☐ C Corporation ☑ S Corporation ☐ Partnership ☐ Trust/estate

☐ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ _____

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.

290 Davidson Avenue

Requester's name and address (optional)

6 City, state, and ZIP code

Somerset, NJ 08873

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

			–			–				

or

Employer identification number

2	2	–	3	0	0	9	6	4	8

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here **Signature of U.S. person ▶** Aij Mizan **Date ▶** 1/11/2024

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, *later.*

Docusign Envelope ID: 2AFE981B-3667-4C31-9F8F-A65A1E2B4A12

SHI International Corp.
290 Davidson Avenue
Somerset, NJ 08873
888-764-8888
SHI.com

Signature Authorization

Effective immediately, the following individuals are authorized to sign such contractual documents for SHI International Corp. as are specified below and on page 2 of this Authorization, and their respective signatures in such capacities shall bind SHI International Corp. to the signed document.

Level 1	Level 2	Level 3
Aimee Cantrell, Manager of Proposals	Chandler Gorda – Lead Contracts Specialist	Cassie Skelton, Director of Contracts
Alicia Jones, Sr. Proposal Specialist	Megan Allen, Sr. Contracts Specialist	Darek Awas, Associate Director of Contracts
Arianne Mount, Director of Public Sector Contract Compliance		Erin Rose, Sr. Lead Contracts Specialist
Cassandra Hansen, Director of Proposal Content Strategy Development		John Oese, Manager of Contracts
Cindy Fuentes, Sr. Proposal Specialist		Jenna Watson, Assistant General Counsel
Cindy Hill, Proposal Specialist		Kevin McCann, General Counsel
Dan Calabrese, Sr. Proposal Specialist		Kristina Mann, Sr. Manager - Contracts
Dan Rouette, Sr. Director of Proposals		Maria Randle, Sr. Lead Contracts Specialist - UK
Jamie Watson, Sr. Proposal Specialist		Mary Youssef, Associate General Counsel
Joanna York, Sr. Lead Contracts Specialist - Operations		Michael Drecolias, Sr. Lead Contracts Specialist
Kayleigh O'Kane, Proposal Specialist		Sarah Perfetto, Sr. Contracts Specialist
Marguerite Berete-Aw, Proposal Specialist		
Maya Lynch, Proposal Specialist		
Moitrayee Majumdar, Sr. Proposal Specialist		
Pamela Wilkinson, Sr. Contracts Administrator		
Staci McDonald, Manager of Proposals		
Stacie Becker, Sr. Proposal Specialist		

This authorization shall be in effect until rescinded. All previous signature authorizations are hereby rescinded.

SHI International Corp.

DocuSigned by:
Thai Lee
427E5237A9CA426...

Signature
Thai Lee
Name
President & CEO
Title
7/1/2024
Date

Docusign Envelope ID: 2AFE981B-3667-4C31-9F8F-A65A1E2B4A12

SHI International Corp.
290 Davidson Avenue
Somerset, NJ 08873
888-764-8888
SHI.com

Levels of Signature Authorization:

Level 1	Level 2	Level 3
Responses to Customer Requests for Proposal, Quote, Information (RFP, RFQ, RFI)	Customer Forms	Responses to Customer Requests for Proposal, Quote, Information (RFP, RFQ, RFI)
Customer Forms	Non-Disclosure Agreements	Customer Forms
Non-Disclosure Agreements	Vendor Forms	Non-Disclosure Agreements
Vendor Forms	Vendor Contracts	Vendor Forms
	Credit Reference Requests	Vendor Contracts
	Trade Reference Requests	Credit Reference Requests
		Trade Reference Requests
		US Customs and Border Protection Power of Attorney Forms
		Customer Contracts

Certification **15505**

CERTIFICATE OF EMPLOYEE INFORMATION REPORT **RENEWAL**

This is to certify that the contractor listed below has submitted an Employee Information Report pursuant to N.J.A.C. 17:27-1.1 et. seq. and the State Treasurer has approved said report. This approval will remain in effect for the period of **15-Feb-2023** to **15-Feb-2026**

SHI INTERNATIONAL, CORP.

290 DAVIDSON AVE.

SOMERSET **NJ** **08873**

ELIZABETH MAHER MUOIO
State Treasurer



SHI Response to AEPA 025 Part D Questionnaire (Q-78CD) Supporting Information

AEPA RFP#025 - F Cyber Security & Training

September 17, 2024

SHI International Corp.
290 Davidson Avenue
Somerset, NJ 08873
888-764-8888
SHI.com

September 17, 2024

Department: Purchasing

The request by the Association of Educational Purchasing Agencies (AEPA) for qualified and experienced cybersecurity contractors is critical to protecting the information assets of its member agencies across the United States. SHI International Corp. (SHI) is prepared to serve AEPA as a trusted vendor to your agencies, delivering solutions and services that provide value for members' purchasing dollar while allowing them to address their cybersecurity challenges with insight, expertise, and resources.

Our security solutions practice, built around the following six critical elements of effective security and outcome-driven roadmaps, will allow AEPA member agencies to realize their cybersecurity objectives:

- **Application Security:** Agencies will be able to adapt their application security practices as the face of current threats change.
- **Data Center and Cloud Security:** Agencies will be able to successfully address modern data center and cloud security challenges.
- **Data-Centric Security:** Agencies will be able to protect their critical data.
- **Identity and Access Management:** Agencies will be able to ensure safe access to critical applications and data.
- **Threat and Vulnerability Management:** Agencies will have the capability to identify and remediate gaps in their security defense.
- **Program Strategy and Operations:** Agencies will be able to successfully plan, set, and achieve their security goals.

We appreciate the opportunity to participate in your request for proposal, AEPA RFP#025 - F Cyber Security & Training. Should you have any questions regarding our response, or if you require additional information, please contact me at Moitrayee_Majumdar@shi.com or 858-232-2931 or Capture and Business Development Manager Chris Dickman at Chris_Dickman@SHI.com or 858-232-2931.

Our cybersecurity practice, our resources, and our experience make us ideally suited as a vendor partner for AEPA. Having grown from a regional, software-only reseller in 1989 to one of the largest, privately held, global technology solutions providers in the world—along with the largest women and minority-owned business in the United States—we are committed, like AEPA, to providing all member agencies with the same level of products, solutions, and services regardless of their size.

We look forward to exceeding your members' expectations and providing the solutions and services to solve their present and future purchasing needs.

Respectfully,

Moitrayee Majumdar

Moitrayee Majumdar

Senior Proposal Specialist.

Table of Contents

Question Set 1: Company Information 1
Sales History 6
Key Contacts 6
SHI Public Sector Account Team Org Chart 7
Customer Support 8
SHI Standard Procedure and Issue Resolution 9
Sales Training 10
Products and Services 15
Distribution 19
Marketing 32
Environmental Initiatives 43
Value Add 47
Disclosures 50
References 50
Question Set 2: Service Questionnaire 52
Sales Data 52
Customer Support 56
Pricing 60
Cooperative Contracts 60
Fees 61

Question Set 1: Company Information

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary additional relevant details for some questions are included here.

1.0.31 Is this business women-owned?

SHI Response:

Yes. SHI is certified by the Women's Business Enterprise National Council (WBENC). Please see our certificate below.



Figure 1: SHI WBENC Certificate

1.0.32 Is this business minority-owned?

SHI Response:

Yes. SHI is certified by the National Minority Supplier Development Council. Please see our certificate below.



THIS CERTIFIES THAT

SHI International Corp.

NMSDC
National Minority Supplier Development Council

* Nationally certified by the: **NEW YORK & NEW JERSEY MINORITY SUPPLIER DEVELOPMENT COUNCIL**

*NAICS Code(s): 423430; 541519

* Description of their product/services as defined by the North American Industry Classification System (NAICS)

02/07/2024
Issued Date

NY03805
Certificate Number

Ying McGuire
NMSDC CEO and President

03/31/2025
Expiration Date

Terrence Clark, President & CEO

By using your password (NMSDC issued only), authorized users may log into NMSDC Central to view the entire profile: http://nmsdc.org

Certify. Develop. Connect. Advocate.

* MBEs certified by an Affiliate of the National Minority Supplier Development Council, Inc.®

Figure 2: SHI MBE Certificate

1.0.33 Does this business have an Affirmative Action plan/statement?

SHI Response:

Yes. As the largest minority woman-owned business in the US, SHI has long supported programs that empower groups facing employment barriers. Our global success is driven by the diversity and inclusion of our team, and we are committed to diversity, equal opportunity, and affirmative action as the foundation of our fair and inclusive workplace. Please see SHI's equal employment opportunity affirmative action plan below.

SHI's Affirmative/EEO Plan

To comply with governmental regulations and the company's Affirmative Action Policy and obligations to employ, retain, promote, terminate, and otherwise treat all employees and job applicants on the basis of merit, qualifications, and competence.

1. A complete up-to-date Personnel Profile of all employees classified by race, sex, and job classification will be maintained, and annual reports will be submitted to the EEOC.
2. All employees will be advised at the time of employment and during the HR orientation that SHI is an equal opportunity/affirmative action employer and that all personnel decisions are based on an individual's qualifications and ability to perform the work.
3. A company policy statement outlining SHI's commitment to equal employment opportunity will be posted on SHI's intranet site, MySHI, as well as within the Handbook. A detailed policy outlining SHI's commitment to affirmative action will be accessible upon request within the Human Resources department.
4. The company has appointed Ellen Mass to serve as the Equal Employment Opportunity/Affirmative Action officer. The EEO/AA officer is authorized to supply reports and represent this company in all matters referenced in this document and regarding the Company's Affirmative Action Plans.
5. The EEO/AA officer will be responsible for the following:
    a. Implementing all phases and requirements of the plan
    b. Conducting quarterly audits of employment practices to ensure nondiscrimination
    c. Providing yearly instruction to supervisors regarding their responsibilities of compliance with Affirmative Action and Equal Employment obligations, ensuring no type of discriminatory practices or harassment are present and all requirements are implemented.
    d. Notification via Job posting (MySHI), SHI newsletter, recruiters to all eligible employees regarding promotions or vacancies to ensure equal employment opportunity.
6. All applicants or employees seeking promotion are reviewed fairly. HR reviews applicant and promotion records with the CEO of SHI to monitor job availability and the recruitment labor area.
7. Training is provided without regard to race, gender, disability status, veteran status, or any other prohibited factor ensuring job opportunities are equally available to all.

Ellen Mass

Ellen Mass, Vice President of Human Resources

5-15-24

Date

These goals are established company-wide and reach each department. They are established for women, minorities, individuals with disabilities, and veterans and are designed to increase availability for greater utilization.

1.0.36 Enter business branch locations, if any. Include address, city, state, zip, phone number for each.

SHI Response:

Please see the graphics and tables for the addresses of SHI's global office and integration center locations on the following pages.

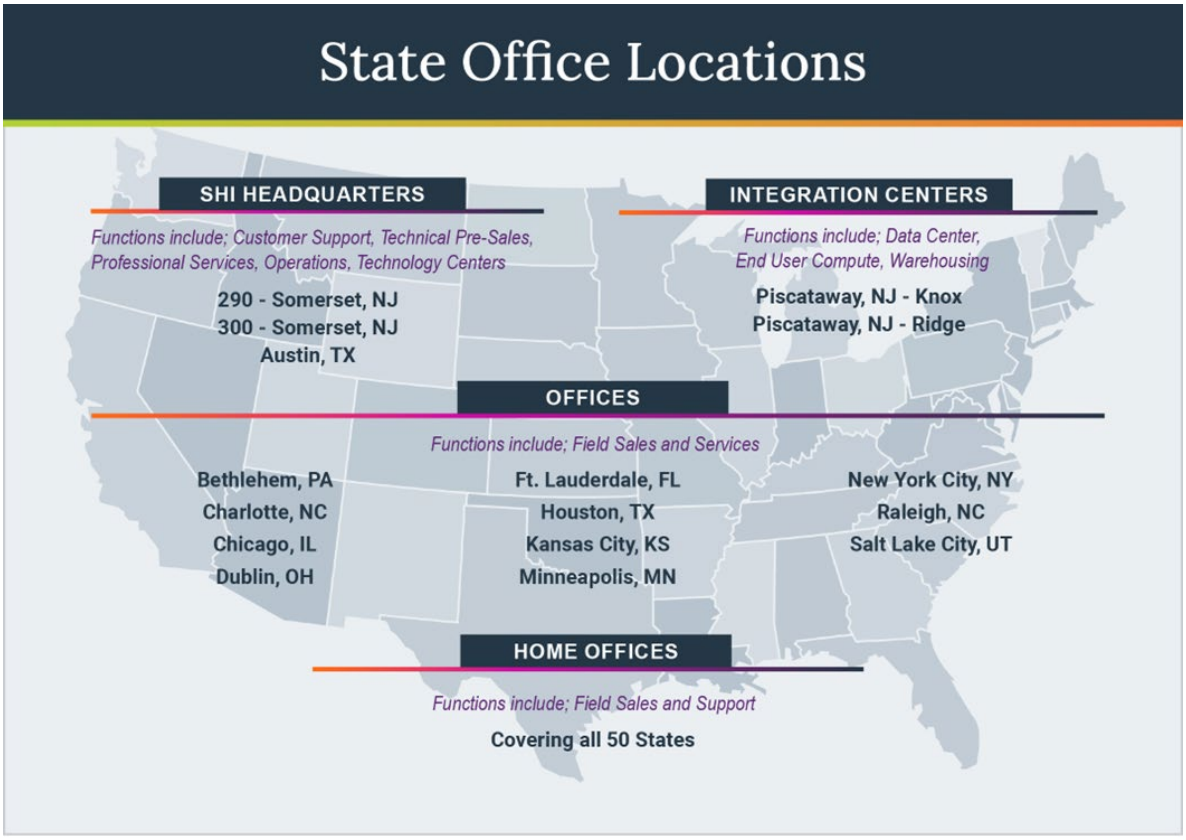


Figure 3: SHI State Office Locations

Table 1: SHI Headquarters and Integration Centers

SHI HEADQUARTERS AND INTEGRATION CENTERS		
LOCATION NAME	**COUNTRY/REGION**	**ADDRESS**
SHI Headquarters – 290	New Jersey	290 Davidson Avenue Somerset, NJ 08873
SHI Headquarters – 300	New Jersey	300 Davidson Avenue Somerset, NJ 08873
SHI Integration Center – Knox	New Jersey	10 Knox Drive Piscataway, NJ 08854
SHI Integration Center – Ridge	New Jersey	400 Ridge Rd Piscataway, NJ 08854
SHI Corporate Call Center	Texas	3828 Pecana Trail Austin, TX 78749

Table 2: SHI US Office Locations

SHI US OFFICE LOCATIONS		
LOCATION NAME	**COUNTRY/REGION**	**ADDRESS**
SHI Bethlehem	Pennsylvania	1605 Valley Center Parkway Bethlehem, PA 18017
SHI Charlotte	North Carolina	101 N. Tryon Street, Suite 500 & 550, Charlotte, NC 28202
SHI Chicago	Illinois	150 North Michigan Avenue, Suite 500 Chicago, IL 60601
SHI Houston	Texas	2000 W. Sam Houston Pkwy South, Suite 800 Houston, TX 77042
SHI Manhattan	New York	One Penn Plaza, Suite 1020 New York, NY 10119
SHI Raleigh	North Carolina	4819 Emperor Boulevard, Suite 210 Durham, NC 27703

Table 3: SHI Global Office Locations

SHI GLOBAL OFFICE LOCATIONS		
LOCATION NAME	**COUNTRY/REGION**	**ADDRESS**
SHI Canada ULC	Canada	325 Front Street W Toronto, Ontario, M5V 2Y1, Canada
SHI International B.V.	Netherlands	Herengracht 124 NL-1015 BT, Netherlands
SHI International Corp Australia Pty. Ltd	Australia	Level 45, 680 George Street, Sydney, New South Wales 2000, Australia
SHI International SAS	France	9-15 Rue Maurice Mallet, 92130 Issy Les Moulineaux, France
SHI International Corp Hong Kong Limited	Hong Kong	29/F, Tower 5, The Gateway, 15 Canton Road, Harbour City, Tsim Sha Tsui, Kowloon, Hong Kong SAR, China
SHI Global IT Solutions Ireland Limited	Ireland	Pembroke House, 28 - 32 Pembroke Street Upper, Dublin, D02 EK84, Ireland
SHI Singapore Solutions Pte. Ltd.	Singapore	One Raffles Place, #20-61 Tower 2, Singapore, 048616
SHI Singapore Solutions Pte. Ltd.	South Korea	Spaces Gran Seoul 7F, Tower1 Gran Seoul, 33 Jong-ro, Jongnogu, Seoul, 03159, South Korea
SHI Corporation UK Limited (HQ)	United Kingdom	401 Grafton Gate, Ground Floor, Milton Keynes, Buckinghamshire, England MK9 1AQ
SHI Corporation UK Limited	United Kingdom	Savoy Tower, 77 Renfrew St, Glasgow G2 3BZ
SHI Corporation UK Limited	United Kingdom	70 White Lion Street, London, N1 9PP
SHI Corporation London Headquarters	United Kingdom	91-93 Farringdon Road, 5th floor, London EC1 3LN

Table 4: SHI Global Integration Centers

SHI GLOBAL INTEGRATION CENTERS		
LOCATION NAME	**COUNTRY/REGION**	**ADDRESS**
Nexus	United Kingdom	Unit 17 Nexus Capitol Court Dodworth, Barnsley S75 3UD
Central Park	France	9-15 rue Maurice Mallet, 92 130 Issy les Moulineaux
Tiel	Netherlands	Tiel, Netherlands, COLO, TechData c/o PDSI, De Geer 2, Tiel 4004 LT, Netherlands
Tampines	Singapore	Tampines, Singapore, COLO, Tech Data AS Pte Ltd, Tampines Industrial Crescent, #06-04/#06-05, Singapore 528605

Sales History

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD).

Key Contacts

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary additional relevant details for a few questions are included here.

1.2.5 Distributors, Dealers, Installers, Sales Reps

SHI Response:

AEPA members will be assigned an account executive for all distribution, dealers and accounting, warranty, or quote-related queries.

The account executive, will provide any contact information, process information, or help escalate with the manufacturer when necessary. Anytime an SHI account executive is out of the office for more than a day, your inside account team will respond to emails, phone calls, and questions left for the dedicated account executive. In addition, your account executive's team of inside account managers is always available to help with any requests. This team of resources is empowered to manage any request or question. Should your inside account managers be unable to answer your question, you will be directed to your account's district manager, who will quickly respond with an answer.

SHI's leadership structure and Public Sector account team organization charts are included below and on the following page. SHI has a very well-defined customer contact, communication, issue escalation, and support path as demonstrated below.

SHI Public Sector Account Team Org Chart

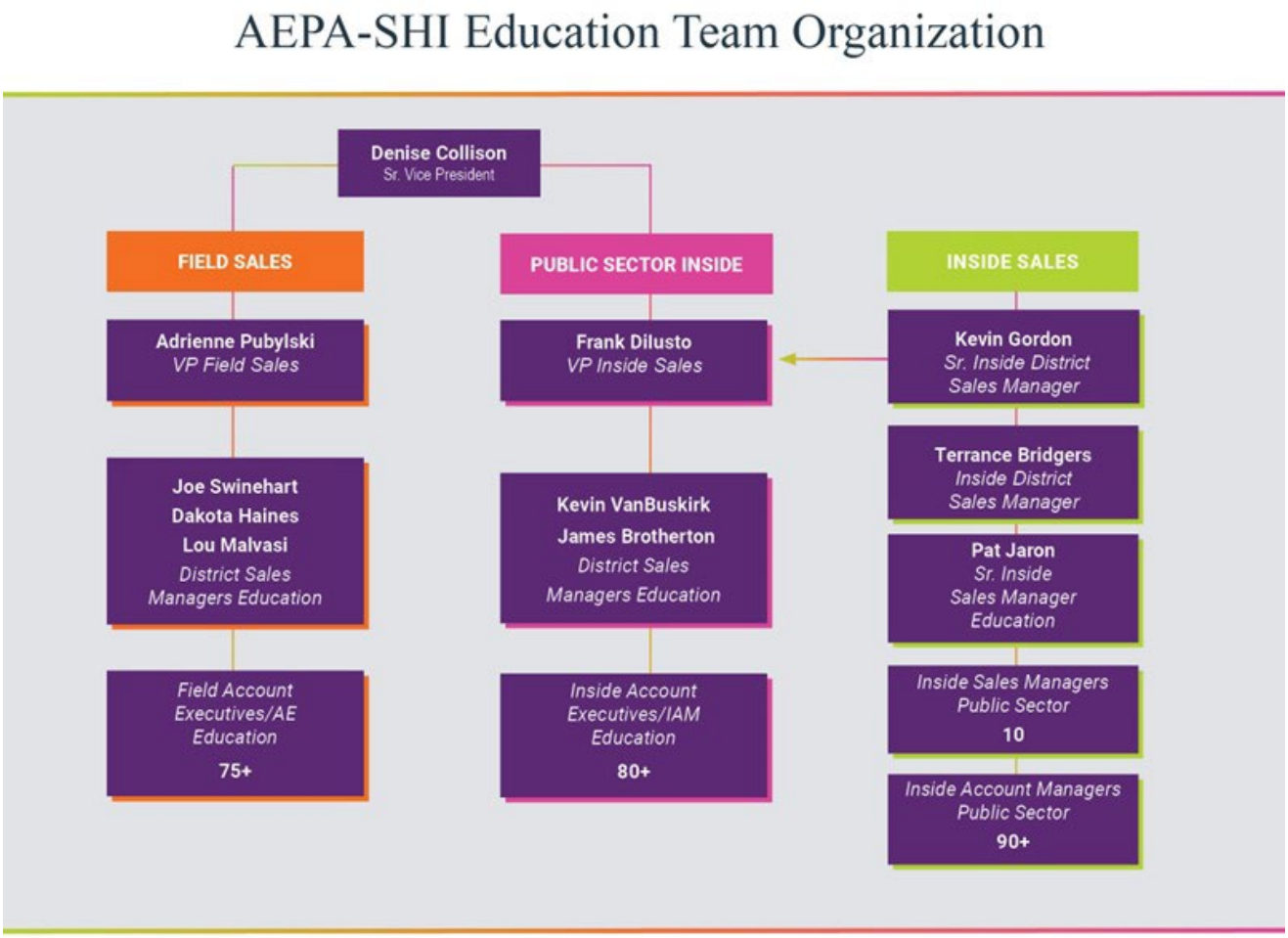


Figure 4: SHI Education Team Organizational Chart

AEPA-SHI Government Team Organization

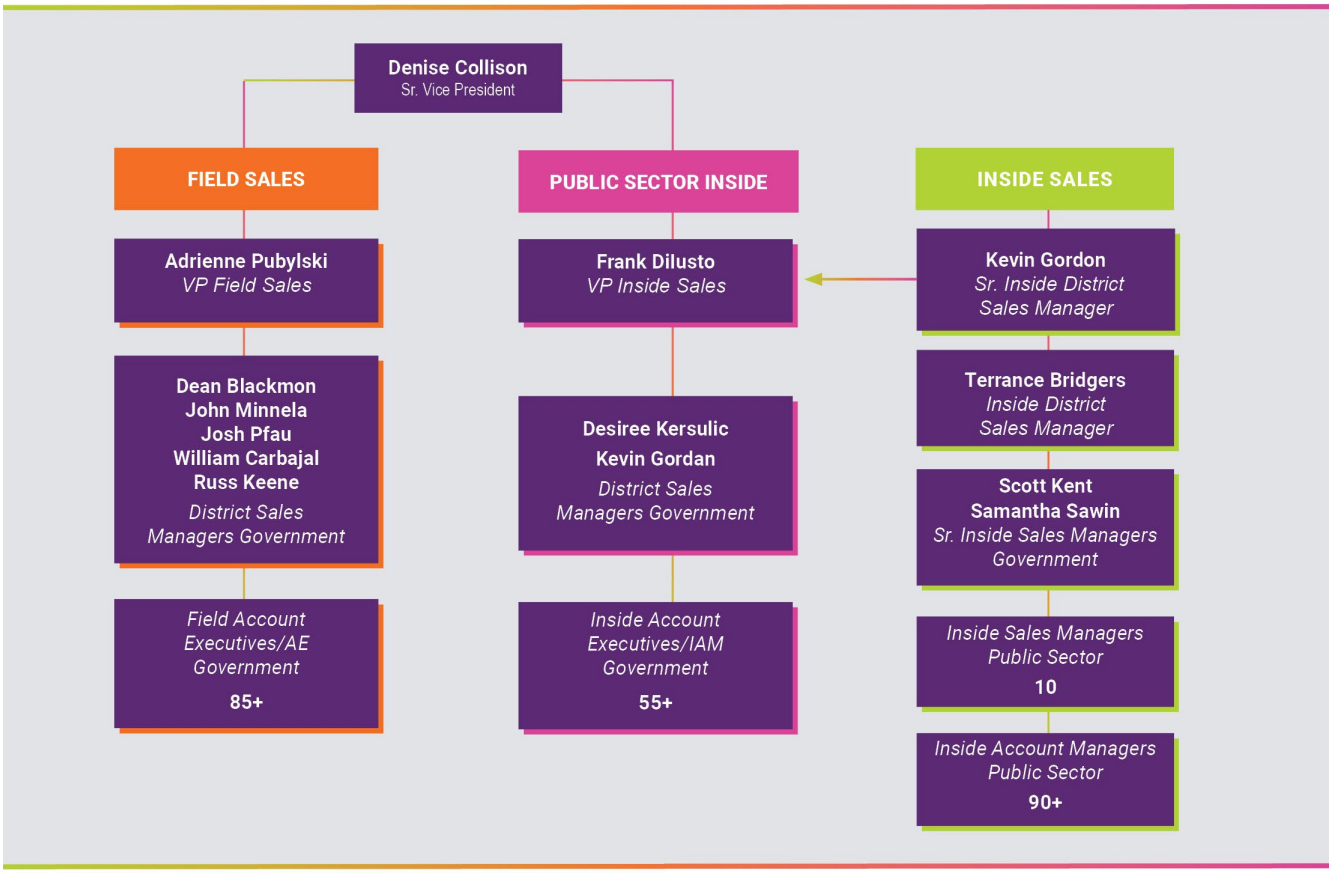


Figure 5: SHI Government Team Organizational Chart

CUSTOMER SUPPORT

Provided below is an overview of SHI's support path for AEPA and member agencies covering standard procedures and accounting.

SHI provides a comprehensive customer support plan to ensure we are meeting each member agency's needs. Members are supported by a dedicated account executive and a dedicated inside sales team. Field territories are structured vertically and geographically. The proposed SLA will include:

A. On-boarding times

B. Types of resources included

C. Tracking communications

D. Follow-up process and timelines

We realize the need for extraordinary responsiveness regarding technical issues, product/solution delivery, billing, and requests regarding Statements of Work. We also understand the need for timely

information communication to keep your projects moving forward. The first step to ensuring success in these areas is to define SLAs that meet member agencies' needs collaboratively and clearly.

SHI's escalation process is simple and straightforward. You may escalate a question to the next level at any time that you feel is appropriate. Also, if necessary, your SHI account team escalates an issue internally for resolution.

ESCALATION PATH

INSIDE ACCOUNT MANAGERS	INSIDE SALES MANAGER/CAPTURE MANAGER	ACCOUNT EXECUTIVE	DISTRICT MANAGER/Sr. CAPTURE MANAGER
Public Sector Ops 888-764-8888	Inside Sales Capture Manager 888-764-8888	Account Executive 888-764-8888	District Manager Sr. Capture Manager 888-764-8888

Figure 6: Escalation Path

SHI Standard Procedure and Issue Resolution

Calls Answered in a Timely Manner: AEPA member agency and AEPA customer calls are directed to the applicable dedicated account team. If the dedicated contact is helping another customer, calls are directed to voicemail. These voicemails are returned within the response times listed in the table on the following page. If the member agency has an urgent request, they can escalate their request to the inside sales team manager or account executive for immediate assistance.

Quotes Turnaround: Quotes from the customer's standard catalog are fulfilled within eight business hours. For quotes requested for items that are third-party source/weird ware items, the inside account managers reply to customer requests within two to four hours, confirming receipt of request and relaying to the customer they are working on their request and notifying them of additional time the request may take because of external factors—such as awaiting vendor response or additional required information from the customer.

Reporting to be provided to AEPA Member Agencies: All standard reports can be set up on a subscription basis and delivered automatically daily, weekly, quarterly, or in whatever frequency members choose. Ad-hoc reporting is available on SHI.com and those timelines may vary.

Onboarding: SHI works quickly to onboard new AEPA member agencies and can, in most cases, do it within 48 hours.

Order Tracking Communication and Follow-up Process:

- SHI accurately enters purchase orders into the system 98 percent of the time based on monthly data.

- Orders are entered in a timely manner (including order confirmation).
- AEPA member agency orders are processed within the agreed-upon SLA. SLAs will vary by partner. For many software publishers and distribution partners, the typical turnaround for electronic license distribution is 24-48 hours. SHI works with these partners on AEPA member agencies' behalf to set expectations for the expected SLAs turnaround for member's licensing standards.

1.2.11 Provide total number and location of salespersons employed by your business in the United States by city and state.

SHI Response:

Please see the table below for a breakdown of SHI's employees by location and also our response to question 2.1.3.

Our sales organization is so vast that we have coworkers in cities across the country and we have 6000 plus total employees within that public sector sales we employ more than 250 salespeople, as well as a breakdown of our overall employee base by office location.

Table 5: SHI US Employees

SHI USA EMPLOYEES	
LOCATION	**EMPLOYEE COUNT**
SHI Headquarters - 290 - Somerset, NJ	1,268
SHI Headquarters - 300 - Somerset, NJ	648
SHI Corporate Call Center - Austin, TX	1,005
SHI Integration Center - Knox - Piscataway, NJ	283
SHI Integration Center - Ridge - Piscataway NJ	150
SHI Bethlehem, PA	67
SHI Chicago, IL	31
SHI Houston, TX	13
SHI New York City, NY	24
SHI Raleigh, NC	9
Customer Site	62
Home Office	2,258

Sales Training

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary relevant details for a few questions are included here.

1.3.1 Describe how your company will implement training and knowledge of the contract with your respective sales force. Furthermore, describe how your company plans to support and train your sales force on a national, regional, or local level and generally assist with the education of sales personnel about the resulting contract.

SHI Response:

SHI will commit to training our sales force on the new AEPA contract immediately upon award, as we understand this will be critical to our mutual success. Within one week of an award, SHI will organize a call that includes Public Sector senior leadership, marketing, sales, and contract personnel from AEPA. We will design a plan to:

- Train and enable all SHI Public Sector field account executives and leadership.
- Train and enable SHI Public Sector inside account executives and leadership.
- Announce contract strategies.
- Facilitate current and prospective agency member market strategy.
- Create ongoing marketing plans.

SHI has a process in place and has successfully launched other similar contracts in the past. We are confident in our abilities to train our sales teams quickly.

Since our account executives in the field are located all over the country, the most efficient way to conduct training and enablement amongst them is through regional webcasts. There are, on average, 30 account executives per region, so this will allow each call to have a more collaborative feel, while also allowing for in-depth discussion and answers.

Once awarded, SHI Public Sector sales and leadership will work with the following people to create and execute this marketing plan:

- Aimee Ballenger, Sr. Director of Contract Capture and Development, Aimee_Ballenger@SHI.com
- Amelia Jakubczyk, Director SLED Contract Capture and Development, Amelia_Jakubczyk@SHI.com
- Chris Dickman, Capture & Business Development Manager, Chris_Dickman@SHI.com

1.3.2 What is your company's plan, if your company were awarded the contract, to service up to 30 states (or the region awarded in a regional bid). Describe if your company has a national sales force, dealer network, or distributor(s) with the ability to call on eligible agencies in the participating states in AEPA.

SHI Response:

Upon award, SHI will coordinate with AEPA representatives on an implementation plan to ensure the successful rollout of our contract. We will engage our extensive internal resources and national salesforce to serve customers in up to 30 states or as awarded by AEPA.

With the largest and most highly certified sales support team in the industry, SHI will act as a trusted advisor to our AEPA customers across the United States. We follow a select, deploy, and manage method that ensures our team's efforts will support their vision, facilitating each project from conception to successful implementation and helping uncover cost savings at all phases of a project lifecycle.

Our dedicated account team approach will be key in executing an effective customer service strategy for all of our AEPA customers. We will customize the team structure to meet the individual needs of each customer. Key stakeholders on a customer's team will collaborate extensively with our account team beginning with onboarding session to understand their needs and requirements, help with the development of the plan to onboard your account, and lead the remaining team members through the implementation. Our team will continue to engage with the customer, providing continued visibility and value throughout our partnership.

Public Sector dedicated field account executives are located locally and are available to meet AEPA customers onsite. Our field account executives are supported by a dedicated team of inside account

managers located in SHI's headquarters in Somerset, NJ. The inside account managers interact with AEPA members responsible for procuring under this contract, developing a personal understanding of their specific needs, and ensure customer satisfaction for your member institutions. Integral daily activities include functional areas such as pricing, availability, order entry, tracking, returns, product information, and expedites. SHI also provides dedicated support for small and midsize entities across the US through our inside account executives located in New Jersey. Their proactive approach to supporting smaller education entities allows SHI to give the best targeted support for all AEPA members across the 50 states. Our team is well educated on the methodology, requirements, and SLAs of contracts like AEPA and provides consistent and efficient support. Together, this team will service as the point of contact for all questions and problem resolution.

The combination of our warehouse/integration centers and our relationships with our leading distributors allows us to provide efficient product delivery across the globe (or nation):

- SHI's warehousing capabilities rely on our SHI-owned and operated facilities and a robust network of distribution partners.
- Our ISO-certified integration centers/warehouses located in Piscataway, NJ, can securely store AEPA member agency inventory for configuration and integration services.
- SHI is proud of our abundant and broad community of distributors and partners. We work loyally to maintain relationships with both our large IT distributors (Ingram Micro, TD SYNNEX, and D&H) and smaller, local distributors and manufacturers directly.
- Our procurement team has sourcing specialists who monitor purchase orders with the partner and distributor community to ensure no savings have been missed.

Public Sector Field Team

The Public Sector Field team supports state and local government, K-12, higher education, federal, and public healthcare entities across the country. Customers in the public sector are supported by an account executive, who lives and works in the territory, and a dedicated inside sales team.

Account executives meet with the participating entities and individual contract users to review their business with SHI. During these review meetings, we discuss purchase history and the customer's plans. With open discussions, SHI can provide significant value in supporting future initiatives and will engage the support teams as needed to help meet the customer's goals and objectives.

The member agency's account executive is supported by a dedicated team of inside account managers in SHI's headquarters in Somerset, NJ. The inside account managers interact with the state teams responsible for procuring under this contract and develop a personal understanding of their specific needs and are responsible for ensuring customer satisfaction.

Public Sector Inside Team

Our Public Sector Inside team focuses on supporting the needs of smaller local government, K-12, and higher education institutions across the country and offers personalized attention regardless of organizational size. Based at our global headquarters in Somerset, NJ, the Public Sector Inside team supports customers' needs from start to finish.

Capture and Strategy

To bring together support for our larger contracts and their users as well as the sales organization, SHI developed a Capture and Development team. This team focuses on ensuring we are educating our

customers and sales about our available contracts as well as being a primary resource for our large contract holders, like AEPA, when there are questions or to discuss future strategy. This team will also be implementing reviews with all customers listed on the AEPA contract. The team will meet with each customer's contracting officer on a quarterly basis. These meetings help ensure contract success not only for SHI but for all AEPA customers by:

- Providing updates on any changes that might impact the contract
- Reviewing contract highlights, such as spend, new customers, new vendors
- Discussing any concerns with the contract
- Identifying areas for improvement
- Sharing our strategies for promoting the contract
- Maintaining and encouraging open lines of communication

To further demonstrate our ability to service all applicable states or regions, we have provided our organizational charts on the following pages. This extensive team can support AEPA members nationally.

SHI Public Sector Account Team Org Chart

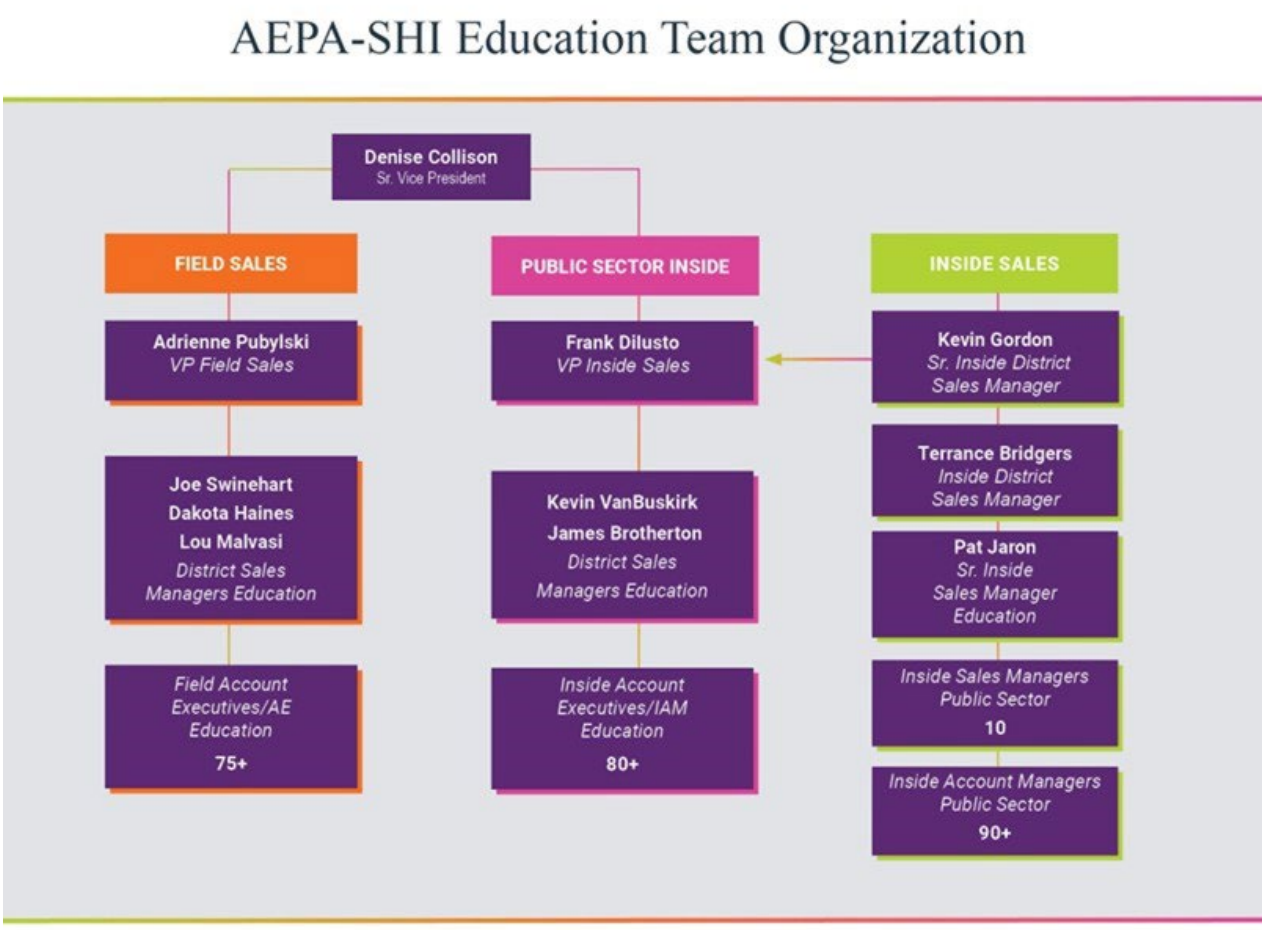


Figure 7: SHI Education Team Organizational Chart

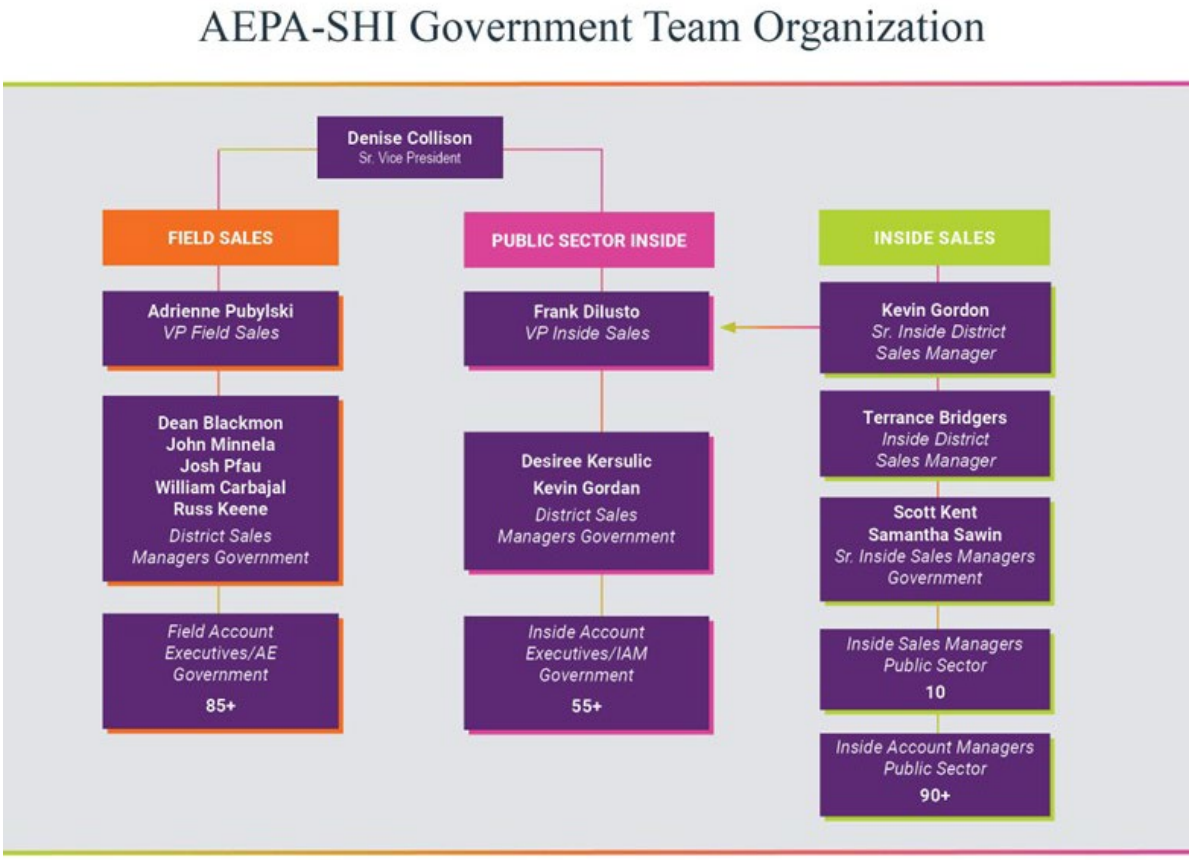


Figure 8: SHI Government Team Organizational Chart

Distribution network

Our major distribution centers are located strategically in:

- Atlanta, GA
- Chicago, IL
- Dallas, TX
- Fontana, CA
- Fort Worth, TX
- Jonestown, PA
- Los Angeles, CA
- Memphis, TN
- Miami, FL
- Ontario, CA
- South Bend, IN
- Suwanee, GA
- Swedesboro, NJ

PRODUCTS AND SERVICES

1.4.1 Provide a description of the Products, Services & Solutions to be provided by the product category set forth in Part B - Specifications. The primary objective is for each Supplier to provide its complete product, service, and solutions offerings that fall within the scope of this solicitation so that participating agencies may order a range of products as appropriate for their needs.

SHI Response:

It is important to ensure all aspects of your environment are covered by a robust cybersecurity strategy. By taking a holistic approach, SHI's Cybersecurity practice can help AEPA member agencies minimize the risk to their organizations, while enabling them to achieve desired objectives. And because SHI will approach each AEPA customer through a vendor-neutral approach, with hundreds of security offerings available, we will be able to match the right solution to their specific needs and requirements. We offer people, technology, and process-focused solutions in data center and cloud security, application security, data-centric security, identity and access management, threat and vulnerability management, and program strategy and operations. The SHI Lab supports vendor comparisons with integration validation for your organizations. SHI Labs has cloud-based lab environments, as well as on premise labs within at our Somerset, New Jersey headquarters. Our laboratory environments are purpose-built to help customers evaluate and implement complex IT solutions quickly. Our labs are all interconnected, showcasing full interoperability between environments. Combined with a cross-functional team of experts and industry-leading partners, we can help you assess, design, and integrate the latest data center, end-user computing, cybersecurity, and cloud technologies.

Our data-supported use-case analysis enables member agencies to deliver on their cybersecurity strategic objectives, achieve cross-departmental consensus, and secure their budget. Our security solutions practice is built around six critical elements of effective security and outcome-driven roadmaps:

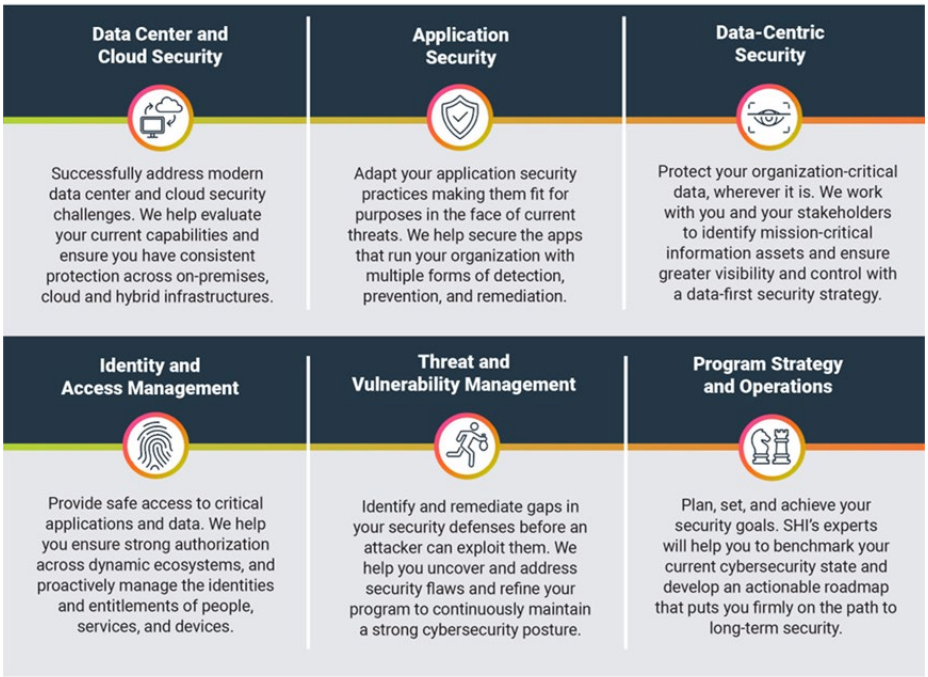


Figure 9: SHI Security Solutions Practice

SHI Cybersecurity Solutions Briefs



SHI provides people, technology, and process-focused cybersecurity solutions to keep you ahead of security threats. Our industry expertise, trusted partnerships, security assessments, and lab-proven integration strategies help you improve your security maturity and manage risk with confidence.

From zero-day to zero trust

SHI cybersecurity solutions enable your teams to provide enterprise risk management as a service across your organization. From establishing strategy with roadmaps and assessments, to solution design including architecture and implementation planning, to creating and maintaining frameworks and programs, our specialists help you achieve your security objectives.

We support your evaluation, selection, and procurement objectives with multiple OEM and purchasing options, and SHI's procurement portals reduce purchasing friction. Our deployment teams deliver integrations, project management, and regular business reviews with partners and account teams.

Address cyber challenges with insight, expertise, and resources

SHI aligns security experts with your strategic objectives, offering SHI Lab data-driven recommendations and a range of market-leading and technology emergent OEMs. Our solutions help you:

- Protect your expanding attack surface
- Automate at scale
- Adhere to regional regulations and governance frameworks
- Base integration/upgrade decisions on lab-proven data
- Improve security maturity, no matter your size
- Simplify your vendor stack with frameworks and programs to deliver business outcomes
- Procure with ease and reduce friction

Stay ahead of the latest threats

From automating your threat detection and remediation to offering insights into leading and emerging technologies, SHI can help.

SHI Labs offer a vendor-neutral analysis of security capabilities specific to your use case, allowing you to rely on data and evidence. You can confidently make procurement, integration, and consolidation decisions based on lab-tested data and optimized costs.

We also provide network security implementation, deployment, and configuration services. Our certified engineers hold deep expertise in Cisco, Fortinet, Microsoft, Okta, and Palo Alto.

Deployment

- Cisco Firewall
- Cisco ISE
- Cisco Meraki Wireless
- Palo Alto Firewall

Assessments

- Cyber Security Assessment Workshop
- Incident Response Tabletop
- Security Posture Review
- Identity Workshop
- Zero Trust Workshop
- DevSecOps Workshop
- Security Roadmap Workshop

SHI Lab PoC

- Identity Program Foundry
- DLP Optimization and Implementation
- Cloud Security Assessment
- Controls Framework Assessment
- DevSecOps Program Advisory
- Data Security and Governance Assessment
- Network Defense Maturity Evaluation

SHI International Corp. \\ SHI.com \\ 888-764-8888 \\ 1

Cybersecurity solutions

Our wide-ranging security portfolio supports the six main components of cybersecurity.

Identity and Access Management	Manage your end-user identity with a robust framework that controls access to critical data, secures profile information, and maximizes data governance.	• Identity Governance Administration (IGA) • Management strategy • IAM active management
Application Security	Incorporate innovative tools at front-end, cloud, and SDLC, and validate effectiveness of tools, integrations, software development, and initiatives.	• Web application firewall • API security • DevSecOps • SDLC: vulnerability detection • Testing: SAST, DAST, RASP • Containerization • Cloud WAAP
Data-Centric Security	Reduce costs, optimize efficiencies, and focus on future growth strategies as SHI helps you navigate the evolving digital landscape.	• Data discovery and classification • Key management • Encryption and database security • Data loss prevention • Data access governance
Data Center and Cloud Security	Protect sensitive data and maintain industry regulatory compliance.	• Next-generation firewall/proxy/intrusion prevention system, and DDoS protection • Network malware analysis/sandbox • Network and remote access control • Cloud security • Privilege account access, data exfiltration, and man-in-the-cloud • Hybrid cloud • Cloud security architecture
Threat and Vulnerability Management	Address vulnerabilities with a risk-based approach, and leverage security automation to increase efficiency.	• Automate remediation • EPP/EDR/MDR/XDR • SIEM • Phishing detection and posture assessment • Attack surface management (as-a-service) • ICS/IoT/SCADA
Program Strategy and Operations	Gain expert guidance on NIST SP 800-53 R5 policies, standards, and procedures, and align with NIST Cybersecurity Framework, ISO 27001/27002, NIST 800-171/CMMC, NIST 800-53, and the Secure Controls Framework (SCF).	• Regulations and frameworks • Operational activities • Incident response and security operations • Cyber Asset Attack Surface Monitoring (CAASM) • SOAR

SHI's unique combination of security experts, partnerships, SHI Labs, and cyber assessments enables confident, data-driven decisions on information security strategy and vendor integrations – so your team can solve what's next in today's ever-evolving cybersecurity landscape.

Learn More

SHI International Corp. \\ SHI.com \\ 888-764-8888 \\ 2

In today's digital age, SHI's Advanced Solutions Group can be AEPA's trusted partner in securing your digital landscape. We understand that cybersecurity is not a one-size-fits-all solution. We can help tailor a robust cybersecurity strategy that aligns with member agencies' unique organizational objectives and risk tolerance.

Our team of dedicated professionals brings the benefits of advanced technology, industry-leading practices, and around-the-clock vigilance. We do not just respond to threats—we proactively identify potential vulnerabilities, offering AEPA member agencies the peace of mind that comes from knowing their digital assets are secure. With Advanced Solutions Group Cybersecurity, member agencies benefit from securing their digital environment, as well as the freedom to focus on driving their organization forward, knowing that their cybersecurity is in expert hands. As such, we have organized our key focus around network and security practices:



Figure 10: SHI's Advanced Solutions Group

SHI is your trusted partner in navigating the complex landscape of digital security. We specialize in providing comprehensive and tailored cybersecurity solutions designed to safeguard an organization's digital assets. The following are a few examples of successful implementations of SHI Cybersecurity services.



Figure 11: Proven Success

DISTRIBUTION

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary relevant details for a few questions are included here.

1.5.4 Provide a list of current subcontractors, distributors, installers, and other independent service providers who are contracted to perform the type of work outlined in this solicitation in the member agency states. Include, if applicable, contractor license or certificate information and the state(s) wherein they are eligible to provide services on behalf of the business.

SHI Response:

SHI offers full IT solutions—from commodity software and hardware procurement and integration to complete, end-to-end data center solutions. Our diverse partner ecosystem supports 15,000 unique publishers and OEMs today. SHI has top-tier authorizations and certifications for every major OEM. The table below represents SHI's sample list of authorized publishers/OEMs and partner status. SHI will

update this list with the AEPA and member agencies on the services part before signing any customer SOW requiring a subcontractor.

Table 6: SHI Authorized Publishers/OEMs and Partner Status

SPARTNER	HARDWARE / SOFTWARE / CLOUD / SERVICES	PARTNER STATUS	SHI RESOURCES
ESET	Software	Silver Partner	1 Presales Partner Specialist 1 Emerging Security Specialist
IBM Software	Software	Silver Business Partner	1 Presales Business Development Manager 2 Presales Partner Specialists
Infoblox	Software	Authorized Partner	2 Emerging Partner Specialists
McAfee	Software	Platinum Partner	1 Business Development Manager 1 Presales Partner Specialist 1 Presales Systems Engineer (ESG)
Microsoft	Software	LSP	Team of 70+ Dedicated Licensing & Ops Specialists Software Assurance Benefits Administrators Product Champions Technical Resources (ESG)
Okta	Software / Cloud	Elite Partner	1 Cloud Partner Manager 2 Presales Cloud Licensing Specialists 2 Emerging Partner Specialists
Proofpoint	Software	Platinum Partner	1 Presales Partner Specialist 1 Emerging Security Specialist
Red Hat	Software	Advanced Business Partner	1 Presales Business Development Manager 2 Presales Partner Specialists
Tableau	Software / Big Data	DMR	1 Presales Partner Specialist
Veeam	Software	Platinum Pro Partner	1 Team Manager 1 Presales Partner Specialist

			1 Presales Business Development Manager
VMware	Hardware	• Corporate Reseller, Premier Level • Partner Professional Services, Enterprise Level • Aggregator, Premier Level • VMware Cloud on AWS Authorized	7 Dedicated Presales Resources 2 Solution Architects 1 System Engineer 5 Business Development Managers 1 Top Partner Manager 1 Support Manager
Alert Logic	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Artic Wolf	Software	National Partner	

PARTNER	HARDWARE / SOFTWARE / CLOUD / SERVICES	PARTNER STATUS	SHI RESOURCES
Atlassian	Software	DMR Partner	2 Emerging Partner Specialists
Autodesk	Software	Volume Channel Partner	1 Presales Business Development Manager Presales Partner Specialists
Avecto	Software	Silver Partner	2 Emerging Partner Specialists
Axway	Software	Partner	
Barracuda Networks	Hardware/Software	DMR Partner	1 Presales Partner Specialist Emerging Partner Specialists
Belkin	Accessories	VIP Level Partnership	1 Dedicated Sales Specialist
Beyond Trust	Software	Silver Partner	2 Emerging Partner Specialists
Birst	Software / Big Data	Partner	1 Big Data Solution Architect
BitDefender	Software	Gold Partner	1 Presales Partner Specialist
Bitglass	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
BitTitan	Software / Cloud	Partner	1 Cloud Partner Manager Presales Licensing Specialists

Blancco	Software	Partner	2 Emerging Partner Specialists
Bluebeam Software, Inc.	Software	Driver Level Partner	2 Emerging Partner Specialists
BMC	Software	Bronze Level Partner	2 Emerging Partner Specialists
Box	Software / Cloud	Premier Level Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
C2G	Accessories	Platinum Partner	1 Presales Cabling & Accessories Specialist
CA (Now part of Broadcom)	Software	LAR - Platinum Partner	1 Team Manager 1 Presales Partner Specialist Emerging Partner Specialists
Carbon Black (Now part of Vmware)	Software	Premier Partner	2 Emerging Partner Specialists
Carbonite	Software / Cloud	Premier Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Centrify	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Checkmarx	Software	Checkmarx Plus Partner	2 Emerging Partner Specialists
Checkpoint	Software	3-Star National Reseller	1 Presales Partner Specialist
Cherwell	Software	Fulfillment Alliance Partner	2 Emerging Partner Specialists
Citrix	Software	Platinum Partner (US) Silver Partner (UK)	2 Presales Business Development Managers 2 Presales Partner Specialists
Cloudera	Software / Big Data	Partner	1 Big Data Solution Architect
Code 42	Software	Preferred Premium Partner	2 Emerging Partner Specialists
Cofense (formerly PhishMe)	Software	Gold Partner	2 Emerging Partner Specialists
Commvault	Software	Market Builder (Commvault Advantage Partner Program)	1 Presales Partner Specialist 1 Presales Systems Engineer
Condusiv	Software	Partner	2 Emerging Partner Specialists
Contrast Security	Software	Silver Partner	2 Emerging Partner Specialists
Corel	Software	Platinum Partner	2 Emerging Partner Specialists

Couchbase	Software	Authorized Reseller	2 Emerging Partner Specialists
CrowdStrike	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
CyberArk	Software	Partner	2 Emerging Partner Specialists
Cybereason	Software	Preferred Partner	2 Emerging Partner Specialists
Cylance	Software	National Partner	1 Presales Partner Specialist
Dark Trace	Software	Partner	2 Emerging Partner Specialists
DataDog	Software	Partner	
Datawatch	Software	Partner	
DbVis Software	Software	Partner	
Dell/EMC	Hardware	Dell EMC Titanium Black (Highest Level Attainable) # of Years Authorized: 15+	12 Dedicated Sales Specialists 4 Dedicated Business Development Managers 1 Technical Specialist 1 Systems Engineer 1 Programs & Marketing Specialist 2 Operations Specialists Team Managers 1 Support Manager 1 Top Partner Manager Plus 25+ Dedicated Dell EMC -badged Resources
DialPad	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Docker	Software	Partner	2 Emerging Partner Specialists
DocuSign	Software	Partner	2 Emerging Partner Specialists
DropBox	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Druva	Software	Certified National	1 Specialist
Duo Security	Software	Partner	2 Emerging Partner Specialists
Dynatrace	Software / Cloud	Authorized Reseller	Cloud Partner Manager Presales Cloud Licensing Specialists
Edifecs	Software	Partner	
Egnyte	Software	Preferred Partner	1 Presales Specialist
Elastic Search	Software	Partner	2 Emerging Partner Specialists

Embarcadero Technologies	Software	Partner	
Ergotron	Accessories	Partner	1 Presales Cabling & Accessories Specialist
Erwin	Software	Diamond Level Partner	1 Presales Specialist
ESET	Software	Silver Partner	1 Presales Partner Specialist 1 Emerging Security Specialist
Extensis	Software	Partner	2 Emerging Partner Specialists
Fire Eye	Software	Platinum Partner	1 Presales Partner Specialist
Firemon	Software	Gold Partner	2 Emerging Partner Specialists
Forcepoint	Software	Platinum Partner	1 Presales Partner Specialist
Fortinet	Hardware/Software	Expert Level Partner	1 Presales Partner Specialist
Fuze	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
GFI	Software	Partner	2 Emerging Partner Specialists
Globalscape	Software	Gold Partner	2 Emerging Partner Specialists
Google	Software / Cloud	Premier Partner	1 Presales Partner Specialist Presales Cloud Licensing Specialists
HashiCorp	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Hortonworks	Software / Big Data	Partner	1 Big Data Solution Architect
IBM Software	Software	Silver Business Partner	1 Presales Business Development Manager Presales Partner Specialists
Idaptive (Under Centrify)	Software / Cloud	VAR	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Imperva	Software	Gold	2 Emerging Partner Specialists
INAP (SingleHop)	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Incipio / Griffin	Accessories	Partner	1 Presales Cabling & Accessories Specialist
Infoblox	Software	Authorized Partner	2 Emerging Partner Specialists

Informatica	Software / Cloud	Tier 1 Reseller	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Information Builders	Software / Big Data	Partner	1 Big Data Solution Architect
Infragistics Inc	Software	Partner	2 Emerging Partner Specialists
Infrascale	Software / Cloud	National Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Intuit	Software	Elite Partner	2 Emerging Partner Specialists
Ivanti **Landesk** **Shavlik** **Appsense** **Wavelink** **Heat Software** **RES Software**	Software	National Sales Partner - Platinum Level	1 Presales Partner Specialist
Jabra	Accessories	Premier Partner	Internal Jabra Team 1 Presales Cabling & Accessories Specialist
JAMF Software	Software	Gold Partner	1 Presales Specialist - Mobility Solutions
Juniper Networks	Hardware	Elite Partner	2 Networking Sales Specialists
Kaspersky	Software	Platinum Partner	2 Emerging Partner Specialists
Kensington Computer Products Group	Accessories	Authorized Partner	1 Peripherals & Accessories Specialist
Kepware Technologies	Software	Partner	
KnowBe4	Software	DMR Partner	2 Emerging Partner Specialists
LANDESK	Software	National Sales Partner - Premier Level	1 Presales Specialist
Lightspeed Systems	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
LogicMonitor	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Logitech	Accessories	Authorized Partner	1 Cabling & Accessories Sales Specialist
LogMeIn	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists

LogRhythm	Software	Platinum Partner	1 Presales Partner Specialist 1 Emerging Security Specialist
Lookout	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Malwarebytes	Software	Platinum Partner	1 Presales Partner Specialist
MAPR	Software / Big Data	Partner	1 Big Data Solution Architect
MathWorks	Software	Partner	
Matrikon	Software	Partner	
McAfee	Software	Platinum Partner	1 Business Development Manager 1 Presales Partner Specialist 1 Presales Systems Engineer (ESG)
Micro Focus	Software	Platinum Partner	1 Partner Manager 1 Presales Specialist
Micron	Hardware	Partner	Memory Team
Microsoft	Software	LSP	Team of 70+ Dedicated Licensing & Ops Specialists Software Assurance Benefits Administrators Product Champions Technical Resources (ESG)
Mimecast	Software / Cloud	Elite Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Mindjet	Software	Partner	1 Presales Specialist
Minitab	Software	Partner	2 Emerging Partner Specialists
MobileIron	Hardware/Software	Iron Level Authorization	1 Presales Partner Specialist
MongoDB	Software	Authorized Reseller	2 Emerging Partner Specialists
Morpheus	Software	Partner	
Nasuni	Software / Cloud	Platinum Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
NetIQ	Software	Gold Partner	
Netmotion Wireless	Software	Gold Partner - Tier 1 NSP	2 Emerging Partner Specialists
Netskope	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
New Relic	Software	Preferred Partner	2 Emerging Partner Specialists

Nexthink	Software	Partner	2 Emerging Partner Specialists
Nitro	Software	Premiere Partner	2 Emerging Partner Specialists
Northcraft Analytics	Software	Partner	
Nuance	Software	Authorized Reseller	2 Emerging Partner Specialists
Okta	Software / Cloud	Elite Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists 2 Emerging Partner Specialists
OneLogin	Software / Cloud	Top Tier Strategic Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
OpenText	Software	Partner	2 Emerging Partner Specialists
Oracle	Software	Platinum Partner	1 Presales Partner Specialist 1 Solutions Architect Software Technical Sales Representatives 1 Hardware Technical Sales Representative
Otterbox	Accessories	Partner	1 Presales Cabling & Accessories Specialist
Pagerduty	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Palo Alto Networks	Hardware/Software	Platinum Level Reseller	Business Development Manager 1 Presales Specialist Networking Sales Specialists
Parallels	Software	Premier Partner	1 Presales Partner Specialist
Pentaho (Hitachi)	Software / Big Data	Partner	1 Big Data Solution Architect
Ping Identity	Software	Partner	
Pivotal	Software / Big Data	Partner	1 Big Data Solution Architect
Platfora	Software / Big Data	Partner	1 Big Data Solution Architect
PrinterLogic	Software	Partner	
Progress Software (former	Software	Titanium Partner	1 Presales Partner Specialist
Proofpoint	Software	Platinum Partner	1 Presales Partner Specialist 1 Emerging Security Specialist
Pulse Secure	Software	Secure Plus Partner	2 Emerging Partner Specialists

Puppet Labs	Software	Gold Partner	2 Emerging Partner Specialists
Qlik	Software	Partner	2 Emerging Partner Specialists
Qualys	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Qubole	Software / Big Data	Partner	1 Big Data Solution Architect
Quest Software	Software	Platinum Plus Partner	1 Dedicated Manager 1 Presales Partner Specialist
Rackspace	Software	Partner	
Rapid 7	Software	Gold Partner	2 Emerging Partner Specialists
RealVNC	Software	Partner	
Red Hat	Software	Advanced Business Partner	1 Presales Business Development Manager Presales Partner Specialists
Redgate	Software	Partner	2 Emerging Partner Specialists
RingCentral	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Rockwell Automation	Software	Partner	
RSA	Software	Titanium DMR	1 Presales Business Development Manager 1 Presales Partner Specialist 1 Systems Engineer (ESG)
Rstudio	Software	Partner	
Safeware	Services	Partner	1 Presales Specialist
SAP/Business Objects	Software / Big Data	Large Account Reseller	1 Big Data Solution Architect
SAS	Software / Big Data	Partner	1 Big Data Solution Architect
Seagull Scientific	Software	Partner	2 Emerging Partner Specialists
Security Scorecard	Software	Premier Partner	2 Emerging Partner Specialists
Sentinel One	Software	Platinum Partner	2 Emerging Partner Specialists
ServiceNow	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
SiloBreaker	Software	Registered Partner	2 Emerging Partner Specialists

Skybox Security	Software	Silver Partner	2 Emerging Partner Specialists
Skytree	Software / Big Data	Partner	1 Big Data Solution Architect
Smartbear Software	Software	Authorized Reseller	2 Emerging Partner Specialists
SolarWinds	Software	Authorized Partner	1 Presales Partner Specialist
SonicWALL	Software	DMR Platinum Partner	1 Presales Partner Specialist
Sophos	Software	National Partner	1 Presales Partner Specialist Presales Business Development Managers
Sparx Systems	Software	RE3 Level Reselling Partner (Highest Level)	2 Emerging Partner Specialists
Splunk	Software / Big Data	Elite Partner	1 Presales Partner Specialist
StarTech.com	Accessories	Authorized Partner	1 Peripherals & Accessories Specialist
STEALTHBits	Software	Tier 1 Partner	2 Emerging Partner Specialists
StorageCraft	Software	Premier Partner	2 Emerging Partner Specialists
SUSE	Software	National Partner	1 Presales Partner Specialist
Symantec	Software	Platinum Partner	3 Presales Business Development Managers 1 Team Manager 3 Presales Partner Specialists 1 Presales Operations Specialist
Tableau	Software / Big Data	DMR	1 Presales Partner Specialist
Tanium	Software	Velocity Partner Program	2 Emerging Partner Specialists
Targus	Accessories	Authorized Partner	1 Peripherals & Accessories Specialist
TBI	Software / Cloud	Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists 1 Solution Specialist, Colocation Services
TeamViewer	Software / Cloud	Platinum Level Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
TechSmith	Software	Tier 1 Partner	2 Emerging Partner Specialists

Tenable	Software	Platinum Partner	1 Presales Partner Specialist
Teradata	Software / Big Data	Partner	1 Big Data Solution Architect
Thales - Vormetric	Software	Partner	2 Networking Sales Specialists
Think-Cell	Software	Reseller	2 Emerging Partner Specialists
Thousand Eyes	Software	Partner	2 Networking Sales Specialists
Thycotic	Software	Authorized Partner	1 Presales Partner Specialist
Tibco	Software	Strategic Reseller Partner	2 Emerging Partner Specialists
Tracker Software	Software	Partner	2 Emerging Partner Specialists
Trend Micro	Software	National Channel Partner	1 Presales Partner Specialist
Tripwire	Software	Gold Partner	2 Emerging Partner Specialists
Tufin	Software	Authorized Reseller	2 Emerging Partner Specialists
Turbonomic	Software	Platinum Partner	2 Emerging Partner Specialists
Turtle & Hughes	Software	Partner	
Unitrends	Software	Star Partner	1 Presales Partner Specialist
Vandyke Software	Software	Partner	2 Emerging Partner Specialists
Varonis	Software	Silver Partner	2 Emerging Partner Specialists
Veeam	Software	Platinum Pro Partner	1 Team Manager 1 Presales Partner Specialist 1 Presales Business Development Manager
Veracode	Software	Platinum Partner	2 Emerging Partner Specialists
Veritas	Software	Platinum Partner	1 Team Manager 1 Presales Business Development Manager Presales Partner Specialists
Vertica	Software / Big Data	Partner	
Vidyo	Software	Partner	2 Networking Sales Specialists
Watchguard Technologies	Hardware/Software	National Partner	2 Emerging Partner Specialists
Websense	Software	US Platinum DMR Partner	1 Presales Specialist

Workshare	Software	Partner	
Zendesk	Software / Cloud	1st National Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Zerto	Software / Cloud	Platinum Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists
Zoho Corporation	Software	Partner	2 Emerging Partner Specialists
Zoom Video Communications	Software	Partner	2 Networking Sales Specialists
Zyxel Communications Corp	Software / Hardware	Partner	
Zscaler	Software / Cloud	Gold Partner	1 Cloud Partner Manager Presales Cloud Licensing Specialists

1.5.6 If applicable, describe other ways your company can be sensitive to a participating agencies desire to utilize local and/or MWBE companies, such as the number of local employees and offices with a geographic region, companies your firm uses that may be local (i.e. delivery company), your own company's diversity of owner employees, etc.

Local Representation

SHI supports customers from our Somerset, NJ, global headquarters and from several offices throughout the US, and our sales leadership team and account executives live regionally in the areas that they support. Notably, SHI has local coverage in 48 states.

Use of Local Companies

With our expansive national network, SHI is able to effectively identify local companies with local employees in a customer's region. We are committed to supporting AEPA member agencies in their initiatives to leverage local partners whenever possible, based on the needs of individual projects.

Diversity of Ownership and Employees

Under the leadership of Co-Founder Thai Lee, who has served as our only President and CEO, SHI has organically grown since its founding in 1989 into the largest minority and women-owned business in the United States. Additionally, SHI has long supported programs that empower groups facing employment barriers. We believe that SHI's global success is driven by the diversity and inclusion of our team, and we are committed to diversity, equal opportunity, and affirmative action as the foundation of our fair and inclusive workplace.

SHI's most important asset is our diverse community of employees. We appreciate the unique experiences, knowledge, innovation, and talents they bring and promote an inclusive culture that encourages employees to express their diverse backgrounds and ideas throughout the organization. SHI aims to attract, develop, and maintain a diverse workforce. We attend diversity job fairs and collaborate with hiring partners prioritizing diversity and inclusion. All employees at SHI are expected to treat each other respectfully and promote inclusivity in all work-related activities. Our employees have established employee resource groups to enhance our community, promote a sense of belonging, and celebrate

diversity. All employee resource groups have an executive sponsor from SHI's senior leadership who actively participates in all employee resource group events and discussions.

At SHI, we prioritize creating a respectful environment where equal job opportunities are available to all employees and applicants. As our employees' and customers' priorities change, we constantly review our objectives against diverse perspectives. Our ongoing diversity, equity, and inclusion strategies encompass robust talent acquisition and retention, diversity, equity, and inclusion training for our staff, and inclusive communication practices. We remain committed to fostering and uplifting our community of employees, partners, and diverse suppliers supporting the customers we serve daily.

Supplier Diversity

Committed to economically strengthening diverse-owned businesses, over the last 20 years, SHI's supplier diversity program has enhanced our presence in the minority business community and grown our diversity business development program. We have an executive-level role with a dedicated team that handles supplier diversity matters. Our supplier diversity program fosters relationships with diverse-owned companies, aligning with SHI's core values. We view diverse suppliers as vital for our success, helping us consciously source products and services while maintaining profits, growing our customer base, boosting the economy, and promoting innovation. SHI sponsors and supports more than 50 supplier diversity-related events annually.

SHI's diversity initiatives—influenced in part by our status as the country's largest minority and women-owned enterprise—will align with customers whose strategic business objectives include supplier diversity and development. Our expansive national diversity supplier network affords us the ability to effectively identify local companies with local employees in a customer's region. SHI continues to increase the number of diverse suppliers in SHI's Managed Partner Network.

As many of our customers pursue supplier diversity programs, SHI plays a vital role as a primary vendor or Tier 1 supplier to many of our major business segment customers today. We provide Tier 1 quarterly reports to more than 200 customers today. We continue to grow an effective Tier 2 program that complements their goals by accessing our services partner database utilizing qualified, certified minority, women, veteran, and disabled/small disadvantaged/HUBZone-owned businesses. By customer request, SHI currently tracks and reports Tier 2 direct and Tier 2 indirect spend for more than 375 of our customers each quarter. These reports include breakdowns by diverse-owned business categories, including ethnicity, race, and gender classifications.

MARKETING

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary relevant details for a few questions are included here.

1.6.1 Key Marketing Contact(s): List the name(s), title(s) and contact information of the business's key national and regional marketing office(s).

SHI Response:

The key marketing contacts are listed below. Once awarded, SHI's Public Sector Sales and leadership will work with the following people to create and execute this marketing plan:

- Aimee Ballenger, Sr. Director of Contract Capture and Development, Aimee_Ballenger@SHI.com
- Amelia Jakubczyk, Director SLED Contract Capture and Development, Amelia_Jakubczyk@SHI.com
- Chris Dickman, Capture and Business Development Manager, Chris_Dickman@SHI.com

1.6.2 Describe how this business marketed its products and services to schools, nonprofit organizations, and other public sector audiences for the most recent full year. List all conventions, conferences, and other events at which this company exhibited.

SHI Response:

SHI actively participates in trade shows, conferences, and meetings across the country in order to market our products and services to public sector audiences. The following is a listing of events we have or will take part in this year:

Alabama: ACCS-ISA Conference 2024, ALET Fall Symposium 2024, Alabama Digital Government Summit 2024

Alaska: Alaska Digital Government Summit 2024

Arizona: AzTEA CI & IT Symposium 2024, Arizona Digital Government Summit 2024, K-12 Arizona CIO/CTO Forum 2024, The Copper Chapter of NIGP Reverse Trade Show 2024

Arkansas: Arkansas Local Government Summit 2024, Arkansas Municipal League Conference 2024, Arkansas Digital Government Summit 2024

California: ViVE 2024, UDEL Supplier Diversity Conference 2024, Los Angeles IT Leadership Forum 2024, CISOA Technology Summit 2024, California Public Sector CIO Academy 2024, RTM Spring CIO Congress 2024, RTM Spring Higher Education CIO Congress 2024, California Community Colleges Purchasing Conference 2024, CSU Business Conference 2024, Los Angeles Digital Government Summit 2024, California Government Innovation Summit 2024, Process Palooza 2024, Bay Area Digital Government Summit 2024, MISAC Annual Conference 2024, AICCU Annual Meeting 2024, CollegeBuys Nothern Regional Fall Forum 2024, San Diego Google Event, UCTech Conference 2024, RTM Fall Government IT Congress 2024, RTM Healthcare Tech Congress 2024, CHIME Fall Forum Charity Golf Tournament 2024, CHIME Fall Forum Networking Yacht Reception 2024, CITE 2024

Colorado: CGAIT Summer Conference 2024, ISTE 2024, Colorado Digital Government Summit 2024

Connecticut: CEN Member Conference 2024

Florida: FETC 2024, RTM East CIO Congress 2024, CHIME Innovation Summit on AI 2024, Florida Digital Government Summit 2024, South Florida HIMSS Scholarship and Fundraiser Golf Tournament 2024, Florida Association of MIS Annual Conference 2024, FLGISA 2024, HealthTrust University Conference 2024, Florida Public Sector Cybersecurity Summit 2024, FAEDS 2024

Georgia: Paulding County Schools IT Leadership Meeting 2024, Georgia Occupational Award of Leadership Banquet 2024, Georgia Digital Government Summit 2024, Georgia Higher Education IT Leadership Summit 2024, Georgia GMIS Fall Conference 2024

Hawaii: Hawaii Digital Government Summit 2024, SPOCon VI 2024, Schools of the Future Conference 2024

Illinois: IPEC Annual Conference 2024, Illinois Digital Government Summit 2024

Indiana: Indiana Public Sector Cybersecurity Summit 2024, Indiana Digital Government Summit 2024

Iowa: Iowa Digital Government Summit 2024

Kansas: Kansas Public Sector Cybersecurity Summit 2024, Check Conference 2024, Kansas Digital Government Summit 2024

Kentucky: KySTE 2024

Louisiana: NASCIO Annual Conference 2024, LONI Summit 2024, Louisiana Digital Government Summit 2024, TECH COOKOFF - Technology Expo & Food Fight 2024

Maine: Maine Digital Government Summit 2024

Maryland: NASCIO Midyear Conference 2024, Leidos Supplier Innovation & Technology Symposium 2024, Maryland Digital Government Summit 2024, RTM Summer Higher Education CIO Congress 2024, The Coalition for Government Procurement Golf Tournament 2024, Air Space Cyber Conference 2024

Massachusetts: Harvard IT Summit 2024, Sophos & SHI New England Public Sector Worcester Red Sox Game 2024, Massachusetts Digital Government Summit 2024

Michigan: Michigan Higher Education IT Leadership Summit 2024

Minnesota: Minnesota State IT Conference 2024, Circuit IT Conference (CITC) 2024, Minnesota Digital Government Summit 2024

Missouri: Gateway to Innovation 2024, Missouri Digital Government Summit 2024, JREID INDEED Celebrity Golf Tournament 2024, Digital Health KC Annual Event 2024

Nebraska: Nebraska Educational Technology Association 2024

Nevada: Nevada Public Sector Cybersecurity Summit 2024, TribalNet Conference 2024, Vizient Connections Summit 2024, PurchNevada 2024, Nevada GMIS 2024, SIM Las Vegas Golf Tournament 2024, Nevada Digital Government Summit 2024

New Jersey: TECHSPO 2024, EdgeCon Winter 2024, NJ Edu Extravaganza 2024, EdgeCon Spring 2024, NJ-GMIS TEC 2024, NJSBA's Women's Leadership Conference 2024, NJAC Annual Conference 2024, New Jersey Digital Government Summit 2024, Police Security Expo 2024, Michael Dessino Memorial Annual Golf Outing 2024, Passaic County NJ Fair Sponsorship 2024, NJ GMIS Cybersecurity Mini Conference 2024, NJ/NYC Higher Ed ITL Summit 2024, EdgeCon Fall 2024, NYC Diverse Summit at SHI HQ 2024, NJSBA Workshop 2024, NJLM Annual Conference 2024

New Mexico: New Mexico Digital Learning Conference 2024, Tech Time Conference 2024, New Mexico Tech Summit 2024, CNM ITS Cybersecurity Fair 2024

New York: NYSLGITDA Spring Conference 2024, NY State Forum Membership 2024, NYS Cybersecurity Conference 2024, SUNY Technology Conference 2024, CUNY MWBE and SDVOB Procurement Conference 2024, Spirit of Pace University Awards 2024, Northeast Supplier Diversity Summit 2024, NMSDC Partnership Awards Gala 2024, New York Digital Government Summit 2024, NYSERnet Conference 2024, NYSGLITDA Fall Conference 2024, New York ServiceNow Government Forum 2024, New York City Technology Forum 2024

North Carolina: NASTD South/East Regional Seminar 2024, NCLGISA 2024, North Carolina Digital Government Summit 2024, NIGP Forum 2024, Southeast Regional Supplier Diversity Summit 2024, UNC CAUSE 2024, NCLGISA Fall Symposium 2024

Ohio: Ohio Higher Education Computing Conference 2024, Great Lakes Region NAEP Conference 2024, Ohio Digital Government Summit 2024

Oklahoma: CPN Gaming Golf Tournament 2024, Oklahoma Digital Government Summit 2024

Oregon: Oregon Digital Government Summit 2024

Pennsylvania: PETE&C 2024, Federal Courts Only Courtroom Technology Conference 2024, Penn State Diversity Fair 2024, Penn State Tech Web Pros Conference 2024, 2024 Cybersecurity Summit, Pennsylvania Digital Government Summit 2024, Pittsburgh E-Arena 2024

Rhode Island: NERCOMP Annual Conference 2024, OSHEAN Member Forum 2024, Providence College Field Event with Dell 2024

South Carolina: SCITDA Spring Leadership Meeting 2024

Tennessee: Tennessee Digital Government Summit 2024, TETA Summer Institute 2024, Tennessee Educational Technology Annual Conference 2024

Texas: UTRGV HUB Vendor Fair 2024, TCEA 2024, Texas A&M University System Tech Summit 2024, TAGITM 2024, DIR Information Security Forum 2024, TASSCC Technology Education Conference 2024, TXST Spring Vendor Fair Showcase 2024, UTINFOSEC Spring Conference 2024, Texas Regional HIMSS Conference 2024, Region One ESC Technology Conference 2024, Texas Digital Government Summit 2024, TASSCC Annual Conference 2024, EDUCAUSE 2024, CPS Energy GrillsGiving 2024, Texas Higher Education IT Leadership Summit 2024, Texas IT Leadership Forum 2024

Utah: NIGP Reverse Tradeshow 2024, Utah Digital Government Summit 2024, CHIME CXO Leadership Academy 2024

Virginia: Beyond the Beltway 2024, Run the Greenway 2024, Gov Exec Defense One Tech Summit 2024, COVITS 2024, SHLB Conference 2024, ATARC Federal Zero Trust Summit 2024, ATARC Federal CIO Summit 2024

Washington: NLIT Summit 2024, ACPE 2024, Washington AWS Data Summit 2024, Washington Technology Power Breakfast - Doing Business with NASA 2024, Washington Technology Power Breakfast - Doing Business with DHS, Washington Digital Government Summit 2024

Washington, DC: GovLoop AI in Action 2024, Beyond Earth: The View from Space 2024, Google Public Sector Summit 2024

Wisconsin: BrainStorm 2024, Marquette University Supplier Fair 2024

Other/Virtual: CISOA Partners in Education Program 2024, NJAC Cybersecurity Scholarships 2024, Lenovo AMD Virtual End of Quarter Celebration 2024, IPMA 2024, NC Tech Annual Membership 2024-2025, This Week Health Subscription and Event 2024, Washington Technology Power Breakfast: Doing business through GWACS, MAS, OTAS

1.6.3 Describe how your company will market the resulting contract to eligible Member Agencies. Describe how your company differentiates the new agreement from existing contracts that your company may hold today. Please be specific and detailed in your response.

SHI Response:

SHI understands the critical importance of both internal and external marketing in determining the success of our AEPA contract. We also have a deep understanding of the unique requirements of procurement organizations like AEPA, along with extensive experience in supporting the needs of customers like your member agencies.

Upon award, our dedicated Contract Capture and Strategy, Public Sector leadership, and Public Sector Marketing teams will collaborate along with AEPA in the creation and rollout of a marketing plan to reach eligible member agencies. While we will draw on our extensive experience in holding and marketing

numerous cooperative and group purchasing organization contracts, the details of this plan will be unique and based specifically on the goals of AEPA and the needs of your member agencies.

We will execute the following steps to begin marketing the new contract:

- Create contract announcement materials for electronic distribution to customers via email, on SHI.com, and the SHI Resource HUB blog, posts on LinkedIn and other social media.
- Create co-branded marketing outlining the features of the new contract.
- Design a dedicated website on shi.com including the AEPA awarded vendor logo, a copy of contract documents, a summary of products and pricing, marketing materials, a link to AEPA's website, and all relevant contact information.
- Create internal sales training for new contract compliance, pricing, terms, etc.

We will also welcome any opportunity to work with AEPA on advertise at their events or in their newsletters.

SHI participates in hundreds of trade shows, conferences, and meetings across the country. AEPA has our commitment to participate at specified shows as well as additional opportunities to broadcast and promote our partnership.

We also provide seminars and workshops to our public sector customers across the country and are eager to have AEPA members attend.

Summits

SHI holds technology summits at our corporate headquarters in Somerset, NJ. Our next summit, scheduled for Oct. 8-9, is titled *Infrastructure, Hybrid Cloud and Cybersecurity Foundations for AI Success*. The summit is aimed for Leaders in IT infrastructure (including CIOs, CTOs, CISOs, Directors of IT, and more) who are eager to learn from industry experts how to best address the forces impacting today's infrastructure, cloud, and security environments.

Custom Events

SHI has previously hosted a series of roadshow events, focusing on topics such as cybersecurity and infrastructure at large event spaces around the country with solution partners and special guest speakers.

The account team can also use various other methods to market and sell the products that we represent to AEPA agencies, including customer meetings, vendor presentations, trade shows, web seminars, printed marketing materials, our website, and a monthly electronic newsletter. We also host strategic events with many of the SHI and manufacturer representatives to provide our mutual customers with new product information, product changes, and industry direction. Additionally, we participate in vendor exhibits at numerous monthly events, including technology trade shows.

Some of the marketing-related items contract customers can expect to receive and be able to access include:

Newsletters

SHI creates various informative, monthly newsletters containing information regarding important contract dates, product releases or changes, Q&A, and upcoming events. Thousands of our customers currently receive these newsletters, and we will continue to make them available as a subscription to anyone who is interested.

Web Seminars

SHI hosts a series of web seminars covering a variety of topics including new product announcements, changes to licensing programs for major software OEMs, procurement and technology trends, and foundational IT information. Webinar schedules are published quarterly, and historically, our webinars have a regular audience of AEPA members. Please check the events page on our website https://www.publicsector.shidirect.com/ for the current schedule.

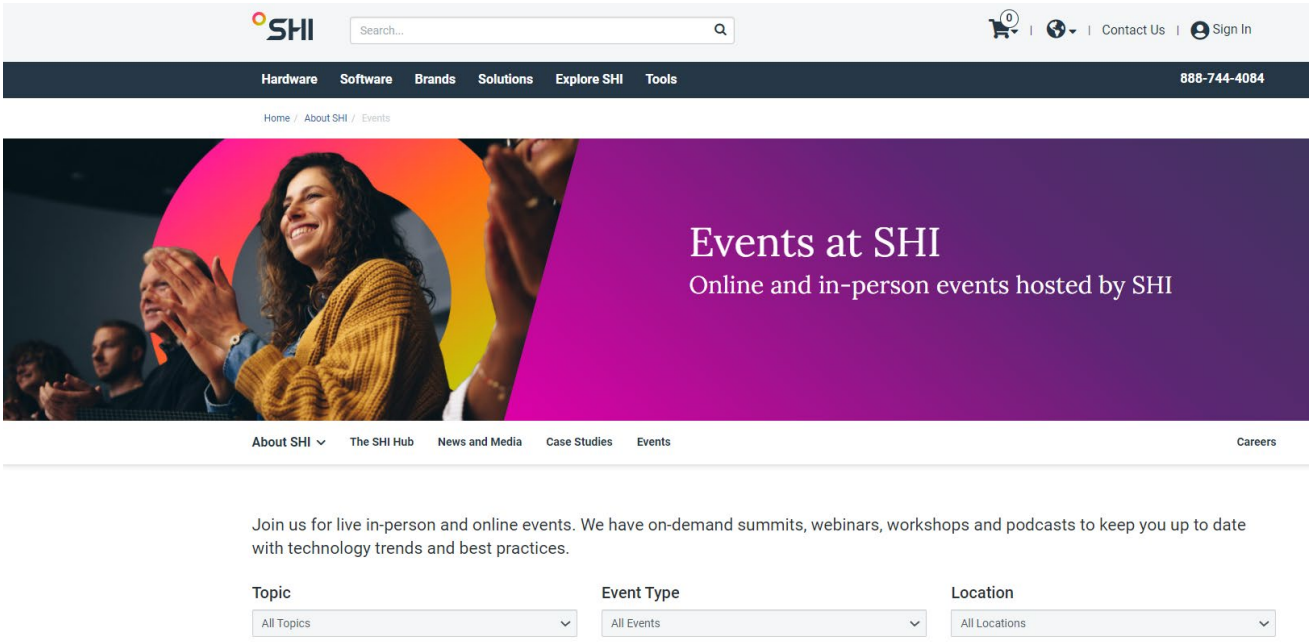


Figure 12: Events at SHI

Marketing Documents

SHI creates hundreds of marketing texts for our major manufacturer partners and SHI core services offerings, all of which are made available to customers through in-person meetings, trade shows, email delivery, and mail-outs. Marketing documents will include those that we receive from the manufacturers, those that SHI creates for a general audience, and those that SHI creates specific to AEPA. An example is included on the following page.



SHI HUB

The SHI HUB is home to eBooks, on-demand articles, and podcasts to keep our customers updated on the latest changes and trends impacting the IT industry. Showcasing short news and informational articles, the SHI HUB keeps our customers up to date on our services and support as well as on emerging trends in technology. Written by SHI's subject matter experts who leverage their knowledge and insight to speak to SHI's broad customer base, SHI is committed to keeping our customers informed. The

screenshot below exemplifies the easy navigation of the SHI Hub website. Customers can browse by IT category, recent articles, or popular posts.

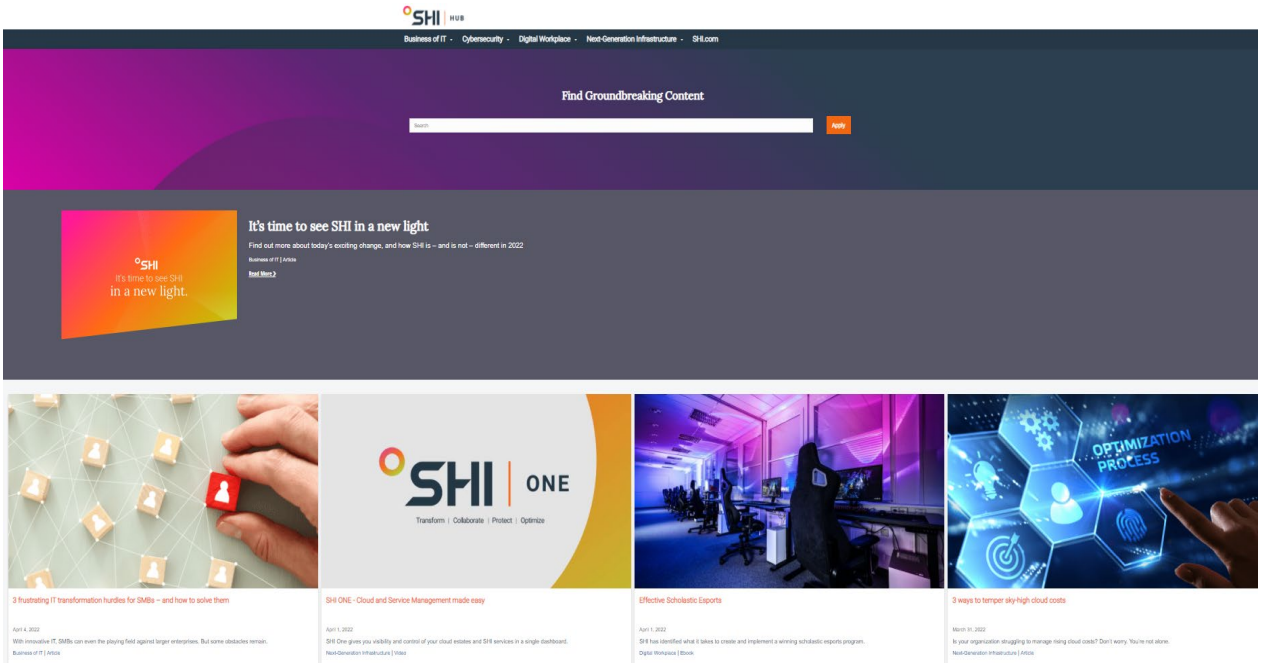


Figure 13: SHI Hub Website

Executive Forums

SHI extends invitations to our customers to attend our annual Executive Forums, which focus on reviewing current industry trends. These forums include keynotes and breakout sessions led by industry experts from both SHI and top OEMs sharing the best practices they use to support digital workspace, hybrid cloud, data center, and security initiatives. Your teams will also be able to attend deep-dive workshops focusing on IT asset management, next-generation data center architectures, and cloud services.

Social Media

In addition to the SHI Hub, SHI utilizes social media applications to keep our customers informed. Customers can get up-to-date information on demand by following SHI on X (formerly Twitter), LinkedIn, Facebook, and YouTube.

1.6.4 Describe the ways in which your company will collaborate with AEPA Agencies to market the resulting contract. Include any contract announcements, planned advertisements, and any other direct or indirect marketing activities promoting the AEPA awarded contract. Add any supplemental materials as pdfs and label them as Exhibit A-Marketing.

SHI Response:

SHI is dedicated to collaborating with AEPA and member agencies in the marketing of this contract. With decades of experience onboarding similar contracts, we have a team and processes in place, along with resources across the country, to ensure the growth and success of our partnership. Upon award, the AEPA team will work with our Public Sector leadership, Marketing team, and the following people to create and execute this marketing plan:

- Aimee Ballenger, Sr. Director of Contract Capture and Development, Aimee_Ballenger@SHI.com
- Amelia Jakubczyk, Director SLED Contract Capture and Development, Amelia_Jakubczyk@SHI.com
- Chris Dickman, Capture and Business Development Manager, Chris_Dickman@SHI.com

Below we have prepared a sample marketing plan for your review, but will remain flexible and open to collaboration with AEPA upon award, including any contract announcements, industry periodicals, or other direct or indirect marketing activities agreed upon.

Please review Exhibit - A Marketing - SHI for more details.

First week

- Post announcement along with contract details and contact information to https://www.SHI.com.
- Begin design of co-branded marketing materials, including print, electronic, email, and presentations.
- Discuss publication and distribution plans, as well as a plan to distribute and follow up on leads.
- Design and implement the AEPA secured website on https://www.SHI.com including the AEPA logos, copy of original RFP, copy of contract and amendments, summary of products and pricing, marketing materials, a link to AEPA's website, and all relevant contact information.

First month

- Complete design of co-branded marketing materials.
- Finalize plans to publish and distribute.
- Begin distribution to current and prospective AEPA agencies.

First 90 days

- Complete training and enablement for SHI sales force.
- Complete publishing and distribution of initial marketing materials.
- Analyze initial activity.
- Discuss the next 90-day plan for marketing.

Ongoing

- Design and publish national and regional advertising in trade publications.
- Market and promote the Master Agreement, including case studies, presentations, campaigns, and blog posts.

SHI also participates in many trade shows, conferences, and meetings across the country, and welcomes any opportunity to work with AEPA on advertising at events. AEPA has our commitment to participate at specified shows as well as additional opportunities to broadcast and promote our partnership.

As part of the response to this requirement, we have also created a separate document, labeled "Exhibit A-Marketing - SHI" as requested and included as part of our response.

1.6.5 Describe the process for how the company will launch the contract with current and potential agencies.

SHI Response:

SHI Capture and Business Development Manager Chris Dickman is aligned to AEPA. He is available to support regular reviews with AEPA representatives as the contract kicks off. A healthy contract review will allow us to stay focused, analyze results for plans and strategies currently in place, discuss new campaign and marketing ideas, and review the overall success of the contract.

SHI's growth has come from a continued assessment of our relationship with our customers—the Sales team and Technical and Operational Support teams enhance our relationship and scale and offer new solutions and services to our clients. We continue to expand our relationship with public sector customers by offering new solutions that solve their business needs. We also remain a tremendously agile and scalable company that allows us to take share and spend from our competitors. SHI's Public Sector Sr. Leadership team continually monitors our business with existing customers and the support that SHI provides, as well as reviews the public sector clients that SHI is not actively working with and creates teams and solutions to build a relationship with new customers to SHI.

Our history of success with similar contracts will be invaluable to a strong launch. Below is our contract implementation plan.

Stage 1: Contract Award

To bring the right solution to AEPA member agencies, we need to first understand your vision, through the initial kick-off meeting. Once we understand your vision, our implementation team—comprised of sales, solution experts, and product-specific resources—helps design a strategy that is suitable to your IT environment today and scalable to meet your future needs. This approach might include conducting assessments of your current environment or proof of concept for a potential solution. When you are ready to move forward, SHI will help confirm AEPA member agencies is procuring products and services using advantageous pricing models.

Seeking a mutually beneficial agreement, SHI will work closely with AEPA member agencies to negotiate pricing along with the contract terms and conditions. This will be led by a member of SHI's Legal team in coordination with the members account team. Once an agreement is made, SHI will assemble a key stakeholder's kick-off call to thoroughly review the contract requirements and the steps needed for implementation, including additional milestone meetings. SHI understands that transitioning from one IT solution provider to another can be disruptive, and we will work with their previous provider, if applicable, to ensure a smooth transition.

Stage 2: Implementation Begins

SHI understands the importance of marketing contracts and reaching all eligible stakeholders. SHI will communicate the scope of the contract to key AEPA member agencies stakeholders and help create awareness of our partnership. Working closely with AEPA member agencies, we can provide specific information regarding the manufacturers and products available under the agreement. We will provide details of relevant SHI contacts that will support their business and additional details, such as how AEPA member agencies end users can obtain quote requests.

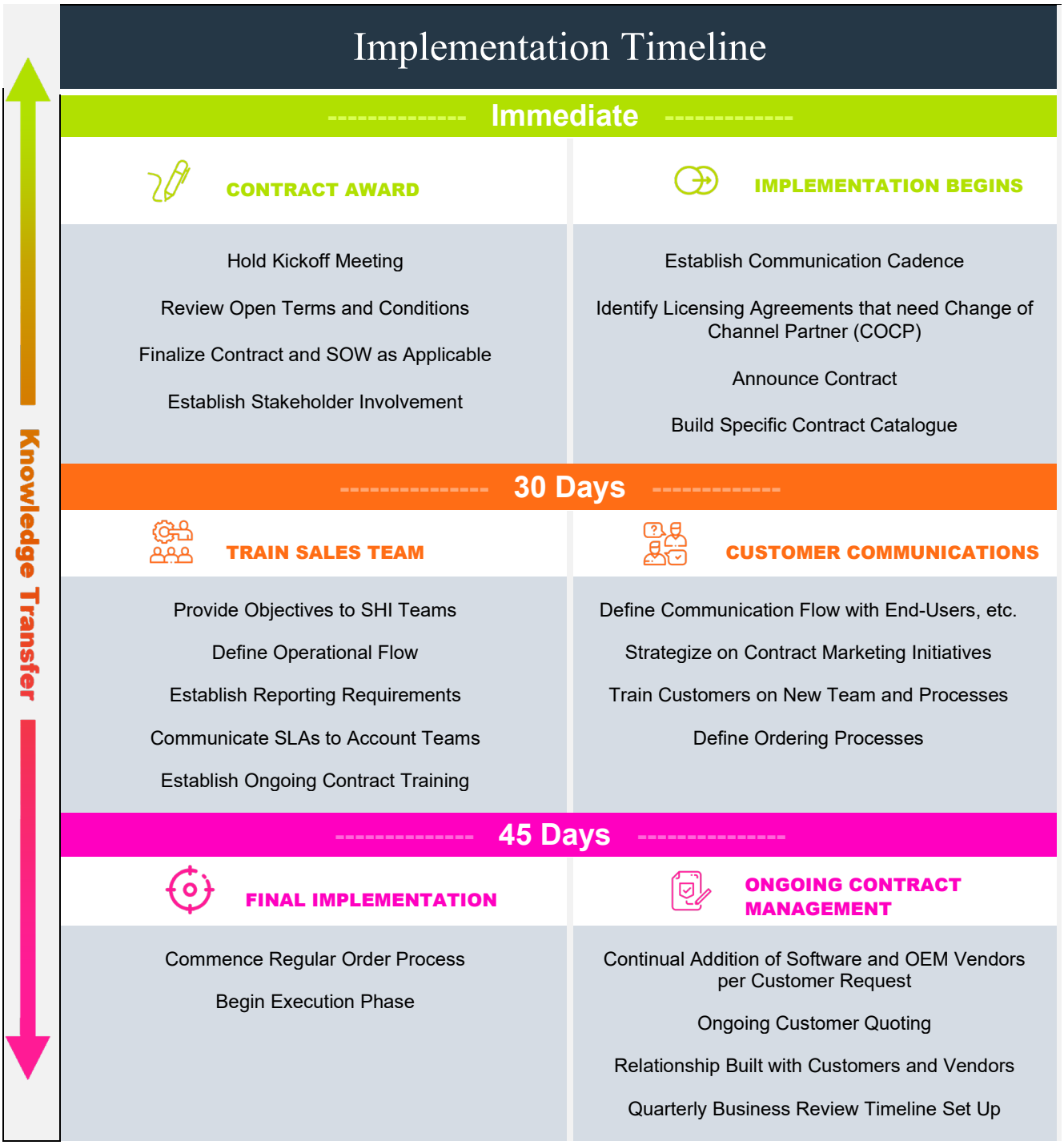


Figure 14: Implementation Timeline

Stage 3: Train Sales Team

SHI will align our Inside Sales practice to meet AEPA member agencies SLAs and reporting requirements as we work together to define the operational flow. We will also create test reports based on agreed upon

reporting files that will be generated by SHI's business intelligence reporting system. AEPA member agencies will provide key contacts within your organization to validate the report.

Stage 4: Customer Communication

SHI will work with AEPA member agencies to identify your order processing requirements including preferred procurement method (EDI, email, web, fax), understanding who will be submitting purchase orders, along with invoicing requirements such as preferred method of receipt of invoice (EDI, paper, email) and preferred payment method (check, electronic transfer, credit card).

SHI will work with AEPA member agencies to identify authorized users who can access our ecommerce platform, SHI.com. Our e-commerce specialists are available to provide training to AEPA member agencies and employees authorized to access contract pricing and information at SHI.com.

Stage 5: Final Implementation

After the implementation is completed, and when AEPA is fully onboarded as a SHI customer, you should expect full support of the dedicated SHI account team that is committed to meeting your contractual requirements. We will engage in continuous discussions with AEPA to understand your IT roadmap and align value-added services with your business objectives. Once SHI has identified AEPA's manufacturer agreements, we will work to provide proactive renewal quotes.

Stage 6: Ongoing Contract Management

SHI will continue to engage post-implementation, as we are committed to providing ongoing support to AEPA. As part of our governance model, we will conduct quarterly business reviews (QBRs) to understand how we can better support you and your business needs. These meetings can be as formal or informal as you like and can be conducted monthly. We believe they are a chance for us to understand the previous quarter's results, gather feedback, celebrate critical accomplishments, and identify potential service improvement opportunities.

QBRs are also a forum to plan for the quarter ahead and beyond. While SHI will cover AEPA's preferred topics, areas typically include an executive overview, review of customer spend, review of SLA's, major accomplishments in cost savings, and setting of newly realized goals/SLA's moving forward. The SHI sales management team regularly reviews our volume and response time to act quickly and enhance staffing levels as needed. We will confirm training and qualifications of staff before introducing them to the contract.

Environmental Initiatives

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary relevant details for a few questions are included here.

1.7.1 Indicate if your company has any products in your offering that have any third-party environmental certifications.

SHI Response:

Because we are responding to the cybersecurity and training category, third-party environmental certifications do not apply to the solutions we are proposing however in support of our sustainable initiatives, SHI has received Gold LEED Green Certifications for both our Global Headquarters in New Jersey and Austin Regional Headquarters in Texas. These projects, along with our building renovation, signify SHI's tremendous growth and are a physical representation of our dedication to sustainability.

In addition to incorporating environmentally friendly initiatives into our business strategy to protect the planet and reduce the amount of IT hardware waste each year, we also help our global IT customers reduce, reuse, and recycle their hardware assets through our sustainable IT solutions. Some of our customer/partner initiatives include recycling office equipment and related items in compliance with county, municipal, and EPA guidelines.

Please see copies of SHI's certifications below:



Figure 15: SHI Headquarters LEED Certification



Figure 16: Garza LEED Certification

SHI is dedicated to environmental sustainability and recognizes its role in affecting the environment. We continually strive to minimize any negative impact from our operations while ensuring the safety and well-being of our staff. Our business strategy heavily emphasizes environmental preservation and the promotion of a sustainable future. By implementing eco-friendly initiatives, both internally and with our partners, we aim to reduce yearly technology waste and contribute more significantly to a greener planet.

SHI's sustainability vision is to operate its business as a responsible environmental citizen committed to managing resources and concern for our environment's well-being. As a reseller and not a manufacturer, SHI is naturally low impact; however, we are always mindful of the environment and work to reduce any damaging effects from our organization while protecting our staff's safety and well-being.



Preserving the environment and fostering a sustainable future are crucial principles of our overall business strategy. Our vision moves to leverage our technical expertise to solve business outcomes while incorporating environmentally friendly initiatives, driving efficiencies to minimize technology, and maximizing our impact toward a greener planet.

When it comes to sustainability, SHI can provide and implement several solutions for your organization, including:

Asset Recovery: We pick up your old equipment, take inventory of what is still usable, and report our findings to you.

E-Waste Recycling: We hold multiple recycling events around the nation so you can quickly and properly dispose of unwanted devices.

Hardware Remarket: We put your hardware back on the market if you cannot or choose not to reuse it.

Asset Disposal: We work with partners worldwide to ensure your old hardware is recycled correctly.

Hardware Redeployment: We determine if your equipment is eligible for reuse and keep stock in our warehouse that you can redeploy at any time.

IT Asset Management: We measure, manage, and optimize software and cloud consumption impacts to enable customers to reduce their environmental impact and waste.

SHI intends to achieve our vision through the following initiatives:

Sustainable Solutions
As a global solutions provider and technology advisor, we are here to help our customers reduce, reuse, and recycle technology assets through our various eco-friendly solutions.

Securing Green Products
SHI works on our customer's behalf to identify and source products with environmental certifications.

Resource Usage and Efficiency
With two LEED Gold certified builds, SHI embraces the spirit of these rigorous standards and seeks to consume fewer natural resources, reduce operating costs, and create safe, healthy environments for their occupants.

Employee Awareness
SHI's employees are at the forefront of achieving our sustainability goals by promoting green products and sustainable solutions to our customers while also understanding their impact on the environment.

Finance and Leasing: We offer financing and leasing opportunities with industry-leading partners, enabling customers to ethically offset their carbon emissions.

Cloud and Data Center Solutions: We have the expertise and people to help our customers migrate, optimize, modernize, and manage your cloud.

The business case for using green products cannot be denied. At SHI, we know our actions make a difference. As a leader in the IT industry, we can influence change by putting eco-friendly products and sustainable services at the forefront of our solutions. We believe accountability can play a positive role in society by working together to drive this change and invite our customers and partners to join us in this endeavor.

1.7.2 " Describe the business's "Green" objectives (e.g. LEED Certification, reducing footprint, reuse, reduce, recycle) "

SHI Response:

SHI has made significant investments in our energy efficiency practices. Our global headquarters located in Somerset, NJ, and regional headquarters in Austin, TX—which represent more than 3,000 employees, half of SHI's total workforce—are both LEED Gold certified. To support our goals and reduce power consumption, SHI has made significant green investments in our facilities by installing solar panels. Today, more than 7,000 solar panels are installed at four SHI-owned facilities, including our global headquarters and integration center in New Jersey, and our regional headquarters in Texas. Installing these solar panels has helped SHI avoid 5,287,000 pounds of carbon dioxide since the system's installation and avoided 13,771 pounds of sulfur dioxide and 5,425 pounds of nitrogen dioxide since installation. We continue to evaluate the installation of additional solar panels at other locations and facilities.

In addition to our investments in solar, facility upgrades have been implemented to utilize advanced energy-saving systems. Improvements include:

- Automatic lighting controls and LED lighting throughout our Austin regional headquarters
- Electronic vehicle charging stations located at our global headquarters, Ridge Integration Center in New Jersey, and our regional headquarters in Texas
- Energy Star equipment/appliances
- Energy recovery from building relief/exhaust air, demand control ventilation sequences for energy savings on ventilation in our Austin regional headquarters
- High-efficiency HVAC equipment
- Occupancy sensor control of lighting fixtures
- Water-efficient and low-flow plumbing

To help us understand our impact and identify areas for improvement, we monitor energy consumption and annually disclose this data to entities such as the Carbon Disclosure Project (CDP) and EcoVadis. As SHI continues to invest in our infrastructure through building upgrades at these facilities, we will evaluate and consider additional energy efficiency improvements.

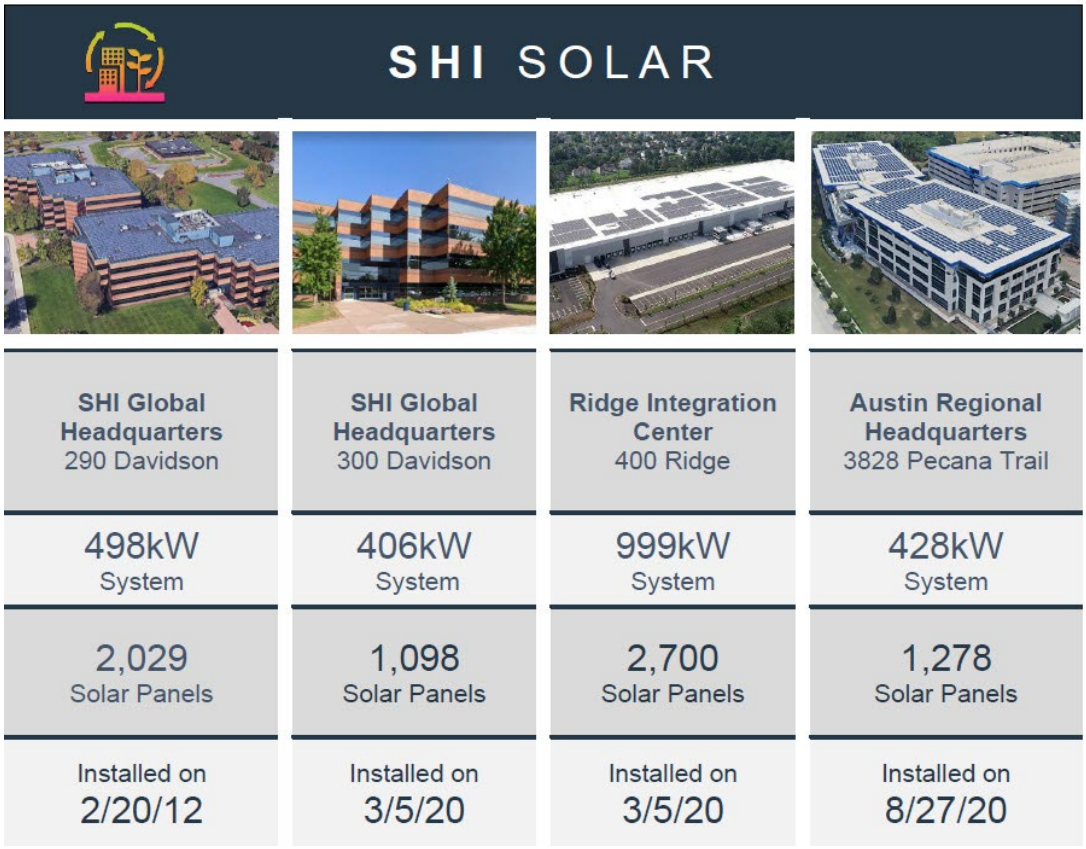


Figure 17: SHI Locations and Installation of Additional Solar Panels

SHI ESG Policy

Kuli Sidhu has been appointed as SHI's environmental, social, and governance director and is responsible for driving assessments of the company's operations and identifying strategic improvements. To support this effort, SHI has mobilized an environmental, social, and governance committee with representation from key functional groups. Executive management, including Chief Executive Officer, Thai Lee and Chief Financial Officer, James Prior, provide oversight of the environmental, social, and governance program through quarterly reviews, determining the effectiveness of the program and evaluating strategic investment decisions to drive sustainability initiatives.

Please see attached file named SHI Sustainability and Action Report 2023_F.pdf uploaded as a separate attachment along with this document on portal.

Value Add

1.8.1 Describe any/all features of your company that you feel will provide additional value and benefit to a participating AEPA agency.

SHI Response:

SHI's vast resources will provide significant value to the technology investment of AEPA member agencies which include, among others:

Core Solutions Engineers

This team's mission is to help customers choose exactly the right technology solutions. Core solutions engineers are tightly aligned with our account executives to bring maximum value to our customers. Core solutions engineers are also unique in the public sector value-added reseller space and help customers compare competing hardware and software products and provide valuable technical insights on choosing the right solution for each unique organization. They consult with customers, often helping them to avoid erroneous or superfluous costs. In addition, core solutions engineers consider organizational skill sets, compatibility with the current environment, redundancy, alignment with objectives, and total cost of ownership—all through a vendor-neutral lens.

Pre-Sales Technical and Product Support

Along with the dedicated sales team, AEPA and member agencies will benefit from SHI's extensive and knowledgeable pre-sales technical and product support. Over the past decade, IT has changed. Although there is still a need for commodity products, attention has turned more and more to building solutions that will solve customers' needs. In response to this evolution, and working within our customer-centered foundation, we developed our Advanced Solutions Group to include solution-based support. This team has more than 200 technical resources who hold more than 3,000 certifications for various products and solutions. These Solutions teams are always vendor-neutral, and they use their breadth of experience to help tailor conversations in order to optimize a customer's specific environment. We engage our customers during the strategy and solution design phases of a project and assist with strategic planning, assessments, whiteboarding, proof of concepts, and more. Initiating conversations early in the process leads to enhanced project outcomes and cost savings. In addition, we provide extensive product and vendor-specific support to ensure successful adoption and development during the life of the project.

This Pre-Sales Technical and Product Support group also includes a team of Field Chief Information Security Officers. This team partners with our customers to assist in developing mature security measures for their environments.

SHI Labs

SHI Labs allows customers to test and compare IT solutions before committing to an investment. SHI Labs is staffed with trained team members and technical professionals who are experts on both products and solutions. As technology advances and changes, the available technologies in the SHI Lab will follow, ensuring that we always have the products and relevant technologies that our customers are interested in evaluating.

Specific to AEPA and AEPA members SHI Labs will allow representatives and individual users from your organization the opportunity to see, touch, and observe hardware in our Showcase Lab, where we house equipment and technology from various OEMS, in addition to our "Software and Sandbox" Lab, where you can engage with hardware and software specifically designed for educational and classroom use. With more than 8,000 square feet of hands-on IT on display, SHI Labs' opportunities include, but are not limited to:

- Server and Database Software
- Management Software Solutions
- Custom Software Solutions
- Security Software

- Hyper-Converged and Converged Infrastructure
- Software-Defined Infrastructure
- Hybrid Cloud
- Big Data
- Mobility / Client Hardware devices

SHI Labs is designed to be used for:

- Demonstrations to evaluate product features and functions in a tangible working environment
- Proofs-of-concept to test next-generation equipment without disrupting your datacenter
- Tangible training for a deep-dive walkthrough from our solution architects
- Test Drives to see our end-user environment and determine what a device will look like in real-world cases.

Our value remains tangible in every component we offer from strategy to solution design, evaluation and selection to procurement, and deployment to support. Below, we present our solution workflow to demonstrate what we do and how we support our customers' vision throughout each step of the process.

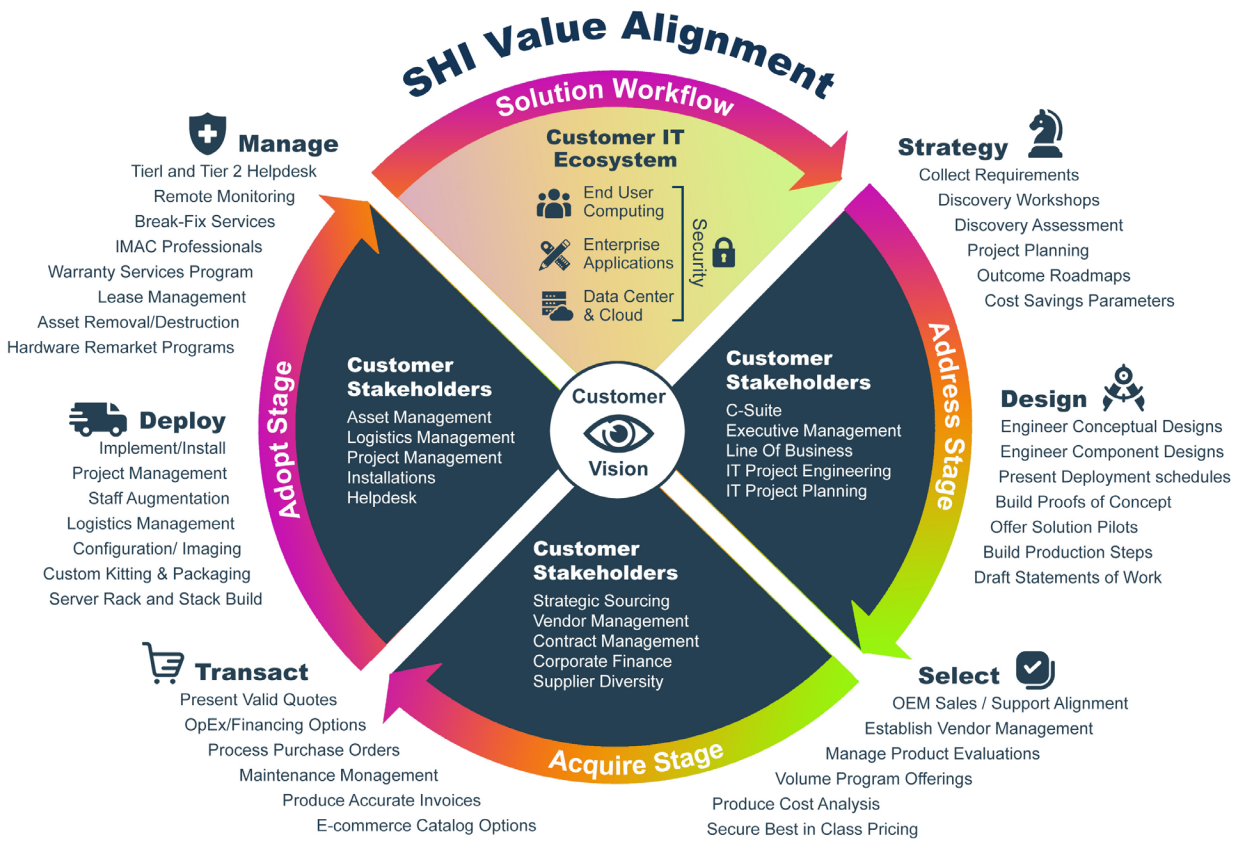


Figure 18: SHI Value Alignment

Consulting with Actionable Insights

Along with leading technology solutions and customized testing in our state-of-the-art configuration center, SHI offers advisory consulting services to help our customers leverage security services and understand key insights into your current cybersecurity state such as processes, infrastructure, risks/threats, with the goal to provide a roadmap to secure and protect your critical data.

We offer guidance around cybersecurity technologies, strategies, environments, and goals. SHI seeks to reduce the effort and time required for AEPA member agencies to build a strategic roadmap and execute a vision. Results are closer alignment to their business initiatives and ultimately elevating the value a security program provides. Our consulting is focused on:

- Security best practices and compliance
- Regulatory requirements and security frameworks
- Security industry trends and guidance to align your organization with the market leaders
- Product comparison and integration

Furthermore, cybersecurity experts provide actionable insight to help you:

- Secure your new hybrid workforce
- Ensure seamless and secure access no matter where users, applications, or devices are located
- Assess the cybersecurity health of your organization and your vendors
- Identify gaps in protection and opportunities for consolidation across security controls
- Streamline security operations with automation
- Guard against accidental and malicious insider threats
- Strengthen your overall cybersecurity and risk management posture

Our field service resources will provide pre-sales support, architecture, and engineering, which are agnostic in approach to SHI's full portfolio. AEPA member agencies have access to experienced engineers who have competencies in design, development, implementation, and management of advanced technologies. SHI employs a team of highly skilled engineers with a wide range of network topologies, applications, and complexity of services. Resources such as presales solutions architects and presales solutions engineers can engage in security discussions with member agencies as well as in areas such as cloud, collaboration, data center, mobility, networking, and security. SHI will align resources to help identify solutions and work in conjunction with technology provider resources for initial planning sessions, leading to additional conversations based on the organization's interest.

DISCLOSURES

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD).

REFERENCES

1.10.1 Provide contact information of your business's five largest public agency customers. Include the customer business name, contact name, title, phone number and email.

SHI Response:

Five SHI Cybersecurity References are listed below:

Reference 1

Customer Business Name: The University of Texas MD Anderson Cancer Center

Contact Name: Sean Walker

Title: CISM, Manager Cybersecurity, Cybersecurity Operations Team

Phone Number: 713-563-5103

Email: swalker@mdanderson.org

Reference 2

Customer Business Name: NYC Public Schools

Contact Name: Demond Waters

Title: Chief information Security Officer

Phone Number: 332-237-0661

Email: dwaters@schools.nyc.gov

Reference 3

Customer Business Name: Louisiana Office of Technology Services

Contact Name: Michael Allison

Title: Chief Administrative Office

Phone Number: 225-342-7144

Email: michael.allison@la.gov

Reference 4

Customer Business Name: Indiana Office of Technology

Contact Name: Chris Barnett

Title: Vendor Management Coordinator

Phone Number: 317-522-9935

Email: Cbarnett2@iot.in.gov

Reference 5

Customer Business Name: University of Nevada, Reno, Office of Information Technology

Contact Name: Brandon Guilbe

Title: Chief Information Security Officer

Phone Number: 775-682-5621

Email: bguilbe@unr.edu

Question Set 2: Service Questionnaire

Sales Data

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary relevant details for a few questions are included here.

2.1.3 Please refer to the chart of participating AEPA member states in this solicitation and list the states in which your company has sales reps, distributors, or dealers.

SHI Response:

SHI is a global company and employs more than 1,500 salespeople. Within our Public Sector Sales organization, we employ more than 250 salespeople. The below graphic demonstrates the nationwide coverage of SHI employees.

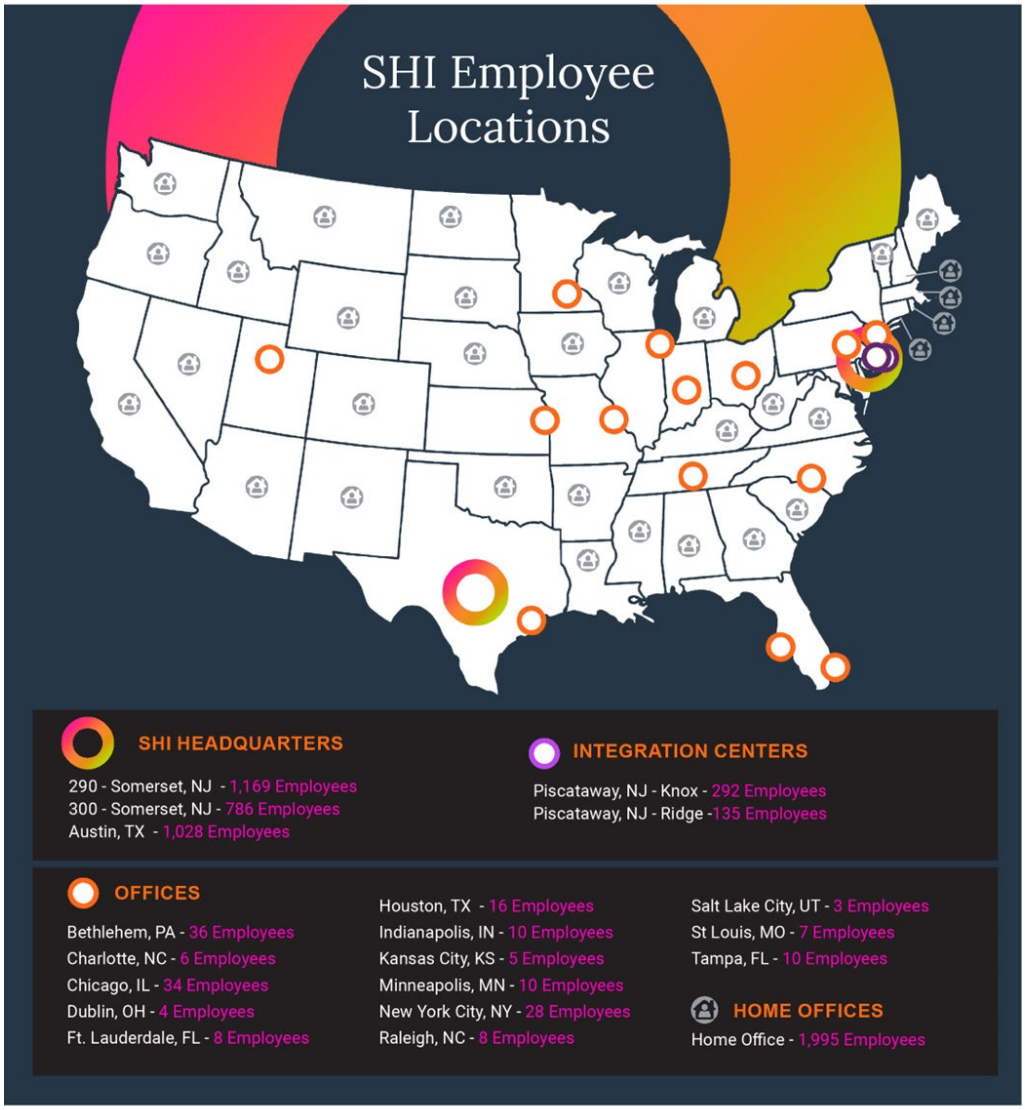


Figure 19: SHI Employees by Location

We work loyally to maintain relationships with both our large IT distributors (Ingram Micro, TD Synnex, and D&H) and smaller, local distributors and manufacturers directly.

2.1.4 Does this company have an e-commerce website?

SHI Response:

SHI.com is SHI's single-source procurement platform available to all SHI customers. From the comfort of their offices, AEPA member agencies can access the most recent catalog features, customization options, approval routing, workflow, reporting, order status, and our renewal organizer timeline.

With more than 470,000 products available, our eCommerce team will ensure each AEPA member agency's site contains only approved products. This requires no additional work for AEPA member agencies: We review their company standards, license agreements, and location to ensure we only offer products that meet their requirements. Please see the SHI e-commerce site home page graphics in response to question 2.1.6 for reference.

2.1.6 If applicable, describe your company's ability to integrate into other ecommerce sites. Include details about your company's ability to create punch out sites and accept orders electronically (cXML, OCI, etc.)

SHI Response:

SHI.com is SHI's single-source procurement platform available to all SHI customers. From the comfort of their offices, AEPA member agencies can access the most recent catalog features, customization options, approval routing, workflow, reporting, order status, and our renewal organizer timeline.

With more than 470,000 products available, our eCommerce team will ensure each AEPA member agency's site contains only approved products. This requires no additional work for AEPA member agencies: We review their company standards, license agreements, and location to ensure we only offer products that meet their requirements.

Self-Service

The platform is designed to support self-service functions, including the registration of new users—of which there is no limit. As an IT company, we take privacy and security seriously. Member agency information will not be shared with software publishers or third parties without explicit permission.

SHI's catalog includes all the features AEPA member agencies should expect every procurement website to have—advanced search capabilities, real-time reporting, permission levels for different user groups (approval routing), and more. AEPA member agencies can also customize the landing page to show their company logo and include a news and announcements section.

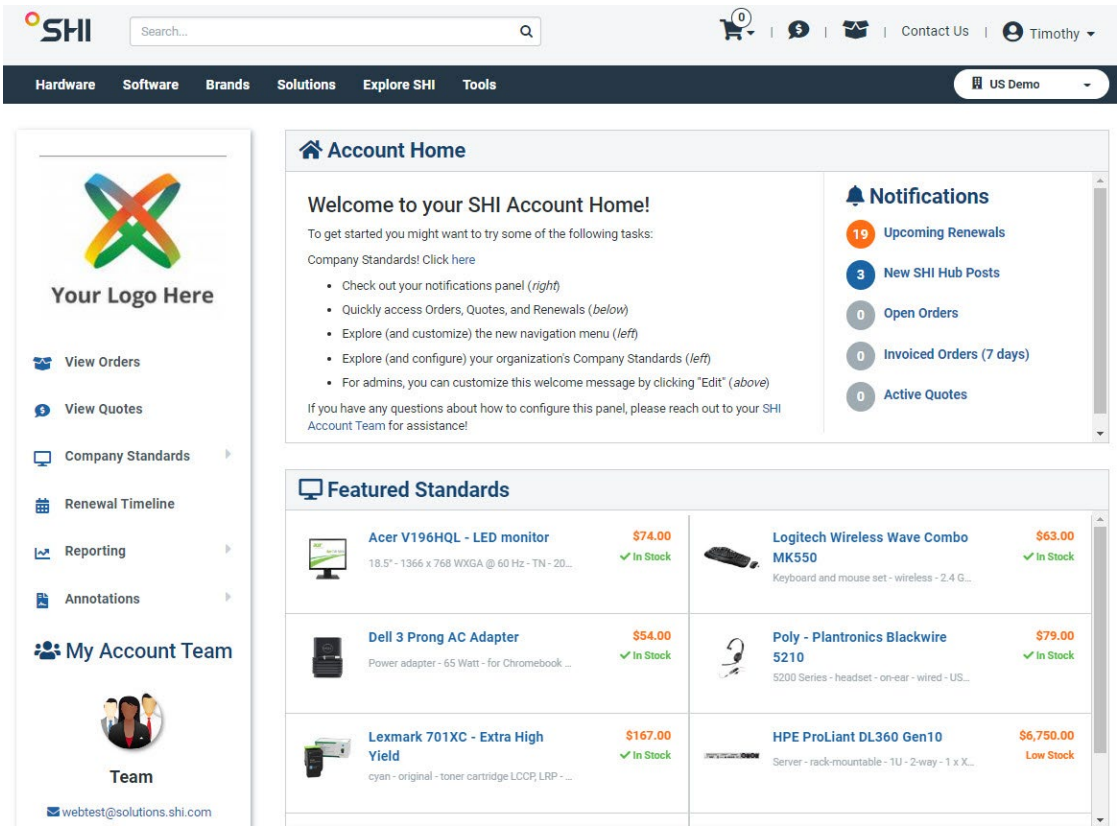


Figure 20: SHI eCommerce Site Home Page

Seamless Integration

Our open architecture system allows us to integrate with most e-commerce platforms, whether through market leaders or a proprietary solution. In addition to supporting the following punch-out types, SHI regularly updates this list as we continue to work with new applications.

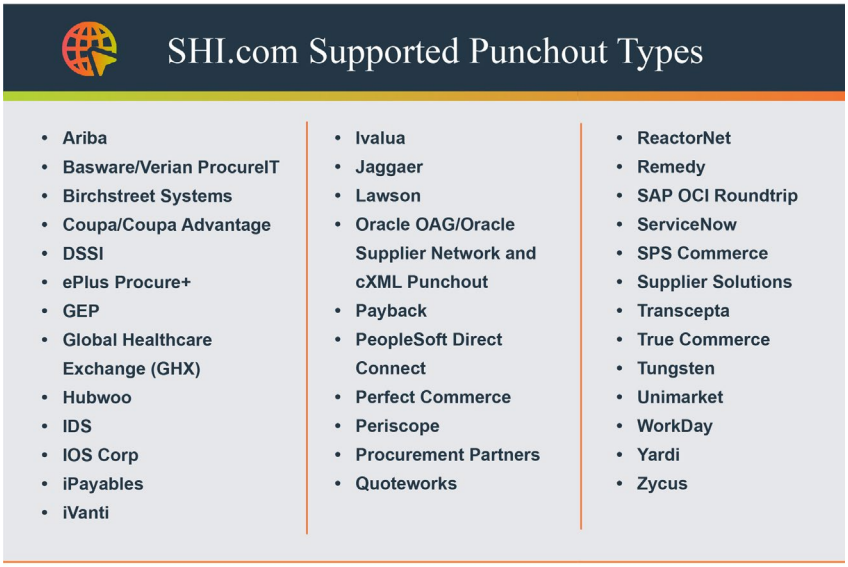


Figure 21: Punchout Types

Regardless of your IT procurement needs, SHI's web catalog can meet the challenge. With the option of eight currencies and four languages, AEPA and member agencies have limitless opportunities to expand.

Training

To better help AEPA and member agencies use the many features SHI.com has to offer, SHI's e-commerce specialists provide training to employees authorized to access Your Home @ SHI.com. We will work with AEPA member agencies to determine the training program and schedule that works best.

2.1.7 Provide detail on where your company has integrated with a public agency's ERP (Oracle, Infor Lawson, SAP, etc.) system in the past and include some details about the resources you have in place to support these integrations. List, by ERP provider, the following information: name of public agency, ERP system used, "go live" date, net sales per calendar year since "go live", and percentage of agency sales being processed through this connection.

SHI Response:

Please see SHI's Electronic Data Interchange overview below:



Figure 22: SHI EDI Overview

SHI has more than 25 years of experience in integrating with eProcurement systems. Sample SHI ERP providers list for the last two years is below with ERP system and go live date. Customer names and applicable sales data are not listed for confidentiality and NDA.

Table 7: Sample SHI ERP Providers

ORGANIZATION UNIT NAME	SYSTEM NAME	FIRST PUNCHOUT SESSION
large education customer	SciQuest	7/27/2023
large education customer	Jaggaer/SciQuest	5/15/2023
large education customer	Jaggaer	5/8/2023
large education customer	Jaggaer	6/6/2024
large education customer	Jaggaer/SciQuest	4/23/2024
large education customer	Jaggaer	2/1/2023
large education customer	Jaggaer	8/5/2023
large education customer	Jaggaer/SciQuest	9/11/2023
large education customer	Jaggaer/SciQuest	5/8/2024
large education customer	ESM Solutions	11/1/2023
large education customer	Oracle	2/13/2024
large education customer	EqualLevel	8/24/2023
large education customer	Workday	2/2/2024
large education customer	Munis	3/28/2023
large education customer	ESM	8/1/2023
large education customer	EqualLevel	3/4/2024
large education customer	EqualLevel	1/29/2024
large education customer	EqualLevel GO	10/20/2023

CUSTOMER SUPPORT

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary relevant details for a few questions are included here.

2.2.1 Does this business have online customer support options?

SHI Response:

Yes. AEPA members can contact online customer support at: https://www.shi.com/us/customerservice/contact-us.

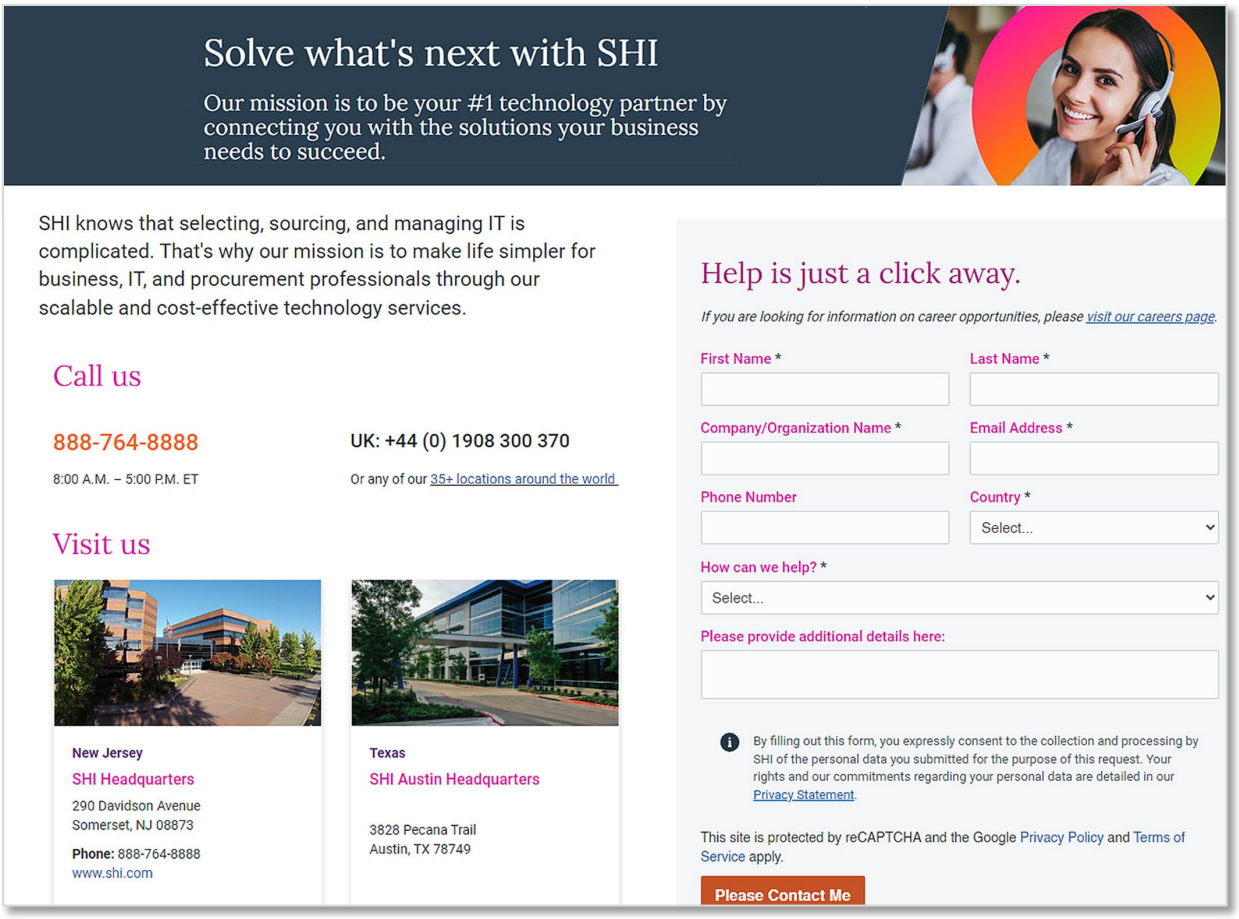


Figure 23: SHI Online Customer Support Option

2.2.5 State your backorder policy. Do you fill the order when available, or cancel the order and require participating agencies to reorder if items are backordered?

SHI Response:

SHI is responding to the Cyber Security & Training RFP, and non-physical items such as software are not typically subject to issues related to backorder. For many software publishers and distribution partners, the typical turnaround time for an electronic license distribution is 24 to 48 hours.

Should our and AEPA's partnership expand moving forward, SHI has a backorder policy in place to support member agencies.

As the backorder status changes, a member agency's inside account manager will provide updates about the estimated time of availability. At any time before shipment, the member agency will have the option to leave the product on backorder, substitute a different product, or cancel the order with SHI.

For proactive order status, agencies can use SHI's order management system to track product shipments. SHI receives the tracking numbers for all products shipped from our distributors daily via electronic data interchange. These tracking numbers are integrated into SHI sales orders and are ready for immediate access by the inside account manager or authorized AEPA member agency's employees through their customized procurement catalog on SHI.com.

SHI can send agencies milestone notifications such as order acknowledgments and shipping notifications. Backorder reports are available upon request.

2.2.7 State your company's return policy and any applicable restocking fees.

SHI Response:

SHI's comprehensive return policy can be viewed on our website, SHI.com.

For customers who have established a custom catalog on SHI.com, authorized users can request returns for physical items. Non-physical items such as software and warranties are not eligible for return via SHI.com. Users are asked to select the reason for the return, if the package has been opened, and to provide any additional information about the request. Once the request is submitted, the customer's dedicated SHI account team will contact the requestor to offer assistance.

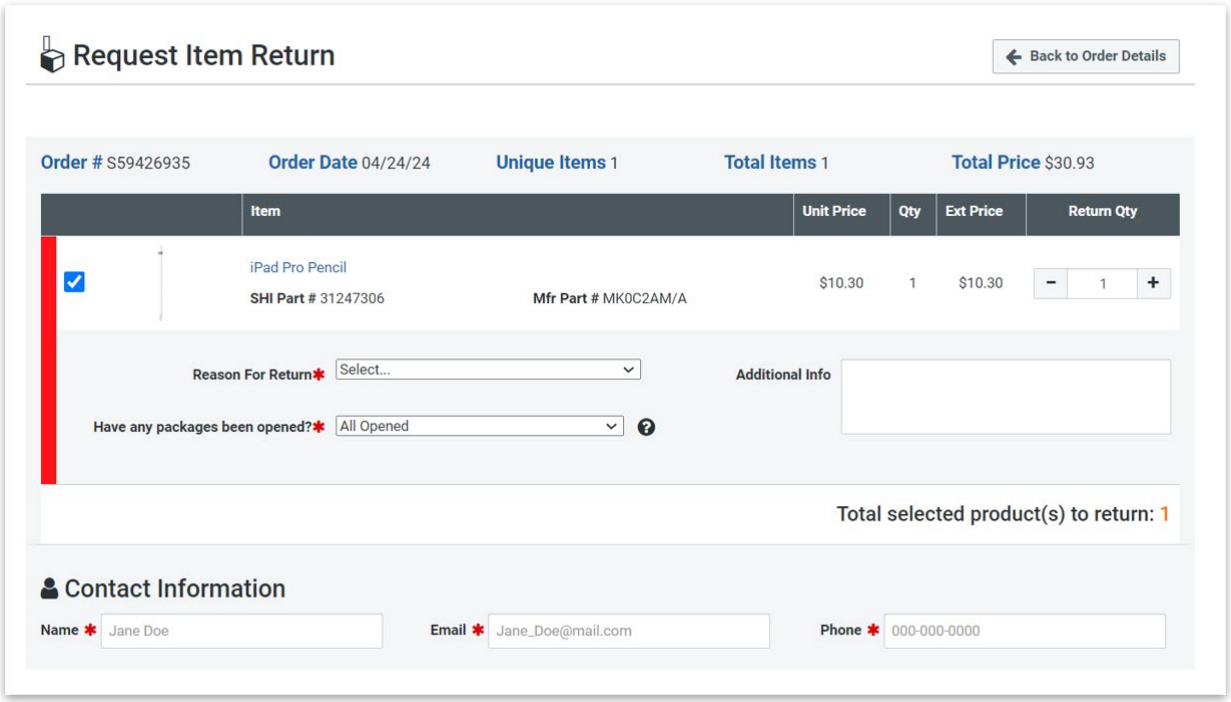


Figure 24: Return Status

2.2.8 Describe any special program that your company offers that will improve customer's ability to access products, on-time delivery, or other innovative strategies.

SHI Response:

SHI One is free to all SHI customers and empowers them to direct multi-cloud, service, and inventory management in one place by consolidating all the essential management, consumption, and cost information into a single view.



Figure 25: SHI One Platform

With visibility across IT projects, cloud consumption, licensing, and services, AEPA member agencies can identify waste and enhance decision-making capabilities with precise data. They can securely manage identity and access single sign-on and granular role-based controls. SHI One's intuitive interface and customizable dashboards present the information critical to the member agency's team's role—reports and analytics across their environment. Authorized users submit and view technical, billing, or account management support requests. Administrators control access in SHI One by adding/editing/removing users, assigning them to security groups, and granting different user permissions. SHI professional services activities can be automatically populated in SHI One, augmenting project management by providing the status, progress, updates, and results of those engagements.

SHI-One gives AEPA member agencies a 360-degree view of their multi-cloud consumption, including Microsoft Azure, Amazon Web Service, Google Cloud Platform, and Microsoft Office 365. Members can expedite cloud governance support by setting rules and parameters in one place and then leveraging SHI One dashboards to monitor policy compliance. The complete view of multiple cloud contracts and providers reveals costs, consumption, and more, allowing you to control cloud resources.

SHI One delivers a multitude of benefits that translate directly to the APEA member agency's bottom line, including:

- **Streamlined lifecycle management:** Optimize asset lifecycle, cut costs, minimize data breach risks, and maximize asset recovery value.
- **Simplified inventory and integration management:** Track Integration Center inventory, monitor configuration visibility, and seamless customization.
- **Real-time shipment and asset tracking:** Ensure delivery accuracy and enhance asset visibility and operational efficiency.

- **Custom API integration:** Connect existing tools and automate workflows.

Committed to the tool's evolution, SHI updates SHI One monthly and continues to invest in the technology to enhance functionality in support of the customer experience. We welcome the opportunity to demonstrate how this SHI tool can enable members to spend less time struggling with reports, management, and support and more time on the strategic initiatives driving their business forward.

PRICING

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD).

COOPERATIVE CONTRACTS

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary relevant details for a few questions are included here.

2.4.2 If YES, list the cooperative name and the respective expiration date(s) of your contract with the cooperative.

SHI Response:

SHI has competitively bid contracts in all 50 States. A full list of our contracts by state can be found at: https://www.shi.com/Contract/PSContract/ContractHome.



Figure 26: SHI Top Public Sector Contracts

2.4.3 If YES, and your business is awarded an AEPA contract, explain which contract your business will lead with in marketing and sales representative presentations (sales calls)?

SHI Response:

Each team member from every Public Sector vertical will support our partnership with AEPA and will advocate for the contract with passion and vigor. Given our position in the Public Sector market, the size of our sales force, and our experience with implementing and growing similar contracts, we are confident that we can extend AEPA's reach not only in terms of revenue achieved but also in terms of the number of distinct agencies who use this contract to the most benefit.

SHI supports a large portfolio of contract vehicles used by our Public Sector customers across the country. Our customers choose which contract vehicle they prefer to utilize for each procurement. SHI tracks the contract used for each procurement at the line-item level.

We will immediately contact current AEPA member agencies, introduce SHI, listen to their needs, and evaluate the best benefits they will receive from the cooperative contracts.

We will work with each member to understand their business preferences (specific information on a quote, reporting requirements, invoicing/billing requirements, and the like), and we will offer webinars on various topics including:

- Getting to know SHI
- SHI.com (eProcurement intro)
- SHI's service capabilities
- Products associated with the contract
- OEM agreements associated with the contract

We recognize why cooperative contract usage is on the rise and realize the value of having strategic partners in this space. In short, our expectations are bold, and they are also achievable. Our SHI team has the required experience with other cooperative contracts, flexible and agile, and we are committed to providing AEPA agencies an extraordinary experience with a purpose and a passion that is incomparable.

FEES

Responses to all questions of this section are included in AEPA 025 Part D Questionnaire (Q-78CD). Necessary relevant details for a few questions are included here.

2.5.4 If not, do you add on applicable shipping and handling fees separately on invoices.

SHI Response:

Reliable and secure delivery is a top priority for SHI. SHI currently leverages small parcel carriers and freight carriers for shipment of larger quantities.

SHI can ship products via any method the customer desires. These include:

- **Standard delivery**: Shipment is delivered to a fixed delivery point (such as a warehouse). Often, shipping is free. Exceptions include very large pallets (servers that are racked/stacked) and any order that requires custom configuration.
- **Overnight and second-day delivery**: This option is available for standard, in-stock items upon request. There is a fee for expedited delivery. The size and weight of the delivery determines shipping prices.

SHI can ship directly to an end user/centralized location or, where applicable, engage a freight carrier for palletized shipments to locations with a receiving area or dock. Shipping can be billed to SHI's carrier accounts or the customer's account, if preferred, with tracking provided.

2.5.6 If yes, please indicate how the rate factor is determined and indicate any other cost factors related to leasing.

SHI Response:

Purchasing new software and related hardware can be an expensive investment for even the most profitable organization. However, purchasing is not the only option: leasing and financing with SHI can be an excellent alternative to buying IT products.

The leasing/financing process is relatively simple. Our pricing models include monthly, quarterly, or annual terms, and once all documents are approved and signed, SHI ships products directly to the customer.

SHI's financial offerings include traditional and non-standard options for software financing.

Software Financing

SHI has a loan capability called an Installment Payment Agreement (IPA) which is available for transactions that are 100 percent soft cost. This option provides ownership at the end of the term for transactions that are software, and services based.

Non-Standard Options

SHI offers non-standard leasing options such as 90-day deferrals and step-up or down payment structures. SHI engages in discussions with your organization and works in good faith to accommodate non-standard terms or payment frequency.

Hardware Leasing

If the portfolio expands SHI has options for hardware leasing.

SHI offers a traditional $1 buyout purchase option, and fair market value leases for hardware. We also offer a rental option.

- Return the equipment and start a new lease.
- Extend the term of the lease.
- Buyout the equipment for its fair market value.
- Customers that do not want to have lease language in the contract or have the option to own the equipment use this structure.
- $1 buyout, lessee owns equipment at the end of the term.
- Fair market value leases have three end-of-term options.

Rental - Return the equipment at the end of term, or extend the term of the rental.



We Are SHI

We bring together
IT and Procurement
like never before

SHI's catalog is on tab 2 of the pricing workbook Part F – Pricing Schedule –SHI. Also including the link here for reference www.shi.com.

SHI International Corp. Comments to Member Agency (State) Terms and Conditions

This proposal is based on mutually agreeable terms and conditions. If SHI is a potential candidate for award, we will be pleased to discuss the details of the terms and conditions for the contract. SHI is a reseller and not the OEM. SHI will also provide professional services, as applicable. Therefore, the terms and conditions have been modified below to reflect this relationship.

Ref.	Customer Terms and Conditions	SHI Redline	SHI Explanation
Member Agency Terms and Conditions **Section 22 - Pennsylvania**	b) Termination for Cause or Convenience: For any purchase or contract in excess of $10,000 made using federal funds, the contractor agrees that the following term and condition shall apply: The KPN member may terminate or cancel any purchase order under this a contract at any time, with or without cause, by providing seven (7) business days' advance written notice to contractor. If an agreement is terminated in accordance with this Paragraph, the KPN member shall only be required to pay contractor for goods or services delivered to the KPN Member prior to the termination and not otherwise returned in accordance with Contractor's return policy. If the KPN member has paid the contractor for goods or services not yet provided as of the date of termination, the contractor shall immediately refund such payment(s).	Termination for Cause or Convenience: For any purchase or contract in excess of $10,000 made using federal funds, the contractor agrees that the following term and condition shall apply: The KPN member may terminate or cancel any purchase order under this a contract at any time, with or without cause, by providing ~~seven~~ thirty (~~7~~30) ~~business~~ days' advance written notice to contractor. If an agreement is terminated in accordance with this Paragraph, the KPN member shall only be required to pay contractor for goods or services delivered to the KPN Member prior to the termination and not otherwise returned in accordance with Contractor's return policy. If the KPN member has paid the contractor for goods or services not yet provided as of the date of termination, the contractor shall immediately refund such payment(s).	SHI requests to have 30 days for termination for convenience.
Member Agency Terms and Conditions **Section 19 – New Mexico**	Liquidated Damages: The CES Member or Participating Entity has the right to assess liquidated damages to the Contractor (and its Surety); and the Contractor shall be liable for the amount of liquidated damages as determined in the contract documents. Such liquidated damages are intended to represent estimated actual damages and are not intended as a penalty, and Contractor shall pay them to Owner without limiting Owner's right to terminate this agreement for default as provided elsewhere herein. The liquidated damages are assessed per calendar day of delay until the work is determined by CES and its Member or Participating Entity to be substantially complete. Liquidated damages will comply with the requirements of 55-2-718 NMSA 1978. Liquidated damages and early completion incentives will be between the CES Member or Participating Entity and the Contractor and must be agreed upon in writing. If the CES Member or Participating Entity declines a liquidated damages or early incentive agreement, the Contractor will ensure such agreement is reflected and included in the project's contract documents.	Liquidated Damages: The CES Member or Participating Entity has the right to assess liquidated damages to the Contractor (and its Surety); and the Contractor shall be liable for the amount of liquidated damages as determined in the mutually agreed upon contract documents. Such liquidated damages are intended to represent estimated actual damages and are not intended as a penalty, and Contractor shall pay them to Owner without limiting Owner's right to terminate this agreement for default as provided elsewhere herein. The liquidated damages are assessed per ~~calendar~~ business day of delay until the work is determined by CES and its Member or Participating Entity to be substantially complete. Liquidated damages will comply with the requirements of 55-2-718 NMSA 1978. Liquidated damages and early completion incentives will be between the CES Member or Participating Entity and the Contractor and must be agreed upon in writing. If the CES Member or Participating Entity declines a liquidated damages or early incentive agreement, the Contractor will ensure such agreement is reflected and included in the project's contract documents.	SHI requests that, in the event CES believe Liquidated Damages are necessary, the parties should mutually agreed upon the nature and amount of such damages.

SHI International Corp. Comments to Member Agency (State) Terms and Conditions

Member Agency **Terms and Conditions** Section 25 - Virginia	**12. TERMINATION FOR CONVENIENCE-**A contract may be terminated in whole or in part by the County in accordance with this clause whenever the County Purchasing Agent shall determine that such a termination is in the best interest of the County. Any such termination shall be effected by delivery to the Contractor at least five (5) working days prior to the termination date of a Notice of Termination specifying the extent to which performance shall be terminated and the date upon which termination becomes effective. An equitable adjustment in the contract price shall be made for completed service, but no amount shall be allowed for anticipated profit on unperformed services.	**12. TERMINATION FOR CONVENIENCE-**A contract may be terminated in whole or in part by the County in accordance with this clause whenever the County Purchasing Agent shall determine that such a termination is in the best interest of the County. Any such termination shall be effected by delivery to the Contractor at least ~~five~~ thirty (~~5~~30) ~~working~~ days prior to the termination date of a Notice of Termination specifying the extent to which performance shall be terminated and the date upon which termination becomes effective. An equitable adjustment in the contract price shall be made for completed service, but no amount shall be allowed for anticipated profit on unperformed services.	SHI requests that terminations for convenience be with 30 days written notice.

SHI International Corp. Comments to Member Agency (State) Terms and Conditions

This proposal is based on mutually agreeable terms and conditions. If SHI is a potential candidate for award, we will be pleased to discuss the details of the terms and conditions for the contract. SHI is a reseller and not the OEM. SHI will also provide professional services, as applicable. Therefore, the terms and conditions have been modified below to reflect this relationship.

Ref.	Customer Terms and Conditions	SHI Redline	SHI Explanation
AEPA Terms and Conditions **Audit Rights**	In accordance with applicable law of the State of the AEPA Member Agency, the Vendor Partner's books, and pertinent records related to this contract may be audited at a reasonable time and place.	In accordance with applicable law of the State of the AEPA Member Agency, the Vendor Partner's books, and pertinent records related to this contract may be audited at a reasonable time and place. Such audits shall be with thirty (30) days written notice and not more than once annually for each AEPA Member Agency unless otherwise required by law.	SHI requests additional language be added which places reasonable limitations on the number of audits and providing of notice before such audits.
AEPA Terms and Conditions **Delivery Terms, Conditions, and Requirements Section 9. Liquidated Damages**	The Buyer may suffer financial loss if the project is not substantially complete, or products or services are not delivered on the established date. The Vendor Partner (if applicable surety) must be liable for and must pay to the Buyer, not as a penalty, the sums that may be hereinafter agreed upon as liquidated damages per calendar day of delay until the work and/or delivery is determined by Buyer to be complete and/or delivered. Liquidated damages will be determined on a project-by-project basis.	The Buyer may suffer financial loss if the project is not substantially complete, or products or services are not delivered on the established date. The Vendor Partner (if applicable surety) must be liable for and must pay to the Buyer, not as a penalty, the sums that may be hereinafter agreed upon as liquidated damages per calendar day of delay until the work and/or delivery is reasonably determined by Buyer to be complete and/or delivered that is within Vendor Partner's reasonable control. Liquidated damages will be determined on a project-by-project basis.	SHI requests such determinations regarding such damages be reasonable and that such damages only be imposed when such delays within SHI's reasonable control.
AEPA Terms and Conditions **Indemnification**	Vendor Partner will indemnify, defend and save harmless AEPA, its Members, Participating Entities, its employees from any and all claims, demands, suits, proceedings, loss, cost and damages of every kind and description, including any attorney's fees and/or litigation expenses, which might be brought or made against or incurred by AEPA, its Members, Participating Entities, its employees on account of loss or damage to any property or for injuries to or death of any person, caused by, arising out of, or contributed to, in whole or in part, by reasons of any act, omission, professional error, fault, mistake, or negligence of Vendor Partner, its employees, agents, representatives, or Subcontractors, their employees, agents, or representatives in connection with or incident to the performance of this agreement, or arising out of worker's compensation claims, unemployment compensation claims, or unemployment disability compensation claims of employees of Vendor Partner, and/or its Subcontractors or claims under similar such laws or obligations. Vendor Partner's obligation under this section will not extend to any liability caused by the sole negligence of AEPA, its Members, participating Entities, its employees. The liability of AEPA, its Members, Participating Entities, or its employees will be subject in all cases to the immunities and limitations of Nevada or the AEPA Member Agency's state laws. Installation: Equipment and items of construction must be installed in accordance with the manufacturer's instructions, specifications, in accordance with any federal, state, local rules, regulations, codes, and the schedule determined by the AEPA	Vendor Partner will indemnify, defend and save harmless AEPA, its Members, Participating Entities, its employees from any and all third party claims, demands, suits, proceedings, loss, cost and damages of every kind and description, including any reasonable attorney's fees and/or litigation expenses, which might be brought or made against or incurred by AEPA, its Members, Participating Entities, its employees on account of loss or damage to any property or for injuries to or death of any person, caused by, arising out of, or contributed to, in whole or in part, by reasons of any negligent act, omission, ~~professional error, fault, mistake,~~ or negligence of Vendor Partner, its employees, agents, representatives, or Subcontractors, their employees, agents, or representatives in connection with or incident to the performance of this agreement, or arising out of worker's compensation claims, unemployment compensation claims, or unemployment disability compensation claims of employees of Vendor Partner, and/or its Subcontractors or claims under similar such laws or obligations. Vendor Partner's obligation under this section will not extend to any liability caused by the ~~sole~~ proportional negligence of AEPA, its Members, participating Entities, its employees. The liability of AEPA, its Members, Participating Entities, or its employees will be subject in all cases to the immunities and limitations of Nevada or the AEPA Member Agency's state laws. Installation: Equipment and items of construction must be installed in accordance with the manufacturer's instructions, specifications, in accordance with any federal, state, local rules, regulations, codes, and the schedule determined by the AEPA Member Agency and/or Participating Entity.	SHI requests indemnification be limited to third parties and attorney's fee be limited to reasonable. SHI also requests indemnification be limited to not

	Member Agency and/or Participating Entity.		
AEPA Terms and Conditions **Patent and Copyright Indemnification**	To the extent permitted by law, Vendor Partner must indemnify and hold harmless Member Agency and its Participating Entities against any liability, including costs and expenses, for infringement of any patent, trademark or copyright arising out of contract performance or use by Member Agency and its Participating Entities of materials furnished or work performed under this contract. Member Agency and its Participating Entities must reasonably notify Vendor Partner of any claim for which it may be liable under this paragraph.	To the extent permitted by law, Vendor Partner must indemnify and hold harmless Member Agency and its Participating Entities against any liability, including costs and expenses, for infringement of any patent, trademark or copyright arising out of ~~contract~~ Vendor Partner's performance or use by Member Agency and its Participating Entities of ~~materials furnished or~~ work performed ~~under this contract~~by Vendor Partner. Member Agency and its Participating Entities must reasonably notify Vendor Partner of any claim for which it may be liable under this paragraph.	As a reseller, SHI cannot provide IP indemnification for the products or third party services SHI sells. SHI can provide IP indemnification for services SHI performs.
AEPA Terms and Conditions **Termination for Convenience**	AEPA Member Agency reserves the right to immediately terminate this contract, without penalty or recourse, in whole or in part, if the AEPA Member Agency determines that termination is in the best interest of Participating Entities. The Vendor Partner, after receipt of a "Notice of Termination," must not accept any new orders after the termination date specified in the notice. Any termination must not affect projects that are in progress at the time the cancellation is received by the AEPA Member Agency. Vendor Partner must be entitled to receive just and equitable compensation in accordance with applicable contract pricing for work in progress, work completed, and materials accepted before the effective date of the cancellation. The Vendor Partner will not be reimbursed for any anticipated profit. The AEPA Member Agency reserves the right to cancel, or suspend the use thereof, any contract resulting from this SOLICITATION if the Vendor Partner files for bankruptcy protection or is acquired by an independent third party. Vendor Partner may cancel this contract upon written notice to the AEPA Member Agency prior to the intended termination date (or on the yearly anniversary of the solicitation). Any termination must not affect projects that are in progress at the time the cancellation is received by the AEPA Member Agency.	AEPA Member Agency reserves the right to immediately terminate this contract with thirty (30) days written notice, without penalty or recourse, in whole or in part, if the AEPA Member Agency determines that termination is in the best interest of Participating Entities. The Vendor Partner, after receipt of a "Notice of Termination," must not accept any new orders after the termination date specified in the notice. Any termination must not affect projects that are in progress at the time the cancellation is received by the AEPA Member Agency. Vendor Partner must be entitled to receive just and equitable compensation in accordance with applicable contract pricing for work in progress, work completed, and materials accepted before the effective date of the cancellation. The Vendor Partner will not be reimbursed for any anticipated profit. The AEPA Member Agency reserves the right to cancel, or suspend the use thereof, any contract resulting from this SOLICITATION if the Vendor Partner files for bankruptcy protection or is acquired by an independent third party. Vendor Partner may cancel this contract upon written notice to the AEPA Member Agency prior to the intended termination date (or on the yearly anniversary of the solicitation). Any termination must not affect projects that are in progress at the time the cancellation is received by the AEPA Member Agency.	SHI requests to have a reasonable written notice termination of the contract for convenience.
AEPA Terms and Conditions **Warranty**	Vendor Partner warrants that all commodities, supplies, materials, equipment, software, and service delivered under this contract must conform to the specifications of this contract. All items should carry a warranty equal to the intended life cycle or a minimum manufacturer's warranty that includes parts and labor unless otherwise specified in the category specifications. The manufacturer has the primary responsibility to honor a manufacturer's warranty; a distributor or dealer agrees to assist the purchaser to reach a solution in a dispute with the manufacturer over a warranty's terms. Any extended manufacturer's warranty will be passed on to the Buyer. For example, if a voice board has a three-year warranty, but the board is in a turnkey system that has a one-year warranty, the voice board's three-year warranty must be honored by the manufacturer and the Vendor Partner.	Vendor Partner warrants that all commodities, supplies, materials, equipment, software, and service delivered under this contract must conform to the specifications of this contract. ~~All items should carry a warranty equal to the intended life cycle or a minimum~~Vendor Partner will pass through all manufacturer's ~~warranty that includes parts and labor unless otherwise specified in the category specifications~~warranties. The manufacturer has the primary responsibility to honor a manufacturer's warranty; ~~a distributor or dealer~~Vendor Partner agrees to reasonably assist the purchaser to reach a solution in a dispute with the manufacturer over a warranty's terms. Any extended manufacturer's warranty will be passed on to the Buyer. For example, if a voice board has a three-year warranty, but the board is in a turnkey system that has a one-year warranty, the voice board's three-year warranty must be honored by the manufacturer and the Vendor Partner. All extended warranties must be passed on, without exception. If upon discovery, the Vendor Partner charges a Buyer for a	SHI cannot warranty all products we resell for their intended life cycle. SHI will pass through all manufacturer warranties to our customers. SHI can provide reasonable support for disagreements with manufacturer warranty terms. As a reseller, SHI disclaims certain warranties since we have no control over these.

	All extended warranties must be passed on, without exception. If upon discovery, the Vendor Partner charges a Buyer for a replacement part that the Vendor Partner actually received at no cost under a warranty, the Vendor Partner will rebate the amount billed and the Buyer reserves the right to cancel the contract.	replacement part that the Vendor Partner actually received at no cost under a warranty, the Vendor Partner will rebate the amount billed and the Buyer reserves the right to cancel the contract. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS AGREEMENT, VENDOR PARTNER HEREBY EXPRESSLY DISCLAIMS ALL WARRANTIES EITHER EXPRESS OR IMPLIED, RELATED TO PRODUCTS OR THIRD PARTY SERVICES PROVIDED BY VENDOR PARTNER HEREUNDER, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WARRANTY OF NONINFRINGEMENT, OR ANY WARRANTY RELATING TO THIRD PARTY PRODUCTS.	
ADD		**Limitation of Liability** NEITHER PARTY WILL BE LIABLE FOR ANY SPECIAL, PUNITIVE, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF OR DAMAGE TO DATA, LOSS OF ANTICIPATED REVENUE OR PROFITS, WORK STOPPAGE OR IMPAIRMENT OF OTHER ASSETS, WHETHER OR NOT FORESEEABLE AND WHETHER OR NOT A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT IN THE CASE OF A PARTY'S OBLIGATION TO INDEMNIFY FOR THIRD PARTY CLAIMS, OR BREACH OF CONFIDENTIALITY, EITHER PARTY'S TOTAL CUMULATIVE LIABILITY TO THE OTHER IN CONNECTION WITH THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR OTHER THEORY, WILL NOT EXCEED THE TOTAL AMOUNT OF FEES ACTUALLY PAID OR PAYABLE BY THE STATE TO CONTRACTOR UNDER THIS AGREEMENT FOR THE YEAR PREVIOUS TO THE INCIDENT WHICH GAVE CAUSE FOR SUCH LIABILITY. THE STATE ACKNOWLEDGES THAT SUCH AMOUNT REFLECTS THE ALLOCATION OF RISK SET FORTH IN THIS AGREEMENT AND THAT CONTRACTOR WOULD NOT ENTER INTO THIS AGREEMENT WITHOUT THESE LIMITATIONS ON ITS LIABILITY.	SHI requests there be a reasonable limitation on its liability.
ADD		**Return Policy** All returns of products, goods, equipment and/or software shall be subject to the terms of Contractor's Return Policy, which can be accessed at: **www.SHIDirect.com/ReturnPolicy**	[In resale situations, ensure SHI's return policy is referenced] If awarded, SHI requires this clause be added to the final agreement.

Sustainability and Action

2023 Report

Table of Contents

03 About SHI

04 Foreword

06 Highlights

09 Environment

19 Social

35 Governance

38 Reporting

43 SASB disclosures

About SHI

Headquartered in Somerset, NJ, SHI International Corp (SHI) is the largest minority- and woman-owned business in the United States, with major operations centers in Austin, TX and Milton Keynes, United Kingdom, and a growing local presence around the world.

Co-founder Thai Lee has served as SHI's only President and CEO. Under her leadership, SHI has grown from a regional, software-only reseller into one of the largest, privately held, global technology solutions providers in the world—while maintaining the agility, dependability, and friendliness of a small business.

SHI employs more than 6,000 employees split into strategic business units who uphold SHI's mission to be every customer's favorite technology solutions provider: "We are passionate about delivering exceptional value and experience as we help customers select, deploy, and manage technology."

Today, over 17,000 global, enterprise, commercial, and public sector organizations rely on SHI to support their transformation, collaboration, security, and optimization needs.



Founded **1989**

$14 BILLION 2023 Gross Sales

Largest US Minority and **Woman Owned** Business Enterprise

30+ Locations **Worldwide** 6,000 Employees

Global Integration Centers in U.S, U.K., NL & SG

WEConnect INTERNATIONAL Certified Women's Business Enterprise (WBE)

Supporting **80%** FORTUNE 50 | **80%** FORTUNE 100 | **65%** FORTUNE 500

ISO 9000 Certified

Our solutions

Transform

Next-generation infrastructure

Accelerate IT modernization with cloud and data center infrastructure

Collaborate

Modern workspace solutions

Prioritize employee experience, productivity, and collaboration

Protect

Advanced cybersecurity solutions

Protect your employees, data, and infrastructure

Optimize

Cost-efficient IT investments

Simplify your spend across the full IT lifecycle

At SHI, our core values guide our commitment to sustainability.

- **Build a culture of equality, inclusion, and diversity**
- **Be accountable and act with integrity**
- **Seek understanding to support sincerely**
- **Embrace change, collaborate, and innovate**
- **Show initiative and execute efficiently**
- **Be resourceful and cost-conscious**
- **Adapt, persevere, and succeed**
- **Learn, grow, and teach**
- **Strive for wellness to achieve balance**
- **Be bold, be fun, behave, and be you**

A message from the CEO

On behalf of SHI, I am pleased to present our Sustainability and Action Report for 2023.

At SHI, sustainability is a guiding principle that shapes our strategy, operations, and relationships. Throughout our history, SHI has helped our customers select, source, and manage technology to meet their business goals, and we aim to support their sustainability climate and broader sustainability objectives as well.

Climate change is a significant challenge that demands an extraordinary level of commitment, cooperation, and investment from governments, businesses, and society. In response, we are developing near-term climate targets, building on our current decarbonization efforts. We aim to submit the targets for validation with the Science Based Targets Initiative (SBTi) in 2024.

In 2023, we invested over $50 million back into our business. This investment spanned IT and infrastructure updates, facility upgrades, and business automation initiatives, where sustainability objectives were a consistent consideration. For example, we doubled the installed capacity of solar PV panels at our Ridge Integration Center. We also installed new solar lights and sensors in our parking facilities at our global headquarters in New Jersey.

We continued our investment in our people, enhancing their benefits and development opportunities with a strong focus on diversity, equity, and inclusion (DEI). In 2023, we replaced our previous learning management platform with a purpose-built platform called SHI Learn. Our employees subsequently doubled their training time, with an average investment of 49 hours per person. We continue to encourage employees to contribute to their local communities, fostering engagement and skills development. Our annual employee surveys help ensure our employee value proposition remains attractive, enabling us to retain the right talent and energy to drive our business growth.

On our business development front, we continued engaging our suppliers and customers on diversity and sustainability. We acknowledge the critical role we play as part of their value chain and remain dedicated to supporting them in their sustainability journeys. Our 2023 SHI Fall Summit was dedicated to sustainability in IT and provided our partners with opportunities to discuss such issues as efficient IT operations, strategies for sustainable lifecycles, and how to tackle IT waste with increased data security.

Looking ahead, we are excited about our progress and are committed to further integrating sustainability into our strategy and operations.

I would like to extend my heartfelt gratitude to all our stakeholders for your support and partnership in positive change. Together, we can create a more sustainable future for generations to come. I hope you enjoy reading the report, and we welcome your feedback.



Thai Lee
President and CEO
SHI International Corp.



A message from the CFO

As SHI's Chief Financial Officer and executive owner of SHI's ESG strategy, I am pleased to share our progress in integrating sustainability into our strategic planning and daily operations.

Building on our foundational commitment to diversity, equity, and inclusion (DEI) and adhering to the principles of the UN Global Compact, we have elevated sustainability to the senior management agenda and made progress in managing our impacts and disclosing information to stakeholders.

In 2023, we enhanced our sustainability management approach, disclosure, and stakeholder engagement processes. Key initiatives and achievements include:

- **Inaugural Sustainability and Action Report:** We published our first external report, detailing an inventory of key sustainability policies, activities, and metrics, and we are continuing this process with this second report.
- **Sustainability Committee:** We formed a Sustainability Committee to drive greater focus, strategic direction, and accountability for sustainability across the organization.
- **Reporting integrity:** We improved our reporting, including an independent review of our GHG inventory and continuous system enhancement of data collection automation.
- **CDP performance:** Our CDP efforts were rewarded with an improved rating of C, in line with the average score for specialized professional services and North America. We anticipate further improvement with the adoption of our climate targets in 2024.
- **EcoVadis Silver score:** We achieved a 20% increase in our overall EcoVadis score.
- **Customer engagement:** We hosted our first Sustainability Summit, fostering dialogue and collaboration with our customers and partners. It was a tremendous success all around, as we shared and learned from our joint efforts.

We're extremely proud of our sustainability journey and remain dedicated to making a positive impact on our environment, communities, and stakeholders.

Thank you for your continued support as we strive for a sustainable future.

Best Regards,

James Prior

James Prior
CFO
SHI International Corp.



Highlights



> **Sustainability is a core tenet of SHI's overall business strategy. We remain steadfast in our pledge to procure, manage, and deliver technology in an eco-conscious manner.**
>
> *James Prior,*
> *Chief Financial Officer*

2023 *sustainability highlights*

242

Recycled over
242 TONS OF CARDBOARD

RECYCLED CARDBOARD used for packaging

DARK FRIDAYS
office buildings limited light, heat, and AC

HYBRID WORKERS
reduce car emissions and power usage

9,197 SOLAR PANELS
generated over
10,191 GJ

EMPLOYEE COMMUNITY GARDEN
donated 365 pounds of fresh harvest to local food bank

BREEAM Very Good

Nexus office
BREEAM RATING VERY GOOD

U.S. Green Building Council LEED GOLD USGBC

Austin office
LEED GOLD CERTIFIED

SHI Sustainability Summit

We held our first-ever Sustainability Summit in November 2023, bringing together stakeholders across the value chain including customers, manufacturers, and suppliers. The two-day event sparked thought-provoking conversations about sustainable IT practices and set a new standard for eco-conscious events at SHI.

WHY? IT sustainability is a top business imperative for organizations, and our goal was to showcase how SHI can help make IT sustainability a fundamental aspect of our customers' organizational strategies.

By centering the conversation around sustainability, the event reflected a heightened awareness of the importance of sustainability in the IT landscape and demonstrated SHI's proactive role in driving positive change within the industry.

Key highlights

Attendees had the opportunity to engage in crucial conversations and hear diverse perspectives regarding efficient IT operations, innovations for sustainable business, strategies for sustainable lifecycles, and tackling IT waste with increased data security.

Our Sustainability Summit also highlighted four ways sustainable technology can help transform organizations:

- **Invest in a sustainable data center.** By implementing end-to-end sustainable data center solutions, organizations can reduce operational costs, energy usage, and carbon emissions and consolidate data center space.
- **Migrate and optimize workloads in the cloud.** Green cloud computing promotes remote work, optimizes resource use, and enables organizations to meet green regulations with modern IT infrastructure.
- **Responsibly redeploy and recycle aging IT.** Circular IT practices help ensure data security, reduce e-waste, and boost the circular economy.
- **Choose sustainable business financing.** By driving circular consumption of sustainable technology, organizations can count on flexible, predictable payments, minimize tech waste, offload lifecycle management, fuel innovation, and accelerate transformation.











Sustainability by the numbers

95% OF BOOTHS
rented or reused

100% OF SURPLUS MATERIALS
sent for upcycling

0 PLASTIC
water bottles used

100% OF MEALS
organic and locally sourced

100% OF FURNITURE
rented or stored for reuse

70% OF ENERGY
sourced from renewables

Environment



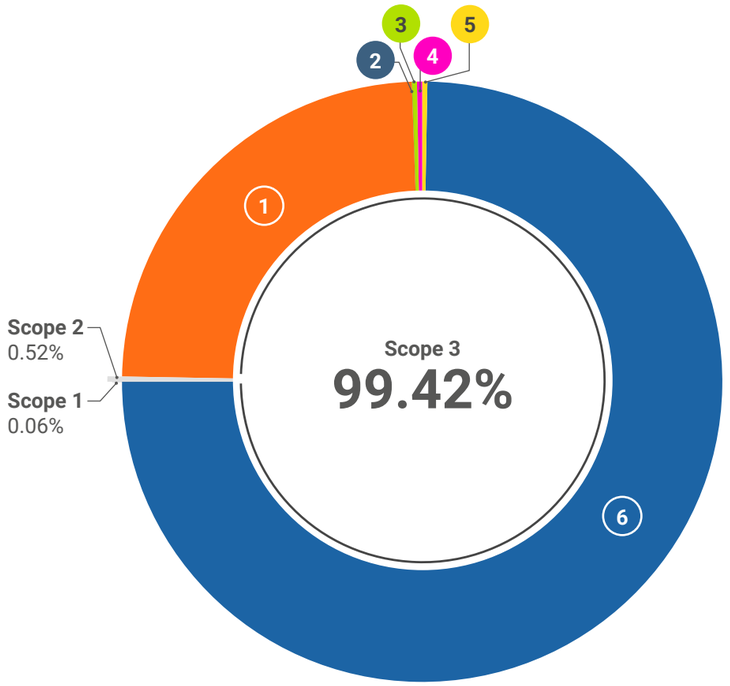
Environmental sustainability is at the heart of SHI's ethos. We acknowledge our responsibility to the planet and are dedicated to minimizing our environmental footprint.

Through the establishment and enforcement of robust global environmental policies, management systems, and performance metrics, SHI actively promotes environmental stewardship across all our locations worldwide. We have taken direct action to reduce waste within our facilities, implementing upgrades across our sites to improve energy efficiency.

Steve Alt,
Vice President of Operations

Carbon emissions profile

SHI is deeply committed to sustainability and environmental responsibility. We measure our carbon footprint using the operational control approach, which involves monitoring and measuring the greenhouse gas emissions from all operations over which SHI has control. This process allows us to gain a comprehensive understanding of our environmental impact. In our pursuit of transparency and accuracy, this data is verified by a third party, and the calculations are performed in accordance with the standards set by the Greenhouse Gas Protocol. These steps enable us to develop more effective and scientifically sound strategies to reduce our carbon footprint. In 2024, we aim to finalize the development of our science-based climate targets and submit them to the SBTi for validation. This will be a significant step in our ESG journey, following an inventory of GHG emissions, the establishment of reporting systems, and the identification and analysis of decarbonization levers.



1	Purchased goods and services (PG&S)	25.52%
2	Waste generated in operations	0.02%
3	Business travel	0.13%
4	Employee commuting	0.43%
5	Downstream transportation and distribution	0.12%
6	Use of sold products	73.19%

Total GHG emissions (MT CO2e)			
Total Scope 1 and 2 emissions (MT CO2e)	**2021**	**2022**	**2023**
Scope 1	1,032	1,302	1,279
Scope 2 (location-based)	6,426	8,440	10,310
Scope 2 (market-based)	6,677	8,760	8,897
Total Scope 1 and 2 (location-based)	**7,458**	**9,742**	**11,589**
Total scope 1 and 2 (market-based)	**7,709**	**10,062**	**10,176**

* Through third-party verification, SHI reviewed its carbon inventory management plan and identified data modeling opportunities for satellite offices. Accordingly, the 2021 and 2022 data have been updated.

2023 Total Scope 3 emissions (MT CO2e)	1,977,905
Cat 1. Purchased goods and services (PG&S)	507,770
Cat 5. Waste generated in operations	317
Cat 6. Business travel	2,653
Cat 7. Employee commuting	8,595
Cat 9. Downstream transportation and distribution	2,477
Cat 11. Use of sold products	1,456,094

SHI has conducted a comprehensive Scope 3 Materiality assessment, identifying relevant emissions categories. This was performed in accordance with the stringent criteria set by the Science Based Targets initiative (SBTi). SBTi encourages businesses to establish ambitious emissions reduction targets that align with contemporary climate science. The standards require that at least 95% of Scope 1 and 2 emissions are included within the targets. Furthermore, for companies like SHI, where Scope 3 emissions comprise ≥40% of total gross emissions (encompassing Scope 1, 2, and 3 emissions), the targets must also cover at least 67% of Scope 3 emissions.

Emissions reduction initiatives

In December 2021, we partnered with En-Power Group to develop a Carbon Reduction Plan. The reduction plan, which details short and medium-term projects, aims to help modernize our facilities and operations with progressive tools to manage our carbon footprint.

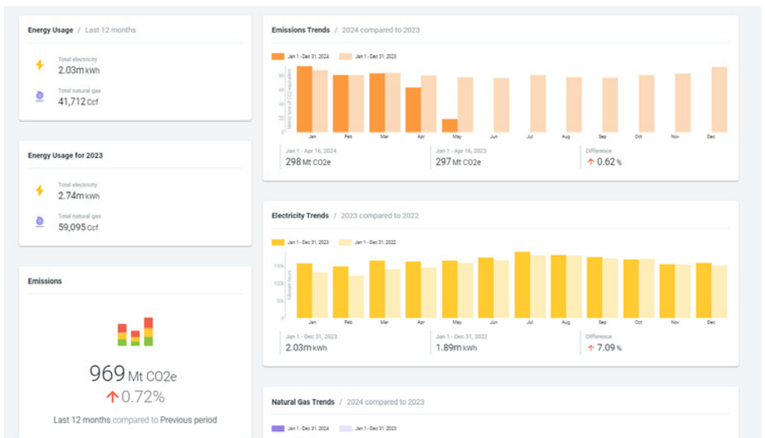
Use of renewable energy

In 2023 **SHI doubled the solar array capacity at our Ridge Integration Center** by installing 2,197 solar panels, generating an additional megawatt of capacity.

Total solar panels (NJ and TX)	9,197
Annual solar energy generation (GJ)	10,191

Monitoring energy consumption

During 2023, SHI has been monitoring the Energy Consumption and associated Carbon Emissions utilizing Atrius' Building OS system which was implemented as part of the Energy Audit conducted by our partner En-Power Group. This technology provides real-time insights, and the data points are captured directly from Utility Billing Information, reducing the risk of errors and ensuring independent verification from En-Power Group.

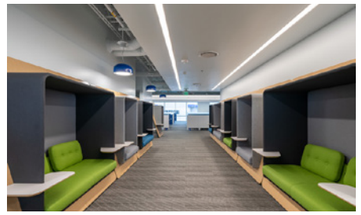


Energy efficiency in buildings

We have adjusted computer room air conditioning temperatures to reduce electricity usage, customized HVAC schedules and setpoints to better align with space occupancy throughout the day, upgraded to more efficient LED lighting, and added a reduced energy consumption functionality to the building management system.

LEED building certifications







Global HQ (NJ)
Awarded Gold for Commercial Interiors

Regional HQ (TX)
Awarded Gold for Building Design and Construction

Lower-carbon shipping

Over 96% of our U.S. product shipments are delivered by logistics providers who have partnered with the U.S. EPA SmartWay program to measure, benchmark, and improve their performance on air quality and fuel efficiency metrics related to freight transportation.



Hybrid working

We have continued our hybrid working policy in the post COVID-19 era, enabling decreased in-office operations and employee commutes. We understand the importance of in-person collaboration while also acknowledging the simultaneous benefits that hybrid working brings to our employees' physical and mental health.



CASE STUDY

SHI Office upgrades

SHI commissioned NJ-based architectural designer Cornerstone to renovate three of our office buildings: two in Somerset, NJ, and one in Bethlehem, PA. The work included reconfiguration of space, new finishes, and electrical and mechanical upgrades.

Electrical upgrades included replacing all non-LED lighting fixtures with new LED fixtures and the addition of lighting controls with motion sensors and daylight harvesting. Mechanical upgrades included the replacement of one chiller to ensure proper cooling of IT rooms and the installation of outside air intakes to provide increased ventilation rates. Where possible, the existing carpet was removed and returned to the original manufacturer for recycling. All new workstations incorporated height adjustable (sit-stand) desks, which have been shown to have positive effects on health, as well as lower panels to provide increased daylight and better access to exterior views from within the open office areas. An energy analysis will be performed to provide metrics on performance gains and energy savings.



Carpet waste environmental impact report

The impact SHI made returning 19,958 square yards of EcoWorx® carpet:

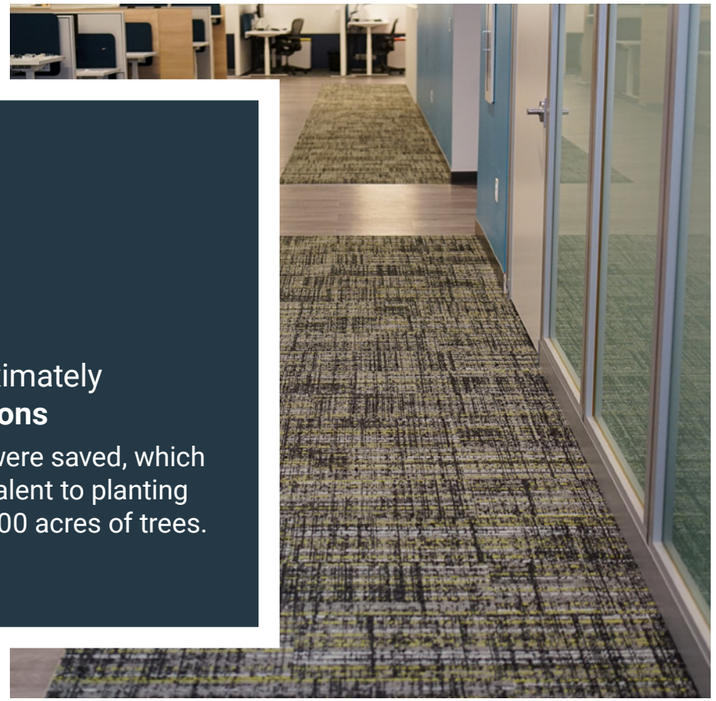
CIRCULAR ECONOMY

Approximately **54,886 tons** of old EcoWorx® carpet have been recycled, thus preventing them from going to the landfill.

CARBON IMPACT

This is the equivalent of **18,530 gallons of gasoline,** which is enough to drive 417,100 miles in an average car

Approximately **181.6 tons** of CO_2 were saved, which is equivalent to planting nearly 200 acres of trees.







CASE STUDY

Monitoring and reducing carbon emissions in France

At our SHI office in France, we have been actively monitoring our carbon footprint using Bilan Carbon, a carbon accounting method developed in France in 2004 by ADEME and now endorsed by the Bilan Carbone Association. The primary goal is to quantify all emissions directly linked to the company's operations. By conducting employee surveys, we have gathered valuable data that has provided insightful findings.

Our team has developed a heightened awareness of their carbon footprint, and has identified several carbon reduction opportunities:

- Prioritizing travel by train over air travel whenever feasible
- Opting for electric cars for rental needs
- Encouraging carpooling and ridesharing for both business and commuting purposes
- Providing education on eco-friendly driving practices and reducing consumption
- Offering incentives for using public transport and cycling for commuting
- Promoting the adoption of vegan diets for at least one day per week
- Implementing measures to reduce waste and raise awareness about energy conservation

CASE STUDY

Improving energy efficiency in the UK and supporting international climate projects

SHI performed a third-party verified Streamlined Energy and Carbon Reporting Regulation (SERC) assessment, a mandatory annual U.K. assessment to report on a company's energy use and carbon emissions, and to perform the Energy Savings Opportunity Scheme (ESOS) assessment, which enabled us to identify opportunities to improve our facilities and reduce our carbon emissions. Additionally, to achieve carbon neutrality on scopes 1 and 2, SHI purchased verified carbon standard offsets. This supported the following projects:

Verified Carbon Standard

Avoid: REDD+ protecting the Amazon

The Amazon, home to 10% of the world's species, faces severe deforestation threats, particularly in Para, where the Pacajai REDD+ Project operates. This project, certified by the Brazilian Amazon Verified Carbon Standard (VCS), prevents emissions from logging and land conversion while safeguarding biodiversity. Local villagers, trained and employed, actively protect the forest. Moreover, the project's Gold Level CCB Award, currently undergoing revalidation, underscores its outstanding social and environmental benefits.

Reduce: Providing clean cookstoves in Kenya

In Kenya, a significant 83% of households rely on traditional biomass stoves and open fires for cooking. To address this, a project was implemented to distribute locally made energy-efficient cookstoves free of charge to rural households still using outdated cooking methods. By replacing these traditional stoves and fires, the project aimed to reduce the reliance on non-renewable sources like coal and wood, thereby promoting sustainability in food preparation practices.

Reduce: Renewable energy, delivering wind generation in India

This project aims to produce clean electricity using wind energy in Maharashtra, India. It consists of 40 turbines with a capacity of 2MW each and 57 turbines with a capacity of 2.1MW each. By utilizing renewable energy, it reduces reliance on fossil fuels for electricity generation, thereby mitigating climate change effects.

Remove: Tree planting in the U.K.

This project entails planting trees in various locations throughout the U.K., such as school grounds, parks, farms, woodlands, and biodiversity sites. This not only creates habitats for wildlife but also fosters educational and community benefits. As part of the offset purchase, 45 trees were planted in the U.K.

Sustainability highlights for our U.K. office and warehouse facility, Nexus.

RATINGS AND CERTIFICATIONS

- BREEAM rating: Very Good
- EPC rating: A
- ISO 14001 certified

FRESH AIR CIRCULATION SYSTEM

installed in place of HVAC in office spaces

ELECTRIC VEHICLE BENEFITS

- Priority car parking for EVs and multioccupancy vehicles
- Free EV charging for employees and visitors

GREEN DELIVERY PARTNERS

- Primary courier: DHL
- Specialist same-day deliveries: Apollo Distribution
- International logistics: Maurice Ward

EMPHASIS ON WASTE REDUCTION AND RECYCLING

- All packaging used at Nexus contains a minimum of 30% recycled materials
  - Packaging infill is primarily paper infill rather than plastic infill
  - Packaging tape is paper rather than plastic
  - We have an onsite cardboard baler, and all waste cardboard is baled and recycled
- All waste is segregated to separate recycling/non-recycling bins.
  - Waste disposal contractor: Biffa

THERE IS AN ENVIRONMENTAL COMMITTEE

at Nexus that meets quarterly.

Minimizing environmental impact

Waste management

SHI encourages individual responsibility and supports waste minimization by:

- Ensuring maximum reuse and recycling of materials at all company facilities, including large volumes of cardboard at our integration centers
- Replacing mailed paper documents with digital PDFs
- Establishing target goals for recycling
- Complying with county and municipal recycling regulations
- Recycling toner, computers, and other office equipment according to U.S. EPA guidelines

Additionally, original equipment manufacturers (OEMs) have engaged SHI to drive a circular economy by integrating considerations around sustainable delivery. As a standard practice, we consider the entire lifecycle of a product from device manufacturing, delivery, use, and retirement. We also use environmentally friendly packing materials to ship products from our locations to the customer, consolidating shipments where possible.



Water consumption

SHI has installed water-efficient, low-flow plumbing fixtures, which reduces water usage by 40%. Our Global Headquarters in Somerset, NJ, has zero irrigation landscaping, while our Regional Headquarters in Austin, TX, has implemented systems for rainwater management. Our mechanical systems include highly efficient chillers and associated cooling towers. We have also installed water coolers throughout our offices to encourage employees to use reusable water bottles.









SHI has taken the following eco-friendly actions at our Knox and Ridge integration centers:

Carton certification
We use FSC-certified cartons for our packaging needs.

Packaging material reuse
We promote the reuse of skids and packaging material.

Recycling program
We initiated a recycling program to reduce waste.

Emission reduction
We are reducing our daily warehouse runs in order to reduce our carbon footprint.

Energy-efficient lighting
We installed LED lighting throughout Knox.

Motion sensor lighting
We installed motion sensors for some lighting to save energy.

SHI is also exploring the following:

1. We are implementing an environmental management system to help control our significant environmental impacts and improve our sustainability efforts in accordance with ISO 14001:2015
2. Waste audit: A waste audit was completed to help achieve a level of recycling that results in a zero-waste output.
3. Carbon footprint reduction: We are looking for ways to reduce the carbon footprint of our packaging materials, including the use of Airpad paper, which is made of recyclable materials.



CASE STUDY

Turning waste into charitable donations

14 tons

SHI and Green Standards diverted 14 tons of waste from landfill and raised $4,420 for charity

Any time an organization moves or renovates, much of the existing workplace – furniture, appliances, equipment, supplies – often ends up in the landfill. In fact, up to 10 million tons of these workplace assets end up in North American landfills each year. This contributes to carbon emissions and other forms of pollution while also locking away valuable materials that could be reused.

SHI chooses to partner with Green Standards on their workplace projects to ensure a better outcome. Green Standards employs charitable donation, resale, and recycling to keep workplace furniture and equipment out of landfills while generating positive local community impact.

SHI and Green Standards have collaborated since July 2023. This cumulative report highlights the environmental and social impact of all projects completed together.

SHI projects with Green Standards have resulted in:

14 tons of materials
diverted from landfill

65 tons of CO_2e
emissions avoided



SHI donation supports veterans in Arlington

Reveille Grounds aims to connect people, convene resources, and curate opportunities for veterans in Maryland. To ensure that all who live, work, play, and serve in Maryland are given the opportunity to thrive, Reveille Grounds is building a tech-empowered home base that equips military-affiliated individuals to climb the ladder of transition and continue to be community leaders.

We just obtained 6,700 sq.ft. of gorgeous, open-concept space right off of I95. Our team was thrilled to find a lease opportunity that was already configured in a way that gave us collaborative huddle rooms, plenty of coworking and "Third Space" square footage, and a large area just begging to host yoga practices, VA Claims Clinics, workforce development programs, workshops, speaker series, comedy shoes featuring veteran talent, and Open Mic Nights. The only thing the space didn't have was the furniture to activate the space and make it somewhere our veterans want to be! Thank you for sharing your office furniture with us. While we have much more to procure, we've already been able to host a few meetings and our very first monthly Muster this past Wednesday. Your gift made it possible!

Katie Kilby, Founder/President, Reveille Grounds



SHI's donations go a long way for Houston families

Since 1987, individuals, businesses, and groups have joined Houston Habitat for Humanity to build or improve a place people call home. Through shelter, they empower people to build a better future for themselves and their families by completing financial and home maintenance training, building homes alongside volunteers, and purchasing their homes with affordable mortgages. With this hand up, they achieve strength, stability, and self-reliance.

This furniture donation will strengthen our mission by allowing us to purchase materials to build more homes in Houston. The proceeds from the sale of furniture items will help Houston Habitat for Humanity procure land to continue our mission to put an end to the affordable housing crisis. This donation has helped put much-needed furniture items in the homes of people in our communities. Thank you so much!

Adam McClarin, Director, Houston Habitat for Humanity



Eternal Light enjoys much-needed donations from SHI

Eternal Light is a nonprofit charity based in Dearborn Heights, MI specializing in food distribution, food drives, and much more, including foster care orphanage.

Thank you for this donation. The items we received have been put to use in our food bank and helped in building the soup kitchen. We definitely appreciate the work the team has done for us!

Sam Bazzi, Founder, Eternal Light

SHI sustainable solutions

Broad portfolio to help customers meet their sustainable IT goals

Sustainable data center

End-to-end sustainable data center solutions

- Lower operational costs
- Reduce energy usage
- Consolidate data center space
- Lower carbon emissions
- Colocation facilities

Our services

- Data center infrastucture site survey
- Data center infrastucture management
- Data center server virtualization
- Data center colo services
- Data center server energy efficiency services
- IT emissions management on-ramp

Green cloud computing

Migrate and optimize workloads in the cloud

- Reduce carbon footprint
- Optimize resource use
- Promotes remote work
- Meets green regulations
- Modernize IT infrastructure

Our services

- Cloud migrations for sustainability
- Cloud/IT infra optimization
- App/code-level optimization
- ARM chipset adoption (Gravitron, Altra, Tau)
- FinOps and GreenOps workshop
- AWS/Azure well-architected sustainability framework

EUC/IT recycling and asset recovery

Responsible recovery and recycling of aging/retired IT

- Boost circular economy
- Ensure data security
- Redeploy old equipment
- Responsible e-waste recycling
- Extended warranties

Our services

- Asset disposal
- Asset recovery
- E-waste recycling
- Hardware redeployment
- Extended warranties
- Device lifecycle management
- Zero touch provisioning

Sustainable business financing

Drive circular consumption of sustainable tech

- Flexible, predictable payments
- Minimize tech waste
- Fuel innovation
- Accelerate transformation
- Offload lifecycle management

Our services

- Sustainable financing with SHI Capital
- Carbon removal units
- Streamlined IT procurement, integration and configuration
- Sustainable IT workshop





SHI sustainable solutions

ITAD program

SHI's IT Asset Disposition (ITAD) program is anchored on sustainable solutions, focusing on asset recovery. Through partnerships with top vendors, SHI ensures customers achieve optimal ROI on their end-of-life technology. The program prioritizes compliance with contracts, legal requirements, and environmental standards, offering a comprehensive solution for managing EOL technology responsibly.

ITAD program: 2023 environmental impact

148,423
total devices recycled

27,635
total device assets reused

59.7
tons, total device weight

191,298
Total emissions avoided (TCO_2e)

Cut data center emissions

Reduce energy usage

Improve efficiency

Streamline procurement

Consolidate and optimize workloads

Support circularity

Responsible ewaste recycling

Sustainable business models



Environmentally conscious partnerships

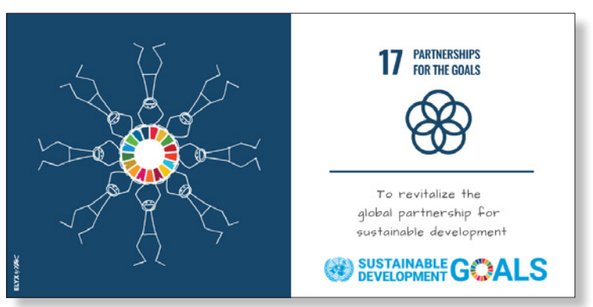
SHI is deeply committed to fostering environmentally conscious partnerships, actively engaging with our partners to promote sustainable practices within our industry. By participating in panels, partner groups, and forums, we leverage our collective expertise to develop, deliver, and shape eco-friendly solutions, amplifying our positive environmental impact.

Furthermore, our commitment extends beyond environmental sustainability. We champion diversity, equity, and inclusion and ESG initiatives. Through collaborative efforts with our partners, we drive development in tools, methodologies, and programs that promote DEI and ESG principles, aiming for both sustainable practices and high-quality end-customer experiences.

Engagement with manufacturers and suppliers

As a value-added reseller, it's crucial to establish strong relationships with our key partners. SHI actively participates in supply chain sustainability initiatives, collaborating closely with manufacturing partners such as Lenovo, Dell, HP, and Cisco.





Social



At SHI, we recognize that our employees are our most valuable asset and are invested in their holistic well-being across the four key pillars of wellness: physical, mental, financial, and community. Every employee is empowered to pursue the opportunities that best align with their own aspirations and life goals. This individualized journey reflects the shared experience of voice and choice, celebrating our culture of inclusion.

Ellen Mass,
Vice President of Human Resources

Diversity, equity and inclusion (DEI)

SHI recognizes the contributions of diverse groups to our company and country. We host webinars, panels, and interviews featuring our employees, aiming to give a voice to underrepresented groups and highlight community achievements. To this end, SHI has introduced online training modules on our internal training system to enhance employee DEI awareness and facilitate open discussions on sensitive topics. These modules are designed to help employees understand different perspectives and experiences in the workplace and promote empathy and understanding. Every employee is required to complete these trainings.

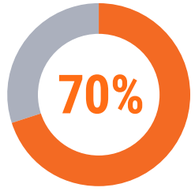
Providing a direct communication channel to our employees from the top down is integral in nurturing an environment built on equity and mutual respect across SHI's landscape. We seek to provide support and a safe space for open dialogue about complex topics with the hope that by discussing these vital topics, our collective workforce strives towards creating and maintaining an inclusive environment, especially for employees from historically marginalized backgrounds.

SHI also provides comprehensive career progression courses via our internal learning platform, SHI Learn, to help employees enhance their skills and capabilities. At SHI, we support and empower our workforce to grow professionally and thrive in their careers.



Employee Engagement

At SHI, employee feedback is crucial to upholding labour and human rights standards. We use Glint, a software platform, to measure and improve employee engagement through regular surveys. This approach helps us address concerns, foster a responsive organizational structure, and involve employees in decision-making. Our commitment to transparency is demonstrated by sharing survey results, with a 70% response rate in 2023, up from 63%. The survey focused on employees' perceptions of working conditions, well-being, and overall happiness at SHI.



response rate, up from 63%



DEI initiatives

SHI actively fosters diversity, equity, and inclusion (DEI) across its organization. As the largest minority- and woman-owned business in the United States, SHI champions programs empowering groups facing employment barriers. This commitment is rooted in the belief that a diverse workforce drives global success.

SHI's DEI initiatives are comprehensive, aiming to promote respectful communication, cooperation, and teamwork among all employees. Through robust talent acquisition and retention strategies, SHI ensures representation of diverse perspectives within our workforce. Additionally, DEI training programs equip employees with the skills to navigate multicultural environments sensitively.

Beyond internal efforts, SHI extends our commitment to DEI principles to the communities we serve, promoting greater understanding and respect for diversity. By integrating DEI into our core values and practices, SHI continues to cultivate a fair, inclusive workplace where every voice is heard and valued.

SHI's Key Diversity Initiatives

- Amplifying diverse voices
- Community outreach
- DEI training
- Employee investment
- Executive support
- Inclusive communication
- Supplier diversity

SHI aims to cultivate a varied team through active recruitment, development, and retention efforts. We engage with diversity job fairs and work closely with hiring partners who share our commitment to diversity and inclusion. Mutual respect and inclusive behavior are core expectations for all SHI employees in their daily interactions. Additionally, we foster a sense of community and belonging by supporting employee resource groups (ERGs) dedicated to celebrating diversity and enhancing our workplace culture. Each ERG is backed by a senior leader from SHI who actively engages in their events and dialogues.

Forbes 2024
BEST EMPLOYERS FOR DIVERSITY
POWERED BY STATISTA







Employee resource groups

Black Culture Collective

The Black Culture Collective at SHI is a dynamic force dedicated to uplifting, empowering, and enhancing the experiences of Black individuals both within our organization and the broader community. Through initiatives centered on leadership, education, and professional development, as well as through strategic partnerships with allies, we strive to create meaningful change. Our collective actively engages in a multitude of events that foster collaboration among members and provide opportunities for community involvement. One notable event in 2023 was the celebration of Juneteenth, where the Black Culture Collective organized block parties at our Austin and New Jersey offices. These gatherings were not only moments of celebration but also instances of community service, as our New Jersey-based members rallied to collect items for weekend meal bags donated to the Trenton Area Soup Kitchen (TASK). Additionally, local Black businesses were invited to showcase and sell their products, further enriching the festivities and supporting economic empowerment within our community.





Embrace

We are here to support one another to find and be the truest, best version of themselves. We intend to do this through mindful knowledge sharing, community-based resources, and inclusive events and programming.

Embrace, SHI's vibrant Employee Resource Group, is dedicated to fostering an inclusive and supportive environment where individuals can embrace their true selves. Through mindful knowledge sharing, community-based resources, and inclusive events, Embrace endeavors to empower its members to be their best selves. With a focus on fun, allyship, intersectionality, health, safety, education, and global inclusion, Embrace actively engages in initiatives that celebrate LGBTQIA+ diversity and advocate for positive change. From sponsoring annual pride events to partnering with organizations like Knit the Rainbow, which provides handmade items for homeless LGBTQ+ youth in NYC, Embrace is committed to making a difference both locally and globally. Whether through in-person meetups, online knit-alongs, or collaborative efforts with other Employee Resource Groups, Embrace provides a supportive space for all.





Employee resource groups

WiSH

WiSH, SHI's Women in Technology Employee Resource Group, is dedicated to celebrating and connecting the diverse voices of women in the tech industry. Our mission is to inspire, empower, and foster collaboration among all employees through a variety of events and forums held throughout the year. WiSH hosts monthly committee calls, providing a safe and inclusive space for women and allies to discuss resources available to all SHI employees, events supporting women at SHI and other ERGs, daily challenges and strategies for maintaining a healthy work/life balance, and plans for expanding WiSH's reach and impact, including local events. Additionally, WiSH actively participates in STEAM activities, aiming to support and encourage women's involvement in science, technology, engineering, arts, and mathematics. Join us in our journey to empower and elevate women in technology at SHI.







Asian Business Community

Formed in February 2024, SHI's newest employee resource group, the Asian Business Community, meets regularly to discuss and celebrate Asian heritage. The group's mission is to promote a culture of inclusion, integrity, advocacy, and education, ensuring all employees feel welcome, supported, and empowered to excel.

Planned initiatives for 2024 include:

- Quarterly members meetings and monthly newsletters to foster a culture of inclusion, integrity, advocacy, and education.
- Recognition of members who exemplify these values.
- A bagged lunches volunteer event and a food drive in honor of World Hunger Day.





Supplier diversity

Over the last 20 years, SHI's supplier diversity program has enhanced our presence in the minority business community and grown our diversity business development program to help economically strengthen diverse-owned businesses. We have an executive-level role with a dedicated team that handles supplier diversity matters.

Our supplier diversity program fosters relationships with diverse-owned companies, aligning with SHI's core values. We view diverse suppliers as vital for our success, helping us consciously source products and services while maintaining profits, growing our customer base, boosting the economy, and promoting innovation.

Every year, SHI sponsors and supports diversity-related events. In 2023, we sponsored NMSDC in Baltimore, Maryland, and WBENC in Nashville, TN. SHI currently has over 2,000 diverse partners and continues to increase the number of diverse suppliers in SHI's Managed Partner Network.

Fostering and uplifting a larger community of diverse suppliers, partners, and employees extends and enhances our service quality. As our employees' and customers' priorities change, we constantly review our objectives against diverse perspectives.



DEI awards and certifications

NATIONAL CERTIFICATION AFFILIATIONS

certified WBENC WOMEN'S BUSINESS ENTERPRISE

NMSDC National Minority Supplier Development Council | Advancing Business Connections that Count

Corporate Plus Member | New York – New Jersey MSDC | WPEO – New York

INTERNATIONAL CERTIFICATION AFFILIATIONS

CAMSC

Canadian Aboriginal and Minority Supplier Council

Certified WEConnect INTERNATIONAL Women's Business Enterprise

SHI CORPORATION UK LIMITED
SHI Global IT Solutions Ireland Limited
SHI International SAS France
SHI Singapore Solutions PTE. LTD

AWARDS AND RECOGNITION

WBENC
NY WBE Connection Award
(WBENC Regional Home Council)

AT&T | **Mega Deal Supplier Diversity Award**

Blue Cross Blue Shield Blue Care Network of Michigan
Secure Diverse Supplier Achievement Award

Aflac
Partner of the Year Award
Diversity Supplier Recognition

CRN UK
WOMEN & DIVERSITY IN CHANNEL AWARDS 2022
Gender Parity Award

Nominated by Merck for
USPAACC FAST 100 AS AN AMERICAN BUSINESS AWARD

WRMSDC
2023 Supplier of the Year

CUSHMAN & WAKEFIELD
2022 Diverse Vendor of the Year

STATE GOVERNMENT CERTIFICATIONS

STATE OF DELAWARE
STATE OF MASSACHUSETTS
STATE OF MISSOURI
STATE OF NEW JERSEY
STATE OF NORTH CAROLINA
STATE OF TENNESSEE
STATE OF VIRGINIA
STATE OF WISCONSIN

Health and safety

Working conditions

SHI has embarked upon a facilities improvement program to enhance and support workplace safety and working conditions within our office spaces. As part of SHI's ongoing commitment to employee health and wellbeing, we have introduced standing riser desks to provide our workforce with the option to alternate between sitting and standing during the workday. This change is designed to improve posture, reduce the risk of sedentary-related health issues, and enhance overall well-being. LED lighting systems have been installed throughout our facilities, offering better illumination and reducing eye strain. This ensures our employees have a well-lit workspace, contributing to their comfort and productivity. In response to feedback from our employees, SHI opted to expand desk space, removing unnecessary tabletop shelving and clutter and allowing for more organized and efficient work setups, which also functions well as a hybrid desk-sharing option. The wider desk space fosters a clutter-free and ergonomically sound workspace. We've redesigned office layouts to create an airy and spacious environment, allowing for improved circulation and a pleasant atmosphere. This redesign contributes to a more comfortable and positive work environment.







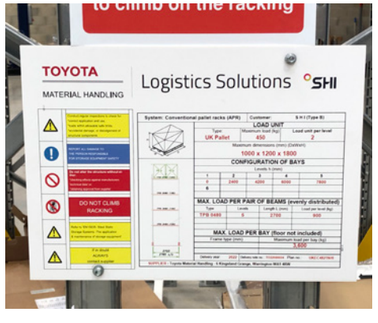
Occupational health and safety

SHI collects and analyzes health and safety performance data in compliance with local legislation and as part of our management approach. By understanding the root causes of incidents, we can identify potential hazards, assess risks, and implement preventive measures to prevent incidents and improve employee well-being, fostering a culture of safety within the organization. To improve health safety and reduce injuries, we foster a culture that prioritizes safety by carrying out regular safety training, enforcing strict safety protocols, providing appropriate personal protective equipment (PPE), conducting regular safety audits, and promoting open communication about safety concerns. Our U.K. facility, Nexus, holds ISO 45001 Occupational Health and Safety Management Systems certification, and we are actively pursuing ISO 45001 at our Knox and Ridge facilities in New Jersey.









Employee well-being

The heartbeat of SHI is our employees – all 6,000 of them. Every one of them has their own story about why they choose to work at SHI. Here's a few of their "why SHI" reasons:

Commitment to diversity.

SHI is the largest minority- and woman-owned enterprise in the United States. From employee resource groups to DEI trainings to diverse talent acquisition practices, we are passionate about building a more inclusive, more equitable workplace where every employee feels seen and valued.





Continuous professional growth opportunities.

At SHI, training doesn't stop after the first few weeks. We offer LinkedIn Learning for all employees, providing access to thousands of on-demand training modules. We have built a comprehensive leadership training curriculum for current and aspiring managers. And we're committed to helping employees attain certifications that will help them advance in their careers.





Benefits to offer peace of mind to employees and their families.

We do not want employees to lose sleep over healthcare or financial security when they work for SHI. That is why we offer comprehensive medical, vision, and dental insurance; 401(k) matching, life insurance, and flexible spending accounts; paid vacation, sick, and wellness days; and wellness programs to support their mental and physical health.





World-class facilities – in our offices or theirs.

We have over 35 offices around the globe, and each of our flagship facilities offers amenities like gyms and basketball courts to promote well-being and camaraderie, cafeterias, and even gardens where they can pick fresh enhancements for their lunches. But we also have many employees who are hybrid or fully remote. We ensure that no matter where they log in, they have the right technology to thrive in their dream roles.





Healthier Somerset

Healthier Somerset Gold Award for our employee Wellness Program

Award criteria from the Healthier Somerset Coalition: "The Healthier Somerset Coalition seeks nominations to honor companies for their outstanding achievements in implementing worksite wellness programs that improve the health and well-being of their employees."

Healthier Somerset Sustainability Award for our employee Wellness Program

Award criteria from the Healthier Somerset Coalition: "An employee wellness program that is actively continuing to grow through membership and program opportunities. Program must be active and growing for three or more years."



CASE STUDY

When we unplug

At SHI, our social community thrives through a variety of lunch break and after-hours activities designed to promote well-being and camaraderie among employees. Employees regularly gather for social events. From friendly games at the basketball and volleyball courts or softball fields in Somerset to fitness sessions at Garza Ranch's gym, there's always something to keep us active and connected.

Beyond physical activities, our social community extends to community spots where colleagues unwind and build friendships outside the office environment. These informal gatherings not only strengthen bonds but also contribute to employee well-being by providing opportunities for relaxation and socializing.

Additionally, SHI fosters a supportive environment that values employee well-being. Whether through wellness programs, mental health initiatives, or community engagement activities, we prioritize the holistic health of our team members. By promoting social interaction and offering diverse activities, we aim to create a vibrant and inclusive community where everyone can thrive professionally and personally.











"The SHI gym is an excellent destination for a refreshing energy boost during the day. Additionally, it serves as an informal setting where you can interact and catch up with your colleagues. The gym facilities are indeed one of the highly valued benefits of being an SHI employee.

I make it a point to visit the gym as frequently as I can. At SHI, I also participate in special events and classes conducted by the fitness staff. If I'm not in the gym, I'm likely to be found outdoors, taking advantage of our beautiful campus for exercise."

Christopher Bergen, Purchasing Representative



"The gym at our workplace is something I genuinely appreciate. It enables me to utilize my lunch break effectively by getting in a workout session, a good break from the continuous sitting we do all day. It's a healthier alternative to the usual routine of eating out, which only adds to our sedentary lifestyle. The cherry on top is its cost-free accessibility, making it an unbeatable perk. Moreover, it contributes to our overall well-being, helping us stay fit and healthy.

The experience is great. I have the opportunity to engage in workout sessions alongside my colleagues, which makes the experience enjoyable. Despite the fun and laughter, we still manage to maintain the seriousness of our exercise routine. After each session, I am left with a sense of accomplishment and a feeling of increased strength."

Rita Katransky, Purchasing Trainer

CASE STUDY

SHI's Gardening Club

The club cultivates more than just plants—it fosters connections among SHI colleagues, neighboring communities, and local schools. Our community garden is a vibrant hub of activity, brimming with a variety of vegetables, fruits, herbs, and flowers, all lovingly tended by our dedicated volunteers. In alignment with our commitment to sustainability, the garden is entirely organic, free from harmful chemicals, and includes diverse species of flowers to support pollinators. Beyond our core gardening group, over 100 volunteers from our Public Sector teams pitch in throughout the year, contributing to our collective efforts. In the past year alone, our harvest yielded an impressive 356 pounds of fresh produce, ranging from crisp vegetables to succulent fruits and fragrant herbs, all of which were joyfully donated to those in need.

365
pounds of produce

Our harvest yielded 356 pounds of fresh produce, ranging from crisp vegetables to succulent fruits and fragrant herbs, all of which were joyfully donated to those in need.







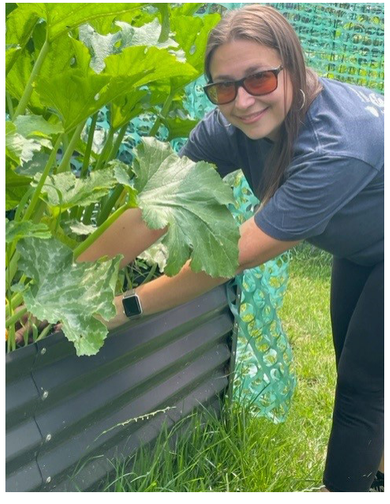














Recruitment and training

Recruitment

Recruiting and retaining a diverse workforce is essential to our success, providing us with a wealth of skills and ideas, increasing employee engagement, and tying us closer to the clients we serve within our local communities. We are committed to providing an environment of mutual respect where equal employment opportunities are available to all applicants and teammates. Our most important asset is the diverse group of employees who make up our SHI community. We acknowledge and support the collective sum of the individual differences, life experiences, knowledge, innovation, self-expression, unique capabilities, and talent that our employees bring to SHI.

To support these efforts, SHI partners with various third parties to promote our job opportunities nationally across job boards that promote diversity, such as military and veteran sites, underrepresented group sites, state job banks, colleges, universities, and more. SHI partners with vendors who are committed to providing equal access to the opportunities available at SHI and that promote diversity and inclusion. SHI.com and SHI.com/careers pages have content devoted to hiring a diverse workforce. We are also an equal opportunity employer and comply with all characteristics protected by applicable law.

Training

We have implemented online DEI training modules via our internal training system to enhance employee awareness and foster constructive dialogues on sensitive topics. These modules cover unconscious bias, how to foster inclusive teams, anti-harassment and anti-discrimination policies, and more. They are mandatory for all employees on an annual basis and are designed to encourage empathy by allowing employees to understand diverse perspectives within the workplace. Additionally, in 2023, we integrated ESG-focused training into our new hire curriculum. Our leadership and professional development initiatives also incorporate visual aids and language support to effectively promote and foster diversity principles.













SHI's community engagement

At SHI, our dedication to diversity and inclusion doesn't stop at our office doors. It permeates into the communities we call home. Our goal is to empower our employees to enrich the communities we serve, extending the values of SHI beyond corporate boundaries. We actively engage in local initiatives such as blood drives, food bank donations, and fundraising efforts for causes close to our employees' hearts. Moreover, we encourage our employees to volunteer their time and skills to support local charities and initiatives, embodying our commitment to making a positive impact on those in need.

Explore a few examples of our community involvement below:

Atlanta Community Food Bank

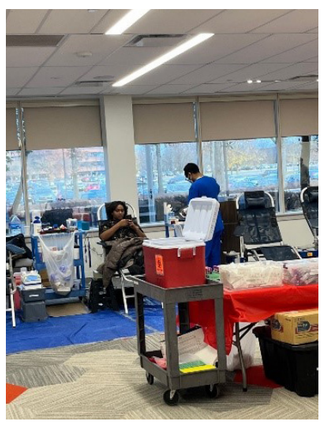
Staff from SHI volunteered their time at the Atlanta Community Food Bank, which helped to provide **37,060 pounds of food**. This equated to **3,883 meals for local residents in need**. Through these efforts, **146 families were fed**.





Blood drives with Robert Wood Johnson and other organizations

SHI hosted our annual blood drive with Robert Wood Johnson in late November. Employees were encouraged to pre-register or walk in to donate their blood. **We had over 25 employees donate their blood in NJ, and another 30 employees in Pennsylvania** donated in a separate blood drive. We aim to start hosting blood drives at our NJ headquarters twice a year.



28th Annual Legends at Woodcreek Charity Golf Tournament and Banquet

This event broke all previous years' records, **raising over $15,000 to benefit Bruno's Foundation**, a dog rescue in Lincoln, California. These funds will be used to help rescue dogs at risk of euthanasia throughout central and Northern California's shelters.



Local NJ schools

Over a dozen SHI staff members helped raise funds for two local schools in New Jersey. Through these efforts, **our team furnished students with a reading nook, bookshelves, an ottoman, floor cushions, and vital school supplies**.

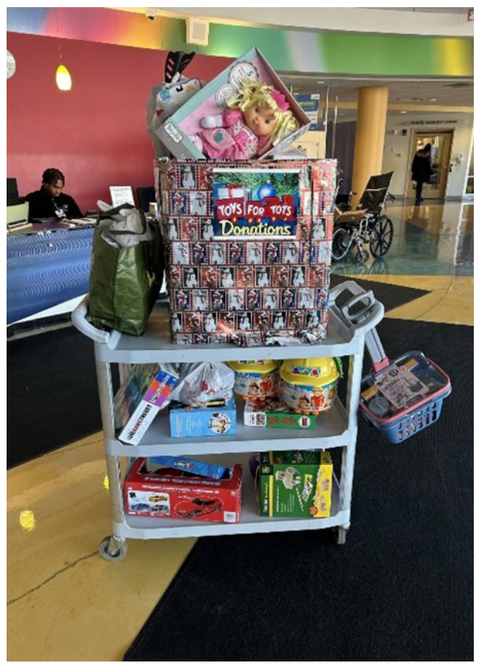




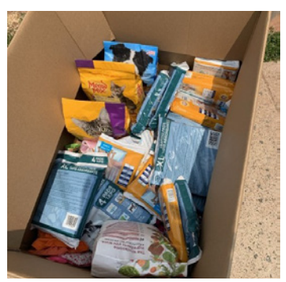


Food, clothing, toy, and pet supply drives

SHI hosts donation drives in our New Jersey and Austin locations throughout the year. In May, we hosted a donation drive for pet donations in honor of National Pet Month. We collected pet supplies and donated them to our local animal shelter. From October-January, we host an annual Giving Season in our New Jersey and Austin locations, collecting coats, clothing, food, and toys to donate to the following organizations: Casa Marinella (Clothing, Austin, TX), Central Texas Food Bank (Food, Austin, TX), RWJ Specialized Children's Hospital (Toys, New Brunswick, NJ), Franklin Food Bank (Food, Somerset, NJ), and Jersey Cares (Coats, NJ).





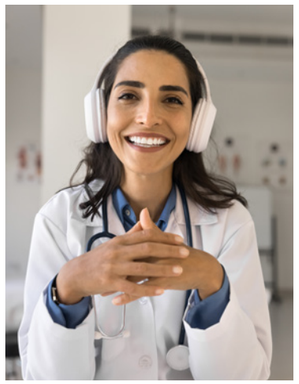


SHI's community engagement

Leukemia and Lymphoma Society volunteer opportunities

On April 5, 2023, SHI hosted a virtual webinar with the Leukemia and Lymphoma Society to provide employees with information on volunteer opportunities in their local communities with the organization. Over 30 employees participated in the webinar, with a subset joining the volunteer activities.

Robert Wood Johnson mental health and nutritional health webinars



SHI regularly partners with Robert Wood Johnson professionals for educational webinars. In 2023, we hosted a webinar on May 12 for Mental Health Awareness Month. Additionally, we hosted a webinar on March 31 for National Nutrition Month. We had around **200 participants** in both webinars, and we hope to continue hosting these events annually.

Local park cleanups



The Black Culture Collective partnered with the International WeLoveU Foundation, a Korean-owned nonprofit, to collect **41 bags of trash weighing 1,025 pounds and 18 bags of recyclables weighing 270 pounds**. Additionally, our team painted over two large graffitied walls, amphitheater stairs, and railings, and planted seeds.

Trenton Area Soup Kitchen

Several members of SHI's Black Culture Collective group volunteered at the Trenton Area Soup Kitchen (TASK) in New Jersey. **The team provided nourishing meals to 187 individuals** and **donated food parcels** collected during their Juneteenth food drive. This act of generosity further exemplified their dedication to positively impacting the community.





SHI Meals on Wheels group

For the past 13 years, every Monday, the SHI Meals on Wheels group members have been delivering food to 6-8 elderly and disabled clients within their local south Austin area. In December 2023, SHI employees assembled holiday gift bags for these regular clients. The impact of this ongoing initiative has provided these clients with a sense of security, companionship, and community support. SHI employees are filled with a sense of purpose and satisfaction, knowing they are making a meaningful difference in the lives of others.



Big Brothers Big Sisters of Central Texas

An SHI staff member has been deeply involved with Big Brothers Big Sisters, dedicating over seven years to mentoring a young man named Javon. Through this mentoring program, our employee provided guidance and support to Javon, who has since entered the Navy at the age of 18. Their ongoing relationship is a testament to the positive impact of mentorship.

In addition to his mentorship role, our employee organized a toy drive and collected donations from over 30 SHI employees, resulting in **$400 worth of gift cards** distributed to children at the organization's Christmas party. Moreover, our employee's commitment extended beyond his personal time investment, as he estimated around **$2,000 was raised collectively by SHI employees for events like Bowl for Kids and the annual Ice Ball Gala**.

These initiatives not only provide financial support but also foster community engagement and support for young people in need of positive role models who may come from low-income or disadvantaged families.





SHI's community engagement

Christmas toy drive

During the 2023 holiday season, nearly **30 SHI employees** donated money to purchase toys for local children in Austin, TX. Toys were purchased and personally delivered to the following initiatives: Any Baby Can, Toys for Tots, Blue Santa, SAFE Children's Shelter, and Big Brother Big Sisters. This initiative is an annual event, typically taking place once a year in November, with donations collected by December, fostering continued support and engagement from SHI staff.





Hill Country Nursing and Rehab Center

Our SMB Cares Organization partnered with HPE to **spread love during Valentine's Day** by delivering roses and handmade cards to the Hill Country Nursing and Rehab Center.





The Beanhill Community Garden

Six SHI volunteers dedicated their well-being days to supporting The Beanhill Community Garden in Milton Keynes, U.K. They weeded, cleared up, and disposed of the rubbish, leaving behind a pristine environment for the local community. The impact was tangible, as the tidy space now serves as a valuable learning resource for the nearby primary school. Managed by the Woughton Community Council, it fosters community engagement and educational opportunities.





Ronald McDonald House

The IT Fun and Giving Committee in Austin, TX, organized a successful Rose Sale, with **all proceeds benefiting the Ronald McDonald House of Central Texas**.

Stacy Albrecht, Chief Advancement Officer at Ronald McDonald House Charities of Central Texas, wrote in to express gratitude for the support:

"Grateful. It's one of the words that comes up most often when we read notes from the families at Ronald McDonald House Charities of Central Texas. They are grateful to have a comfortable place to stay near their hospitalized child, a warm meal, and the kindness of our staff, volunteers, and friends like you."

Thank you for your amazing support. The kids and families at Ronald McDonald House Charities of Central Texas are facing difficult times, but because of you they won't face them alone. A family who recently stayed in one of our Ronald McDonald Family Rooms summed it up perfectly:

"It's been hard having him here but it would have been so much harder if we couldn't be close to him."

Please know that your generosity is already hard at work. Thank you again for helping families stay close to each other and for the care their children need.

Elijah's Promise Charity

The IT Fun and Giving Committee at SHI received tremendous support as **46 participants** assembled snack bags and boxed them for delivery. It was a gratifying experience for all involved. In total, **80 snack bags** were prepared and delivered to the local food bank, Elijah's Promise, located in New Brunswick, NJ. All donations originated from the IT department in Somerset, NJ.







Supply chain

SHI's Supply Chain department conducts reviews to assess current practices and identify areas for enhancement in alignment with our sustainability objectives. The review emphasizes policy and compliance, supplier assessment, environmental impact, social responsibility, risk assessment, and performance metrics. It aims to drive innovation, align with industry reporting standards, and leverage best practices from Fortune 100 partners and customers. Specific objectives include evaluating supplier sustainability initiatives, ensuring compliance with SHI's ethical standards, and enhancing the procurement strategy. Our Sustainable Procurement Policy and Framework provide guidelines for purchasing decisions, reflecting SHI's commitment to sustainability, ethical practices, and social responsibility.

Where possible, our Supply Chain department seeks to minimize its environmental impact, optimize resource usage, and uphold ethical labor practices throughout the supply chain lifecycle.

SHI dispatches shipments to customers by logistics providers enrolled in the U.S. EPA SmartWay program to measure, benchmark, and improve their performance on air quality and fuel efficiency metrics related to freight transportation.

The SmartWay program helps companies advance supply chain sustainability by measuring, benchmarking, and improving freight transportation efficiency.



SmartWay®

Governance



We believe that effective governance is crucial for our development and business strategy at SHI. By promoting transparency and accountability, we aim to enhance decision-making and ensure timely implementation. Our ESG efforts, such as establishing a new Sustainability Committee and publishing our first Sustainability and Action Report, have contributed to advancing our governance. We are dedicated to continuously improving on this journey.

Kuli Sidhu,
Director of Business Assurance and ESG

SHI's commitment to ethics and integrity

The SHI Code of Ethics, Anti-Bribery, Anti-Corruption, and Whistleblowing Policy, which applies to all officers and employees, serves as the foundation for high standards of integrity and ethics throughout all levels of our organization, the deterrence of wrongdoing, and the promotion of compliance with applicable regulations. These policies and processes are overseen by General Counsel and are readily available to all employees.

Audit Committee

At SHI, we believe in robust and transparent corporate governance. An integral part of this commitment is our Audit Committee, a committee comprising our Executive Leadership, chaired by CFO James Prior. The Audit Committee meets quarterly and provides oversight for the integrity of our financial reporting, internal controls, and compliance with laws and regulations. The Audit Committee is the cornerstone of our commitment to maintaining ethical practices and high standards of corporate governance.

Sustainability Committee

At SHI, our Sustainability Committee plays a pivotal role in fostering environmental stewardship and social responsibility throughout our operations. Headed by CFO James Prior, supported by the ESG Department and comprising representatives from various departments, the committee convenes bimonthly to assess our sustainability performance, identify areas for improvement, and develop strategies to minimize our environmental footprint. By meeting regularly, we ensure ongoing progress and alignment with our sustainability goals. Recent initiatives have included implementing energy-saving measures, reducing waste through recycling and composting programs, and promoting employee engagement in sustainability practices. Through collaborative efforts and innovative projects, our Sustainability Committee strives to drive positive change within our organization and contribute to a more sustainable future for all stakeholders.



Cybersecurity and data privacy

At SHI, our commitment to sustainability extends beyond environmental practices to encompass the security and privacy of information vital to our business, customers, and employees. Our cybersecurity and data privacy initiatives adhere to stringent state and global data privacy laws and cybersecurity frameworks, including the California Consumer Privacy Act (CCPA) and European Union (EU) General Data Protection Regulations (GDPR).

Our cybersecurity and data privacy programs are continuously updated and incorporate robust physical, administrative, and technical controls to safeguard our systems, networks, and sensitive data. Aligned with ISO 27001, NIST, PCI DSS, SOC 2, and Cyber Essentials frameworks, our cybersecurity and data privacy programs are at the forefront of industry standards.

Our cybersecurity department oversees all aspects of our security strategy, from proactive risk management to ongoing education for our workforce. Comprising seven specialized teams, including security engineering and architecture, offensive security, and threat and vulnerability management, we ensure comprehensive protection against evolving threats.

For further insight into our cybersecurity and data privacy initiatives, please reach out to your SHI sales representative for access to our detailed Cybersecurity and Data Privacy Overview documentation. Together, we remain steadfast in our commitment to sustainability through robust cybersecurity practices.

Risk management

SHI consistently conducts thorough assessments to identify and address potential threats with the greatest impact on the organization. These assessments meticulously analyze the convergence of assets, threats, and vulnerabilities to create a comprehensive risk profile.

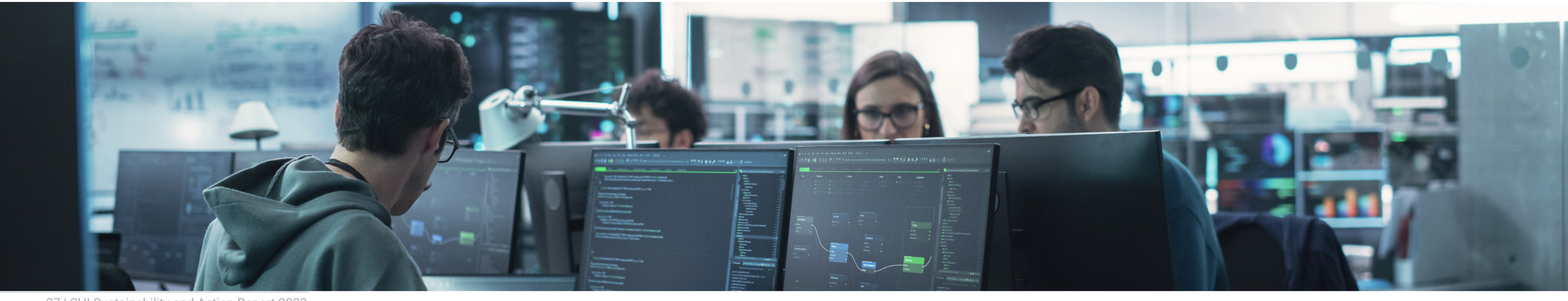
The Risk and Resiliency Steering Committee, comprised of SHI's Executive Leadership Team, spearheads the establishment of the organization's global risk management strategy. This committee plays a pivotal role in major decision-making related to operational risk, including oversight of the Business Continuity Program and the Core Team. Empowered by the committee, designated representatives can assess and declare business continuity incidents, activating appropriate portions of our Business Continuity/Disaster Recovery (BC/DR) Plans.

SHI prioritizes the development and refinement of detailed Business Continuity and Disaster Recovery Plans, regularly testing their efficacy to ensure critical processes and operations can be swiftly restored. Dedicated resources bolster contingency planning, disaster recovery initiatives, and incident response efforts.

Key elements of SHI's planning approach include:

- Identification of alternate physical site locations and readiness
- Strategic human capital resource planning and coverage models
- Ensuring network and telecommunications accessibility
- Robust cybersecurity incident response and management protocols
- Critical system backup and recovery procedures
- Cultivation of strong supplier and third-party partnerships supported by formal agreements.

SHI's Risk Management framework emphasizes effective and efficient practices aligned with ISO 31000 standards, highlighting the value and intent behind risk management efforts. Additionally, SHI conducts third-party assessments of operational vendors to evaluate their control environments against established standards and accepted information security practices.



Reporting



"We understand that our sustainability reporting integrity reflects our approach to financial reporting. Transparent reporting on our sustainability progress is not just about compliance; it is a crucial part of our corporate responsibility and a commitment to our stakeholders. It allows us to accurately measure our impact on the environment and society, establish meaningful goals, and track our progress with the same diligence we apply to our financial results. By openly discussing our achievements and areas requiring improvement, we build trust and ensure that our sustainability efforts align with our corporate values and long-term strategic objectives. We believe that transparency is essential for sustainability, and we are dedicated to keeping all stakeholders informed about our progress."

James Prior,
Chief Financial Officer

Material ESG topics

We recognize the importance of transparency and accountability in our sustainability efforts. Through a materiality assessment, we have identified key sustainability topics that are significant to our stakeholders and have a substantial impact on our business operations. These material topics encompass environmental, social, and governance aspects of our operations. Our sustainability strategy and reporting are aligned with addressing these material topics, demonstrating our commitment to responsible business practices and long-term value creation for all stakeholders.

ENVIRONMENTAL

Circular economy
Energy consumption and emissions
Energy-efficient IT
Environmental management
GHG emissions
Logistics and packaging
Waste management
Water

SOCIAL

Business diversity
Community engagement
Diversity, equity, and inclusion
Employee wellbeing
Occupational health and safety
Learning and Development
Responsible supply chain
Supply chain responsibility

GOVERNANCE

Ethics and compliance
Information security and data protection
Risk management

Regulatory disclosures

SHI adheres to global regulatory disclosure requirements. As a private company, we are subject to fewer disclosure regulations than a public company; however, we promptly submit data requests to regulatory bodies around the world. Examples include France's mandatory carbon disclosures and the U.K.'s mandatory gender pay gap reporting. In addition to regulatory disclosures, we also submit voluntary disclosures to EcoVadis and CDP, as outlined in the Framework Alignment Section.

SHI Corporation UK Limited recently conducted its second annual gender pay gap report in accordance with the U.K. Government's regulations. By regularly examining and analyzing the pay disparities between genders, we can identify areas where gender biases may exist within our compensation practices. This allows SHI to implement targeted strategies to address these disparities and ensure that employees are compensated fairly for their work, regardless of gender. View our 2023 U.K. Gender Pay Gap Report.



Framework and standards alignment

SHI supports and participates in the following sustainability frameworks and standards:

SUSTAINABLE DEVELOPMENT GOALS

The Sustainability Development Goals (SDGs) are a set of 17 global objectives focused on tackling issues such as poverty, hunger, education, healthcare, gender equality, clean energy, environmental conservation, and peace. They provide a framework for international cooperation to build a more sustainable and equitable world for all.

We have aligned ourselves with eight of these goals:



United Nations Global Compact

The United Nations Global Compact (UNGC) is a voluntary initiative that encourages businesses and organizations to adopt sustainable and socially responsible policies and practices. It provides a framework for companies to align their operations and strategies within ten universally accepted human rights, labor rights, environment, and anti-corruption principles. Signing up for the Global Compact includes a commitment to submit an annual Communication on Progress (COP) report. In 2022, SHI signed up with the UNGC and publicly declared our commitment to sustainable development and responsible business practices.

CDP

CDP is a global nonprofit that helps organizations disclose their environmental impacts, focusing on climate change, water security, and deforestation. They promote transparency and action to address environmental risks and opportunities.

SHI participates in the annual CDP climate and water assessment, and our most recent 2023 assessment results are as follows:

Climate Change score: C
Supplier Engagement score: B -
Water Security score: D

SASB

The International Financial Reporting Standards Foundation(IFRS Foundation) develops global accounting and sustainability disclosure standards, known as IFRS Standards. These include SASB's sustainability accounting standards, which govern how companies disclose environmental, social, and governance (ESG) information to investors.

Please refer to page 43 for our list of SASB standards report.

ecovadis

EcoVadis is a platform that assesses and rates companies' sustainability practices. It helps businesses understand their strengths and weaknesses, benchmark against peers, build reputation, manage risks, collaborate with suppliers, and access markets. It promotes responsible business practices and sustainability integration. Every year, SHI completes an EcoVadis assessment that evaluates our business practices within four areas: environment, ethics, sustainable procurement, and labor and human rights.

EcoVadis uses a rating scale ranging from 0 to 100. The scores are based on evidence-based qualitative and quantitative factors, considering the company's policies and practices.

This year, SHI increased our score from 52 (Bronze medal) to 62. EcoVadis awarded us our first Silver medal for our efforts.



Framework and standards alignment

GREENHOUSE GAS PROTOCOL

The GHG Protocol is a globally recognized initiative establishing standardized frameworks for measuring and managing greenhouse gas (GHG) emissions. It covers many entities, including private and public sector operations, value chains, and mitigation actions. The GHG protocol provides comprehensive guidelines and tools to help organizations accurately measure, report, and manage their GHG emissions. SHI utilizes these guidelines to help manage and reduce our environmental impact while contributing to sustainability efforts.

SCIENCE BASED TARGETS

Science-based targets provide companies with a clearly defined path to reduce emissions in line with the Paris Agreement goals. The Science Based Targets initiative (SBTi) provides a recognized framework for setting science-based targets aligned with the goals of the Paris Agreement. It is a collaborative initiative between several organizations, including the United Nations Global Compact (UGNC), the World Resources Institute (WRI), and the World Wide Fund for Nature (WWF).

Streamlined Energy and Carbon Reporting Regulation (SECR)

Streamlined Energy and Carbon Reporting (SECR) is a mandatory reporting framework in the U.K. aimed at increasing transparency around energy consumption and carbon emissions for large organizations. It applies to U.K.-incorporated companies and limited liability partnerships (LLPs) that meet certain criteria regarding energy usage and employee count. SECR has been implemented in the U.K. to help businesses understand and manage their energy consumption and carbon emissions better. Find out more information about our report on page 13.

Energy Savings Opportunity Scheme (ESOS)

Energy Savings Opportunity Scheme (ESOS) is a mandatory energy assessment scheme in the U.K. aimed at increasing energy efficiency and reducing carbon emissions for large enterprises. ESOS applies to U.K.-based organizations that meet certain criteria regarding energy usage, such as having over 250 employees or an annual turnover exceeding a specified amount. ESOS has been implemented in the U.K. to help businesses identify energy saving opportunities and improve their overall energy performance. Find out more information on page 13.

Partnerships to enhance data quality

We work with third-party consultants to measure our carbon emissions data against Scope 1, 2, and specifics of Scope 3. Moving forward, we plan to include more Scope 3 data that has been recently identified as relevant to our business within our annual reports. For more information, see page 10.



Appendix:

Sustainability Accounting Standards Board ("SASB") Disclosure

The Sustainability Accounting Standards Board is an independent non-profit organization that sets standards to guide the disclosure of financially material sustainability information by companies. The SASB reporting standards are sector specific, covering ESG reporting criteria for 77 different industries. Each SASB standard defines a minimum set of ESG-related topics that are reasonably likely to affect a company's long-term performance based on the industry it operates within. For SHI, the most relevant industry group is Software and IT Services. Certain accounting metrics within the SASB Standard for Software and IT Services were deemed not material or not relevant based on SHI's business model. These metrics would be explicitly omitted based on allowable justifications by SASB.

Appendix

Table 1. Sustainability Disclosure Topics & Accounting Metrics

Material Topic	SASB Code	Accounting Metric and Disclosure
Environmental Footprint of Hardware Infrastructure	TC-SI-130a.1	*(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable* (1) Total Energy Consumed – 112,271 GJ (2) Percentage Grid Electricity – 91% (3) Percentage Renewable – 9% Note: • Energy amounts were converted from kWh to GJ using standard conversion of 1 GJ = 277.8 kWh. • Percentage Renewable includes renewable energy from solar panels installed at SHI facilities.
	TC-SI-130a.2	*(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress* (1) Total water withdrawn - 16,855,683 gallons (63,806 cubic meters) (2) 0% from regions with High or Extremely High Baseline Water Stress Note: • Using the WRI Aqueduct tool, SHI determined that SHI locations with water metrics (addresses in New Jersey and Texas) do not fall in the High or Extremely High Baseline Water Stress range. SHI determined that their locations with water metrics (addresses in New Jersey and Texas) do not fall in the High or Extremely High Baseline Water Stress range.. • New Jersey locations are Medium – High (20-40%) • Texas locations are Low – Medium (10-20%)
	TC-SI-130a.3	*Discussion of the integration of environmental considerations into strategic planning for data center needs* **Omitted** – This metric is not relevant to SHI's operation.

Appendix

Table 1. Sustainability Disclosure Topics & Accounting Metrics (continued)

Material Topic	SASB Code	Accounting Metric and Disclosure
Data Privacy & Freedom of Expression	TC-SI-220a.1	*Description of policies and practices relating to behavioral advertising and user privacy* SHI's Data Privacy program is compliant with state and global Data Privacy laws and regulations, including the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR). • SHI designates a Data Protection Representative to oversee the Data Privacy program. • SHI regularly engages a multi-national law firm to ensure our policies and procedures remain compliant with updates to Data Privacy laws and regulations. • SHI provides consumers certain rights with respect to their personal information. These rights include the rights to deletion, to be informed, to opt out, to access, to have data portability, and not to be subject to discrimination for the exercise of these rights. • Where SHI has been engaged by our corporate customers to process personal information on behalf of the corporate customer, SHI's Terms and Conditions include Data Protection Agreements as applicable to the services. • SHI identifies operational vendors with whom SHI shares personal information and signs Data Protection Agreements with these vendors as applicable to the services.
	TC-SI-220a.2	*Number of users whose information is used for secondary purposes* **Omitted** – This metric is not relevant to SHI's operations.
	TC-SI-220a.3	*Total amount of monetary losses as a result of legal proceedings associated with user privacy* **Omitted** – This metric is not relevant to SHI's operations.
	TC-SI-220a.4	*(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure* **Omitted** – This metric is not relevant to SHI's operations.
	TC-SI-220a.5	*List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring* **Omitted** – This metric is not relevant to SHI's operations.
Data Security	TC-SI-230a.1	*1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected* **Omitted** – This metric is not relevant to SHI's operations.
	TC-SI-230a.2	*Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards* See Cybersecurity and Data Privacy under the Governance section of this report.

Appendix

Table 1. Sustainability Disclosure Topics & Accounting Metrics (continued)

Material Topic	SASB Code	Accounting Metric and Disclosure
Recruiting & Managing a Global, Diverse and Skilled Workforce	TC-SI-330a.1	*Percentage of employees that are (1) foreign nationals and (2) located offshore* **Omitted** – This metric is not relevant to SHI's operations.
	TC-SI-330a.2	*Employee engagement as a percentage* SHI performs annual employee engagement surveys through Glint. Employee participation in 2023 was 70%, up from 63% in 2022.
	TC-SI-330a.3	Percentage of people managers with one or more racial/ethnic backgrounds: 23% Percentage of people managers who identify as female: 32% Percentage of technical staff with one or more racial/ethnic backgrounds: 63% Percentage of technical staff who identify as female: 7% Percentage of all other employees with one or more racial/ethnic backgrounds: 33% Percentage of all other employees who identify as female: 36%
Intellectual Property Protection & Competitive Behavior	TC-SI-520a.1	*Total amount of monetary losses as a result of legal proceedings associated with anticompetitive behavior regulations* **Omitted** – This metric is not relevant to SHI's operations.

Appendix

Table 1. Sustainability Disclosure Topics & Accounting Metrics (continued)

Material Topic	SASB Code	Accounting Metric and Disclosure
Managing Systematic Risks from Technology Disruptions	TC-SI-550a.1	*Number of (1) performance issues and (2) service disruptions; (3) total customer downtime* **Omitted** – This metric is not relevant to SHI's operations.
	TC-SI-550a.2	*Description of business continuity risks related to disruptions of operations* SHI has dedicated resources to support its contingency planning and disaster recovery program. Key features of SHI's planning process include alternate physical site location and preparedness, human capital resource planning and coverage models, network and telecommunications accessibility, critical system backup and recovery, and supplier/third-party agreements. The business continuity management (BCM) program consists of policies that govern the health and validity of the framework. The policies and guidelines align to ISO 22301 and incorporate industry best practices. See Cybersecurity and Data Privacy and Risk Management under Governance section of this report for further details.

Table 2. Activity Metrics

SASB Code	Activity Metric and Disclosure
TC-SI-000.A	*(1) Number of licenses or subscriptions, (2) percentage cloud based* **Omitted** – This metric is not relevant to SHI's operations.
TC-SI-000.B	*(1) Data processing capacity, (2) percentage outsourced* **Omitted** – This metric is not relevant to SHI's operations.
TC-SI-000.C	*(1) Amount of data storage, (2) percentage outsourced* **Omitted** – This metric is not relevant to SHI's operations.

Appendix

Table 3. Waste Metrics

Other	Activity Metric and Disclosure
Waste Management	Total weight of waste: 814 tons Total weight of general waste: 446 tons Total weight of hazardous waste: 0 tons Total weight of waste recycled: 368 tons Total weight of WEEE-waste collected: 59.7 tons

Table 4. Accidents and Injuries

Other	Activity Metric and Disclosure
SHI Global Accident and Injury Stats	Lost time injury (LTI) frequency rate for direct workforce: 0.55% Lost time injury (LTI) frequency rate for temporary workers: 0 Lost time injury (LTI) severity rate for direct workforce: 0.27 Lost time injury (LTI) severity rate for temporary workers: 0.27 Number of days lost to work-related injuries, fatalities, and ill health: 27 Number of fatalities as a result of work-related injuries and ill health: 0 % of all operational sites for which an employee health & safety risk assessment has been conducted: 100%

Part E – Signature Forms

AEPA 025-F
Cyber Security and Training

Instructions

Contained herein are forms that **require a signature** from an authorized person at your company. All items found within this document are **mandatory**. Failure to sign the required areas, sections, or signature lines may lead AEPA to consider your company's proposal as **non-responsive**.

To submit the required signed forms, follow these steps:

1. Read the documents in their entirety.
2. Complete all forms and sign when required.
3. Return the forms and pages in their correct order and scan one (1) single PDF format titled ***"Part E – Signature Forms – Name of Responding Company"*** (i.e. one PDF document for all signature forms).
4. Submit Part E, along with other required documents in Bonfire.

*Note, a solicitation checklist has been provided to review with your submission.

The following sections will need to be completed prior to submission as one (1), single PDF titled "Part E – Signature Forms – Name of Responding Company".

Uniform Guidance "EDGAR" Certification Form – ****signature required***
Solicitation Affidavit – ****signature required***
Acceptance of Solicitation & Contract – ****signature required***

Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7. Clean Air Act and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended, contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein.		
Respondent Certification (By Item)	**Respondent Certification:** **YES**, I agree	**Initial**
1. Violation of Contract Terms and Conditions	YES, I agree	MM
2. Termination for Cause of Convenience	YES, I agree	MM
3. Equal Employment Opportunity	YES, I agree	MM
4. Davis-Bacon Act	YES, I agree	MM
5. Contract Work Hours and Safety Standards Act	YES, I agree	MM
6. Right to Inventions Made Under a Contract or Agreement	YES, I agree	MM
7. Clean Air Act and Federal Water Pollution Control Act	YES, I agree	MM
8. Debarment and Suspension	YES, I agree	MM
9. Byrd Anti-Lobbying Amendment	YES, I agree	MM
10. Procurement of Recovered Materials	YES, I agree	MM
11. Profit as a Separate Element of Price	YES, I agree	MM
12. General Compliance with Participating Agencies	YES, I agree	MM
13. Governing Law; Forum Selection.	YES, I agree	MM

SHI International Corp.
Name of Business

Moitrayee Majumdar
Signature of Authorized Representative

Moitrayee Majumdar
Printed Name

08/28/2024
Date

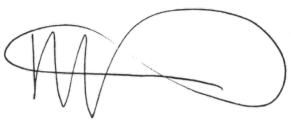
Solicitation Affidavit

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

Moitrayee Majumdar	290 Davidson Ave.
Authorized Representative (Please print or type)	Mailing Address
Senior Proposal Specialist	Somerset, NJ 08873
Title (Please print or type)	City, State, Zip
Moitrayee Majumdar	08/28/2024
Signature of Authorized Representative	Date

Please review SHI Exception Document uploaded as a separate file attached under the supporting information section of the portal.



MAYA LYNCH
Commission # 50211505
Notary Public, State of New Jersey
My Commission Expires
June 28, 2028

8/28/2024

Acceptance of Solicitation & Contract

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	SHI International Corp.	**Date**	08/28/2024
Address	290 Davidson Ave.	**City, State Zip**	Somerset, NJ 08873
Contact Person	Moitrayee Majumdar	**Title**	Senior Proposal Specialist
Authorized Signature	Moitrayee Majumdar	**Title**	Senior Proposal Specialist
Email	Moitrayee_Majumdar@SHI.com	**Phone**	858-232-2931

Please review SHI Exception Document uploaded as a separate file attached under the supporting information section of the portal.

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Solicitation Checklist

Instructions: Utilize the checklist below, reviewing to confirm that all the required documents have been uploaded to Public Purchase, in their ***specified/required format***, by the due date and time listed for this solicitation. ***Submissions not following the specified/required format may result in being marked non-responsive and may not be considered for evaluation.*** Respondents are reminded that failure to follow, comply with, and adhere to the enclosed instructions of this solicitation may result in their response being deemed non-responsive. AEPA, its Member Agencies, affiliate agencies, and authorized representatives are not responsible for bid proposals that are incomplete, unreadable, or received after the solicitation deadline submission date.

"x"	**Document Title, Uploaded to Bonfire** *(Respondent must submit documents in the required title/format)*	**Format of Uploaded Document**	**Notes**
	Bid Bond – if Required, see Part A if applicable.	Upload PDF copy of the bid security.	The original bid security must be received by Lakes Country Service Cooperative by due date and time.
	Part C – State-Specific Forms – ***Name of Responding Company***	Single, Scanned PDF	**New Jersey Only Requirement.** Signatures Required.
	Part D - Questionnaire – ***Name of Responding Company*** Includes: ● Company Information ● Service Questionnaire ● Exceptions ● Deviations	Single, Scanned PDF	**Required.**
	Part E – Signature Forms – ***Name of Responding Company*** Includes: ● Uniform Guidance "EDGAR" Certification ● Solicitation Affidavit ● Acceptance of Solicitation & Contract	Single, Scanned PDF	**Required.** Signatures required.
	Part F – Pricing Schedule – ***Name of Responding Company***	Excel Workbook	**Required.**
	Price List and/or Catalog – ***Name of Responding Company***	Upload PDF	**Required.**
	Exhibit A – Marketing Plan – ***Name of Responding Company***	Scanned PDF	**Optional.** Form not provided by AEPA, Respondent Created

Contents

1-Exhibit A - Marketing Plan-Twotrees Technologies 1
Introduction 1
1. Customized Contact Lists Development 1
Strategy 1
Action Plan 1
2. Onsite Generalist Cybersecurity Seminars 1
Strategy 1
Action Plan 1
3. Participation in Local and Regional Conferences 2
Strategy 2
Action Plan 2
4. Multi-Channel Marketing Promotion 2
Strategy 2
Action Plan 2
Examples of Past Marketing Efforts 2
Conclusion 5
1-(Amd) Twotrees Amended Part E Signature Forms 6
2-F - Cyber Security Training Part E Signature Forms Twotrees 14

Marketing Plan for Purchasing Agency Engagement

Introduction

The objective of this marketing plan is to outline strategies for promoting purchasing agencies and engaging with local agencies through various marketing mediums. The plan focuses on leveraging local account executives, organizing onsite seminars, participating in regional events, and utilizing a multi-channel marketing approach to maximize reach and impact.

1. Customized Contact Lists Development

Strategy

Utilize local account executives to develop customized contact lists tailored to each agency. This approach ensures that our outreach is personalized and relevant, fostering stronger relationships and higher engagement rates.

Action Plan

- Assign account executives to specific regions and agencies.
- Gather agency-specific information, including key decision-makers and points of contact.
- Update and maintain contact lists regularly to ensure accuracy and relevance.
- Use tailored communication strategies to address the unique needs and concerns of each agency.

2. Onsite Generalist Cybersecurity Seminars

Strategy

Organize and conduct onsite, in-person cybersecurity seminars focusing on best practices and enhancing cybersecurity stances. The seminars will be educational and free from product placement, emphasizing practical knowledge and skills.

Action Plan

- Identify suitable locations for hosting seminars at agency premises or nearby venues.
- Develop a seminar curriculum that covers general cybersecurity best practices and strategies.
- Recruit experienced cybersecurity professionals to lead the seminars.
- Promote the seminars through direct invitations, newsletters, and agency communication channels.

- Collect feedback from participants to improve future seminars and address specific concerns.

3. Participation in Local and Regional Conferences

Strategy

Engage with local and regional conferences and seminars to expand purchasing agency reach, share expertise, and promote our cybersecurity initiatives.

Action Plan

- Identify key local and regional conferences and seminars.
- Register as speakers or exhibitors at selected events.
- Develop presentation materials and exhibits that highlight our expertise and seminar offerings.
- Network with attendees and organizers to build relationships and explore collaboration opportunities.
- Follow up with contacts made during events to foster ongoing engagement.

4. Multi-Channel Marketing Promotion

Strategy

Promote our purchasing agencies through various marketing mediums, including social media, websites, flyers, and radio advertisements. This multi-channel approach ensures broad visibility and engagement across different audience segments.

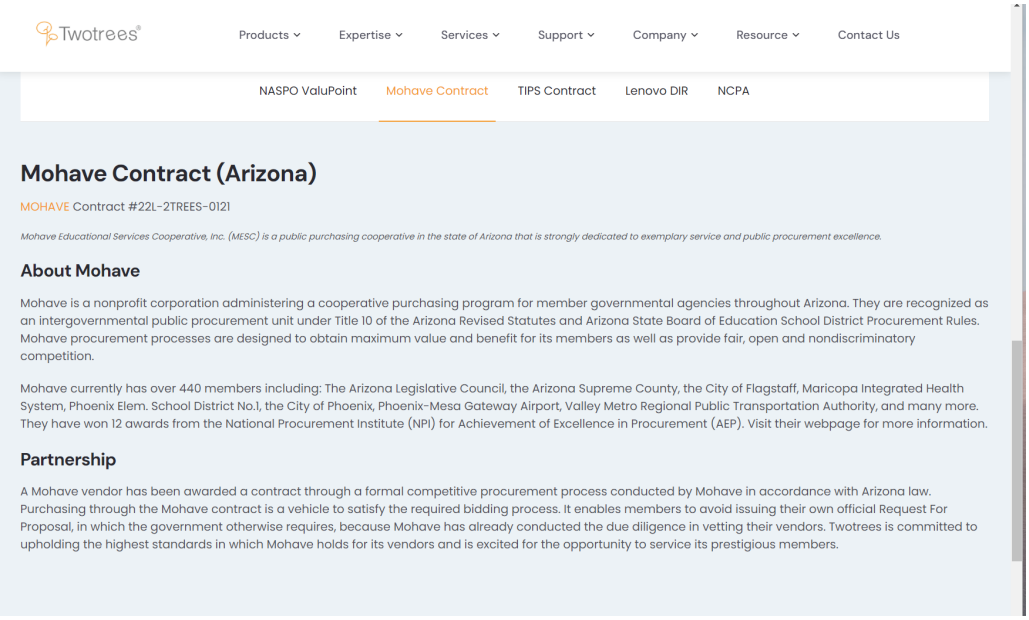
Action Plan

- Develop a comprehensive social media strategy to share updates, success stories, and upcoming events.
- Create engaging content for our website, including blog posts, case studies, and event announcements.
- Design eye-catching flyers and distribute them at relevant locations, including agency offices and community centers.
- Produce radio advertisements to reach a wider audience and promote our initiatives.
- Measure the effectiveness of each marketing channel and adjust strategies based on performance data.

Examples of Past Marketing Efforts

To provide context and inspiration, here are some examples of successful marketing efforts we have executed in the past:

Twotrees Website Contracts Page:



Midwest Tech Talk Booth-TIPS Contract Placement



Radio Script:

From: Keppy, Eleaner <keppy@kmuw.org>

Sent: Friday, August 2, 2019 2:31:39 PM

To: Susie Smith <ssmith@twotrees.com>

Subject: RE: Script Revision I

Two Trees Technologies, serving school systems and public entities for over 30 years through internet security, technology innovations, and public contract access. "A different kind of technology company." Two...trees...dot – com.

Flyer Sample



Please join Twotrees and our partners for an exciting Lunch-and-Learn to hear about some of our exciting new hardware and software that's being introduced into classrooms!

-Lenovo & Lenovo VR

Hear from Lenovo about the latest Lenovo products entering the education market, as well as their new VR headset designed for EDU!

-BenQ

BenQ will be here to discuss the latest touch panel technology that makes teaching more interactive!

-STEM Products

Checkout the latest STEM & Steam products!

-Anywhere Carts

Anywhere will have their laptop/tablet carts on display and talking about easy ways to charge your student devices to get them back in action ASAP

-Microsoft

Join Microsoft in an fun discussion about products such as Minecraft that bring gaming and learning together!

-Google Creative Apps

We'll be talking about incredible apps that can revolutionize your classroom and get even MORE out of your Chromebooks!

-eSports in EDU Integration

eSports in Education is exploding and we want to get you in on the ground floor on how your students can become eSports Champions!

Conclusion

This marketing plan outlines a strategic approach to promoting AEPA purchasing agencies. By leveraging local expertise, organizing educational seminars, participating in regional events, and utilizing a multi-channel marketing approach, we aim to enhance our visibility, build strong relationships, and drive meaningful impact utilizing AEPA members.

Part E – Signature Forms

AEPA 025-F

Cyber Security and Training

Association of Educational Purchasing Agencies

Instructions

Contained herein are forms that **require a signature** from an authorized person at your company. All items found within this document are **mandatory**. Failure to sign the required areas, sections, or signature lines may lead AEPA to consider your company's proposal as **non-responsive**.

To submit the required signed forms, follow these steps:

1. Read the documents in their entirety.
2. Complete all forms and sign when required.
3. Return the forms and pages in their correct order and scan one (1) single PDF format titled ***"Part E – Signature Forms – Name of Responding Company"*** (i.e. one PDF document for all signature forms).
4. Submit Part E, along with other required documents in Bonfire.

*Note, a solicitation checklist has been provided to review with your submission.

The following sections will need to be completed prior to submission as one (1), single PDF titled "Part E – Signature Forms – Name of Responding Company".

Uniform Guidance "EDGAR" Certification Form – ***signature required***
Solicitation Affidavit – ***signature required***
Acceptance of Solicitation & Contract – ***signature required***

Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7. Clean Air Act and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended, contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein.		
Respondent Certification (By Item)	**Respondent Certification: YES, I agree**	**Initial**
1. Violation of Contract Terms and Conditions	✓	SDS
2. Termination for Cause of Convenience	✓	SDS
3. Equal Employment Opportunity	✓	SDS
4. Davis-Bacon Act	✓	SDS
5. Contract Work Hours and Safety Standards Act	✓	SDS
6. Right to Inventions Made Under a Contract or Agreement	✓	SDS
7. Clean Air Act and Federal Water Pollution Control Act	✓	SDS
8. Debarment and Suspension	✓	SDS
9. Byrd Anti-Lobbying Amendment	✓	SDS
10. Procurement of Recovered Materials	✓	SDS
11. Profit as a Separate Element of Price	✓	SDS
12. General Compliance with Participating Agencies	✓	SDS
13. Governing Law; Forum Selection.	✓	SDS

Twotrees Technologies, L.L.C
Name of Business

Susie D. Smith
Signature of Authorized Representative

Susie D. Smith
Printed Name

9-17-24
Date

Solicitation Affidavit

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

Susie D Smith	200 N. Emporia, Suite 300
Authorized Representative (Please print or type)	Mailing Address
CEO	Wichita KS 67202
Title (Please print or type)	City, State, Zip
Susie D Smith	9-17-24
Signature of Authorized Representative	Date

SANDRA K. STEELE
Notary Public, State of Kansas
My Appointment Expires
8-20-2027

Sandra K. Steele

Acceptance of Solicitation & Contract

Association of Educational PURCHASING AGENCIES

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	Twotrees Technologies, LLC	**Date**	9-14-24
Address	200 North Emporia	**City, State Zip**	Wichita KS 67202
Contact Person	Susie D Smith	**Title**	CEO
Authorized Signature	Susie D Smith	**Title**	CEO
Email	ssmith@twotrees.com	**Phone**	316-634-9302

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Solicitation Checklist

Instructions: Utilize the checklist below, reviewing to confirm that all the required documents have been uploaded to Public Purchase, in their ***specified/required format***, by the due date and time listed for this solicitation. ***Submissions not following the specified/required format may result in being marked non-responsive and may not be considered for evaluation.*** Respondents are reminded that failure to follow, comply with, and adhere to the enclosed instructions of this solicitation may result in their response being deemed non-responsive. AEPA, its Member Agencies, affiliate agencies, and authorized representatives are not responsible for bid proposals that are incomplete, unreadable, or received after the solicitation deadline submission date.

"x"	**Document Title, Uploaded to Bonfire** *(Respondent must submit documents in the required title/format)*	**Format of Uploaded Document**	**Notes**
	Bid Bond – if Required, see Part A if applicable.	Upload PDF copy of the bid security.	The original bid security must be received by Lakes Country Service Cooperative by due date and time.
	Part C – State-Specific Forms – *Name of Responding Company*	Single, Scanned PDF	**New Jersey Only Requirement.** Signatures Required.
	Part D - Questionnaire – *Name of Responding Company* Includes: • Company Information • Service Questionnaire • Exceptions • Deviations	Single, Scanned PDF	**Required.**
	Part E – Signature Forms – *Name of Responding Company* Includes: • Uniform Guidance "EDGAR" Certification • Solicitation Affidavit • Acceptance of Solicitation & Contract	Single, Scanned PDF	**Required.** Signatures required.
	Part F – Pricing Schedule – *Name of Responding Company*	Excel Workbook	**Required.**
	Price List and/or Catalog – *Name of Responding Company*	Upload PDF	**Required.**
	Exhibit A – Marketing Plan – *Name of Responding Company*	Scanned PDF	**Optional.** Form not provided by AEPA, Respondent Created

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein.		
Respondent Certification (By Item)	**Respondent Certification:** YES, I agree	**Initial**
1. Violation of Contract Terms and Conditions	✓	SDS
2. Termination for Cause of Convenience	✓	SDS
3. Equal Employment Opportunity	✓	SDS
4. Davis-Bacon Act	✓	SDS
5. Contract Work Hours and Safety Standards Act	✓	SDS
6. Right to Inventions Made Under a Contract or Agreement	✓	SDS
7. Clean Air Act and Federal Water Pollution Control Act	✓	SDS
8. Debarment and Suspension	✓	SDS
9. Byrd Anti-Lobbying Amendment	✓	SDS
10. Procurement of Recovered Materials	✓	SDS
11. Profit as a Separate Element of Price	✓	SDS
12. General Compliance with Participating Agencies	✓	SDS
13. Governing Law; Forum Selection.	✓	SDS

Twotrees Technologies, LLC
Name of Business

Susie D. Smith
Signature of Authorized Representative

Susie D. Smith
Printed Name

9-17-24
Date

Solicitation Affidavit

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the ***Member Agency***, or any employee thereof, or any person, business or corporation under contract with the ***Member Agency*** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the ***Member Agency***, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.
2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.
3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the ***Member Agency***, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.
4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.
5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.
6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.
7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

Susie D Smith	200 N. Emporia, Suite 300
Authorized Representative (Please print or type)	Mailing Address
CEO	Wichita KS 67202
Title (Please print or type)	City, State, Zip
Susie D Smith	9-17-24
Signature of Authorized Representative	Date

SANDRA K. STEELE
Notary Public, State of Kansas
My Appointment Expires
8-20-2027

Sandra K. Steele

Acceptance of Solicitation & Contract

Association of Educational Purchasing Agencies

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	Twotrees Technologies LLC	**Date**	9-14-24
Address	200 North Emporia	**City, State Zip**	Wichita KS 67202
Contact Person	Susie D Smith	**Title**	CEO
Authorized Signature	Susie D Smith	**Title**	CEO
Email	ssmith@twotrees.com	**Phone**	316-634-4302

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**	**Contract Number**
Contract to commence (Member Agency to select)	3/1/2025	**Or**

Recommendation for New Contracts

AEPA 025-F Cybersecurity & Training

RFPs received that were rejected PRIOR to Category Committee evaluation with cause for rejection:

- **vTech Solution Inc. -** Missing signature forms or pricing documentation.

RFPs received that were rejected DURING Category Committee evaluation with cause for rejection:

- **Beta Systems International**- Scored below 70 points on RFP criteria**.**
- **CCS Global Tech -** No F.1 or F.2 that were required. Limited offering for technical training courses. Pricing was uploaded separately and incorrect format.
- **Clutch Solutions, LLC** – Scored below 70 points on RFP criteria
- **Enterprise Risk Management, Inc. dba ERMProtect** - Scored below 70 points on RFP criteria
- **Executive Option, LLC -** No F.1 or F.2 that were required. Total project amount for AEPA members was estimated. Project total in summary didn't add up to $1,450,960 in project summary. No individual school pricing model provided for school members**.**
- **Fortalice Solutions, LLC** – Scored below 70 points on RFP criteria
- **Hamilton Telecommunications** - Scored below 70 points on RFP criteria
- **Infosec Institute** - Scored below 70 points on RFP criteria
- **Network Technology Partners -** Did not submit pricing file, submitted the Questionnaire Excel file instead.
- **Tyler Technologies** – An extensive list of exceptions added to Part E - Signature Forms and upon further review with the committee and legal-council it was noted that Tyler is unwilling to adhere to AEPAs contract

Methodology Used by the Committee for Determination:

X Responsive and responsible Respondents(s) based on the attached RFP criteria.

X Baseline score of 70 points or higher

Vendor(s) recommended with reason for recommendation:

- **ActZero** – Offers Managed Detection and Response (MDR) services and reporting.
- **Caetra.io** – Provided a clear marketing plan and documentation with tiered pricing discounts with a specific focus on the CyMetric Risk Management Platform.
- **CDW Government, LLC** – Offered full catalog pricing with an expert driven comprehensive suite of cybersecurity tools and training solutions.
- **Forward-Edge** – Managed Cybersecurity Services, using best practices in NIST Cybersecurity Framework (CSF). Knowledgeable team in the areas of cyber liability insurance requirements, data privacy compliance including professional learning services.
- **ResoluteGuard** – A proactive approach through assessment, monitoring, reporting, and training. Offering real-time executive summaries and templated policies to streamline documentation.
- **SHI** – With a vendor-neutral approach, SHI offers solutions in data center security, application security, and identity management while proactively identifying vulnerabilities including a full catalog of products and services for a holistic approach to your network security.
- **TwoTrees Technologies, LLC** – Offering a unique suite of Endpoint Protection, customizable phishing simulations, mobile device management and training programs.

The below responses listed deviations and/or exceptions :

- **CDW Government, LLC** See attached document; 1-CDW Government AEPA RFP 025 Cybersecurity Exceptions.pdf
- **SHI** – See attached documents; 3-Part C- AEPA Terms and Condition Exception-SHI.pdf, 4-Part B - AEPA Terms and Conditions Exceptions - SHI.pdf

Proposed Motion:

The Category Committee recommends AEPA reject the RFPs from:

- Beta Systems International
- CCS Global Tech
- Clutch Solutions, LLC
- Enterprise Risk Management, Inc. dba ERMProtect
- Executive Option, LLC
- Fortalice Solutions, LLC
- Hamilton Telecommunications
- Infosec Institute
- Network Technology Partners
- Tyler Technologies

Proposed Motion:

The Category Committee recommends the following responses for approval by AEPA:

- ActZero
- Caetra.io
- CDW Government, LLC
- Forward-Edge
- ResoluteGuard
- SHI
- TwoTrees Technologies, LLC

Committee Members

Committee Chair – Name & Signature: Hope Hardin-Borbely, IL Hope Hardin-Borbely (Nov 19, 2024 14:04 PST)

Committee Member: Anna Marie Hollander, MI

Committee Member: Craig Peterson, NE

Committee Member: Click or tap here to enter text.

A	RFP Category Committee Evaluation	100 pts
A-1	Complete Response to Bid	5
A-2	Cost Evaluation	55
A-3	Conformance to Bid Terms and Conditions	5
A-4	Pricing Equal to or Better Than That Offered to Individual Entities or Cooperatives with Equal or Lesser Volume	5
A-5	Quality and Suitability of Products Offered	5
A-6	Marketing Plan	5
A-7	Financial Viability	5
A-8	Demonstrated Track Record of Performance in the Public Marketplace	5
A-9	Value Added attributes	5

Docusign Envelope ID: 201C6519-3E11-4284-8D29-0AD32039D90E

Exceptions and Deviations Agreement

Vendor Company Name: SHI

Solicitation Category: Cybersecurity & Training

Solicitation Number: 025-F

This document verifies the original Exceptions and Deviations submitted by Vendor as a part of their Response to the Solicitation referenced above, and the final agreed upon Exceptions and Deviations approved by AEPA and Vendor.

Exceptions

Reference	SHI Changes Submitted with Response to Solicitation	As Agreed
AEPA Terms and Conditions **Delivery Terms, Conditions, and Requirements Section 9. Liquidated Damages**	The Buyer may suffer financial loss if the project is not substantially complete, or products or services are not delivered on the established date. The Vendor Partner (if applicable surety) must be liable for and must pay to the Buyer, not as a penalty, the sums that may be hereinafter agreed upon as liquidated damages per calendar day of delay until the work and/or delivery is reasonably determined by Buyer to be complete and/or delivered that is within Vendor Partner's reasonable control. Liquidated damages will be determined on a project-by-project basis.	SHI is willing to remove the proposed "reasonable control" exception language in the Liquidated Damages section. The agreed-upon language remains as published in the original solicitation document.

AEPA Terms and Conditions **Termination for Convenience**	AEPA Member Agency reserves the right to immediately terminate this contract with thirty (30) days written notice, without penalty or recourse, in whole or in part, if the AEPA Member Agency determines that termination is in the best interest of Participating Entities.	SHI agrees to a 10-day notice period for a member agency to terminate the contract Agreed upon language is as follows: AEPA Member Agency reserves the right to immediately terminate this contract with ten (10) days written notice, without penalty or recourse, in whole or in part, if the AEPA Member Agency determines that termination is in the best interest of Participating Entities.

Docusign Envelope ID: 201C6519-3E11-4284-8D29-0AD32039D90E

Terms and Conditions **Indemnification**	Vendor Partner will indemnify, defend and save harmless AEPA, its Members, Participating Entities, its employees from any and all third party claims, demands, suits, proceedings, loss, cost and damages of every kind and description, including any reasonable attorney's fees and/or litigation expenses, which might be brought or made against or incurred by AEPA, its Members, Participating Entities, its employees on account of loss or damage to any property or for injuries to or death of any person, caused by, arising out of, or contributed to, in whole or in part, by reasons of any negligent act, omission, ~~professional error, fault, mistake,~~ or negligence of Vendor Partner, its employees, agents, representatives, or Subcontractors, their employees, agents, or representatives in connection with or incident to the performance of this agreement, or arising out of worker's compensation claims, unemployment compensation claims, or unemployment disability compensation claims of employees of Vendor Partner, and/or its Subcontractors or claims under similar such laws or obligations. Vendor Partner's obligation under this section will not extend to any liability caused by the ~~sole~~ proportional negligence of AEPA, its Members, participating Entities, its employees. The liability of AEPA, its Members, Participating Entities, or its employees will be subject in all cases to the immunities and limitations of Nevada or the AEPA Member Agency's state laws. Installation: Equipment and items of construction must be installed in accordance with the manufacturer's instructions, specifications, in accordance with any federal, state, local rules, regulations, codes, and the schedule determined by the AEPA Member Agency and/or Participating Entity.	SHI agrees to remove "third party" from SHI proposed exceptions regarding the Indemnification section. The agreed-upon language remains as published in the original solicitation document.

ADD **Limitation of Liability**	NEITHER PARTY WILL BE LIABLE FOR ANY SPECIAL, PUNITIVE, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF OR DAMAGE TO DATA, LOSS OF ANTICIPATED REVENUE OR PROFITS, WORK STOPPAGE OR IMPAIRMENT OF OTHER ASSETS, WHETHER OR NOT FORESEEABLE AND WHETHER OR NOT A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT IN THE CASE OF A PARTY'S OBLIGATION TO INDEMNIFY FOR THIRD PARTY CLAIMS, OR BREACH OF CONFIDENTIALITY, EITHER PARTY'S TOTAL CUMULATIVE LIABILITY TO THE OTHER IN CONNECTION WITH THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR OTHER THEORY, WILL NOT EXCEED THE TOTAL AMOUNT OF FEES ACTUALLY PAID OR PAYABLE BY THE STATE TO CONTRACTOR UNDER THIS AGREEMENT FOR THE YEAR PREVIOUS TO THE INCIDENT WHICH GAVE CAUSE FOR SUCH LIABILITY. THE STATE ACKNOWLEDGES THAT SUCH AMOUNT REFLECTS THE ALLOCATION OF RISK SET FORTH IN THIS AGREEMENT AND THAT CONTRACTOR WOULD NOT ENTER INTO THIS AGREEMENT WITHOUT THESE LIMITATIONS ON ITS LIABILITY.	Neither party will be liable for any special, punitive, indirect, incidental or consequential damages including, but not limited to, loss of or damage to data, loss of anticipated revenue or profits, work stoppage, or impairment of other assets, whether or not foreseeable and whether or not a party has been advised of the possibility of such damages.

AEPA Terms and Conditions **Audit Rights**	In accordance with applicable law of the State of the AEPA Member Agency, the Vendor Partner's books, and pertinent records related to this contract may be audited at a reasonable time and place. Such audits shall be with thirty (30) days written notice and not more than once annually for each AEPA Member Agency unless otherwise required by law.	AEPA agrees to accept these changes.

AEPA Terms and Conditions **Patent and Copyright Indemnification**	To the extent permitted by law, Vendor Partner must indemnify and hold harmless Member Agency and its Participating Entities against any liability, including costs and expenses, for infringement of any patent, trademark or copyright arising out of ~~contract~~ Vendor Partner's performance or use by Member Agency and its Participating Entities of ~~materials furnished or~~ work performed ~~under this contractby~~ Vendor Partner. Member Agency and its Participating Entities must reasonably notify Vendor Partner of any claim for which it may be liable under this paragraph.	AEPA agrees to accept these changes.

AEPA Terms and Conditions **Warranty**	Vendor Partner warrants that all commodities, supplies, materials, equipment, software, and service delivered under this contract must conform to the specifications of this contract. All ~~items should carry a warranty equal to the intended life cycle or a minimum~~Vendor Partner will pass through all manufacturer's ~~warranty that includes parts and labor unless otherwise specified in the category specificationswarranties~~. The manufacturer has the primary responsibility to honor a manufacturer's warranty; ~~a distributor or dealer~~Vendor Partner agrees to reasonably assist the purchaser to reach a solution in a dispute with the manufacturer over a warranty's terms. Any extended manufacturer's warranty will be passed on to the Buyer. For example, if a voice board has a three-year warranty, but the board is in a turnkey system that has a one-year warranty, the voice board's three-year warranty must be honored by the manufacturer and the Vendor Partner. All extended warranties must be passed on, without exception. If upon discovery, the Vendor Partner charges a Buyer for a replacement part that the Vendor Partner actually received at no cost under a warranty, the Vendor Partner will rebate the amount billed and the Buyer reserves the right to cancel the contract. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS AGREEMENT, VENDOR PARTNER HEREBY EXPRESSLY DISCLAIMS ALL WARRANTIES EITHER EXPRESS OR IMPLIED, RELATED TO PRODUCTS OR THIRD PARTY SERVICES PROVIDED BY VENDOR PARTNER HEREUNDER, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WARRANTY OF NONINFRINGEMENT, OR ANY WARRANTY RELATING TO THIRD PARTY PRODUCTS.	AEPA agrees to accept these changes.

ADD **Return Policy**	All returns of products, goods, equipment and/or software shall be subject to the terms of Contractor's Return Policy, which can be accessed at: **www.SHIDirect.com/ReturnPolicy**	AEPA agrees to accept these additions.

Docusign Envelope ID: 201C6519-3E11-4284-8D29-0AD32039D90E

Member Agency Terms and Conditions **Section 19 – New Mexico**	Liquidated Damages: The CES Member or Participating Entity has the right to assess liquidated damages to the Contractor (and its Surety); and the Contractor shall be liable for the amount of liquidated damages as determined in the mutually agreed upon contract documents. Such liquidated damages are intended to represent estimated actual damages and are not intended as a penalty, and Contractor shall pay them to Owner without limiting Owner's right to terminate this agreement for default as provided elsewhere herein. The liquidated damages are assessed per ~~calendar~~ business day of delay until the work is determined by CES and its Member or Participating Entity to be substantially complete. Liquidated damages will comply with the requirements of 55-2-718 NMSA 1978. Liquidated damages and early completion incentives will be between the CES Member or Participating Entity and the Contractor and must be agreed upon in writing. If the CES Member or Participating Entity declines a liquidated damages or early incentive agreement, the Contractor will ensure such agreement is reflected and included in the project's contract documents.	AEPA agrees to accept these changes.

Member Agency **Terms and Conditions** Section 25 - Virginia	**12. TERMINATION FOR CONVENIENCE-**A contract may be terminated in whole or in part by the County in accordance with this clause whenever the County Purchasing Agent shall determine that such a termination is in the best interest of the County. Any such termination shall be effected by delivery to the Contractor at least ~~five~~ thirty (~~5~~30) ~~working~~ days prior to the termination date of a Notice of Termination specifying the extent to which performance shall be terminated and the date upon which termination becomes effective. An equitable adjustment in the contract price shall be made for completed service, but no amount shall be allowed for anticipated profit on unperformed services.	AEPA agrees to accept this change.

Deviations

N/A

Docusign Envelope ID: 201C6519-3E11-4284-8D29-0AD32039D90E

The Vendor and AEPA hereby agree and confirm that the *Final Agreed Upon Exceptions to Terms and Conditions* and the *Final Agreed Upon Deviations from Specifications*, listed above, represent the final agreement between Vendor and AEPA relating to the Solicitation Category and Solicitation Number listed above.

AEPA:

Authorized Signature: Steve Griggs Title: Director of Solicitations

Typed Name: Steve Griggs Date: February 3, 2025

Vendor:

Authorized Signature: DocuSigned by: Kristina Mann EA418E789F09404... Title: Director - Contracts

Typed Name: Kristina Mann Date: 2/4/2025

Exceptions and Deviations Agreement

Vendor Company Name: CDWG

Solicitation Category: Cybersecurity & Training

Solicitation Number: 025-F

This document verifies the original Exceptions and Deviations submitted by Vendor as a part of their Response to the Solicitation referenced above, and the final agreed upon Exceptions and Deviations approved by AEPA and Vendor.

Exceptions

Reference	CDWG Changes Submitted with Response to Solicitation	As Agreed
Limitations of Liability	CDWG is not proposing a specific language exception at this time. Rather, CDWG would request, upon award, the opportunity to discuss the incorporation of a mutually agreeable limitation of liability clause - commiserate (sic) with the clause currently contained in our current 022 contract. CDWG appreciates the opportunity to discuss implementing such a clause and is eager to work with AEPA and its members to build a competitive and mutually beneficial contract.	Neither party will be liable for any special, punitive, indirect, incidental or consequential damages including, but not limited to, loss of or damage to data, loss of anticipated revenue or profits, work stoppage, or impairment of other assets, whether or not foreseeable and whether or not a party has been advised of the possibility of such damages.
Administrative Fees	CDWG is unable to track & report sales falling under the "Value Added Services" component of its proposal response. Accordingly, CDWG will not be able to remit Administrative Fees to AEPA or its Member Agencies for such purchases.	CDWG agrees to the original language in the solicitation documents with regard to Administrative Fee(s).

Deviations

N/A

The Vendor and AEPA hereby agree and confirm that the *Final Agreed Upon Exceptions to Terms and Conditions* and the *Final Agreed Upon Deviations from Specifications*, listed above, represent the final agreement between Vendor and AEPA relating to the Solicitation Category and Solicitation Number listed above.

AEPA:

Authorized Signature: _____ Title: Director of Solicitations

Typed Name: Steve Griggs Date: January 15, 2025

Vendor: JH

Authorized Signature: Brian Fisher (Jan 29, 2025 07:31 CST) Title: Director, Program Management

Typed Name: Brian Fisher Date: Jan 29, 2025

Docusign Envelope ID: 685517F7-5185-47FA-879D-C4CE04D5A5BD

Acceptance of Solicitation & Contract

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	CDW Government LLC	**Date**	9/16/24
Address	230 N. Milwaukee Avenue	**City, State Zip**	Vernon Hills, IL 60061
Contact Person	Stephanie Kessler	**Title**	Deputy Program Manager
Authorized Signature		**Title**	VP Contracting Operations
Email	dariber@cdw.com	**Phone**	203.851.7049

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency Cooperative Purchasing Connection (MN)

Authorized Representative DocuSigned by: Jane Eastes 6D9BB132BB3040A... Executive Deputy Director

Awarded this 18th **day of** February **Contract Number** 025-F

Contract to commence (Member Agency to select) 3/1/2025 **Or**

Docusign Envelope ID: 685517F7-5185-47FA-879D-C4CE04D5A5BD

Acceptance of Solicitation & Contract

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	CDW Government LLC	**Date**	9/16/24
Address	230 N. Milwaukee Avenue	**City, State Zip**	Vernon Hills, IL 60061
Contact Person	Stephanie Kessler	**Title**	Deputy Program Manager
Authorized Signature		**Title**	VP Contracting Operations
Email	dariber@cdw.com	**Phone**	203.851.7049

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency North Dakota Educators Service Cooperative

Authorized Representative DocuSigned by: Jane Eastes 6D9BB132BB3040A... Executive Deputy Director

Awarded this 18th **day of** February **Contract Number** 025-F

Contract to commence (Member Agency to select) 3/1/2025 **Or**