Contents

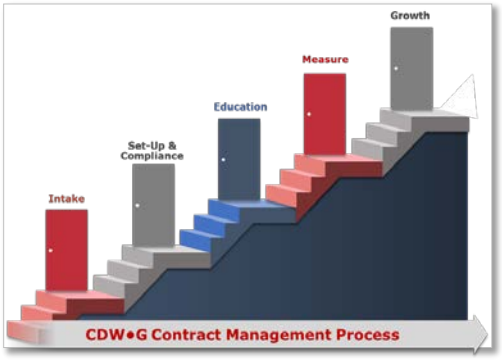
AEPA Marketing Plan Draft

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.

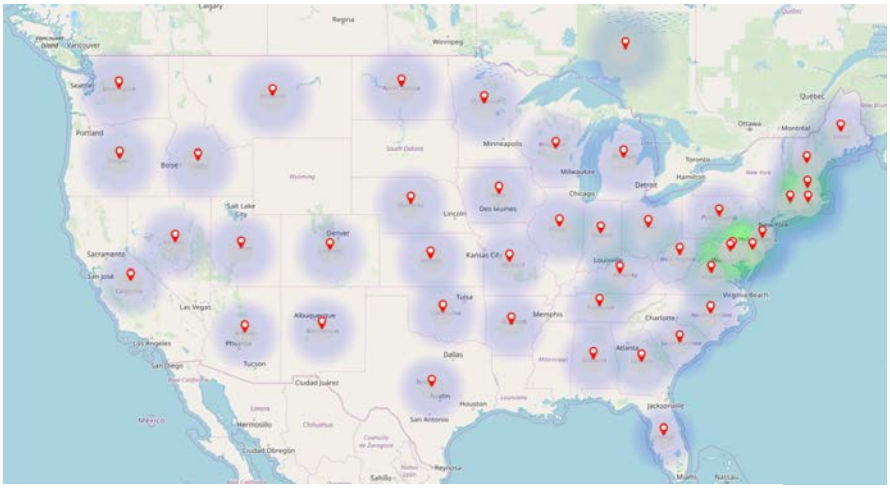
To support this process, we maintain an ecosystem of dedicated coworkers, CDW•G's program management department. This team is singularly devoted to managing contract, distinct from those responsibilities of our sales force. Members of the program management department work full-time to maintain contract 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.



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.

- **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?

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.

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.

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."

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

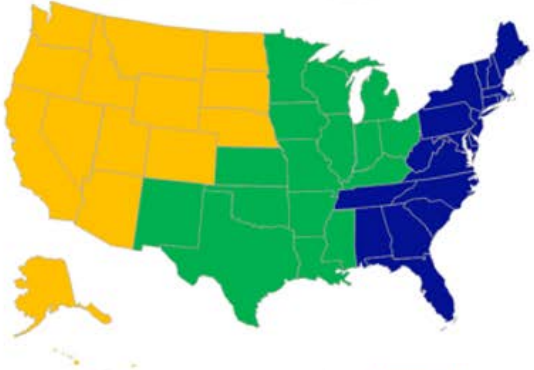
ASHLEY DiCIURCIO
K12 South

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

CDW Education

Higher Education Leadership & Inside Account Managers

Regional Leaders

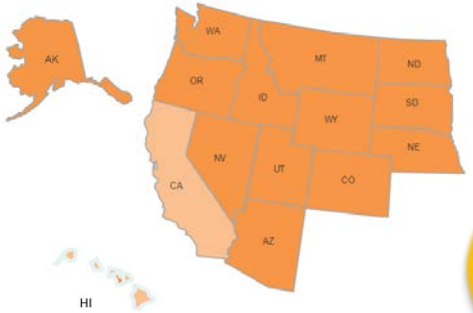
HiEd Regional Leaders West

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:

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

Account Managers

Brittany Atchison
Sales Manager – GS
HiEd West
Email: britatc@cdw.com
Phone: (312) 705-0147
Home Office: Chicago

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

Kyle Cavolo
ATAE – NW
kyle.cavolo@cdwg.com
(847) 465-6000

Dustin Harris
ATAE – OR & WA
dustin.harris@cdwg.com
(847) 465-6000

Larry Rascoe
ATAE – CA
Larry.Rascoe@cdw.com
(310)-968-1802

Erin Walther
ATAE - CA
erinwal@cdwg.com
(312) 705-3291

Trevor Heath
ATAE - CO
trevhea@cdw.com
(720)-626-6786

John Menning
ATAE – MT & NE
trevhea@cdw.com
(720)-626-6786

Tyler Quaranta
ATAE - CA
tylequa@cdw.com
(714)-325-5713

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

 |

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@cdwg.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

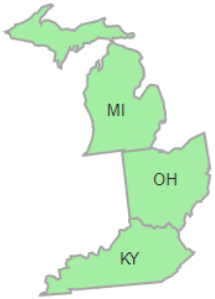
Josh McCray
Account Representative
josh.mccray@cdwg.com
(312) 705-4507

Virgil Cannon Jr
ATAE - IL
virgcan@cdwg.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

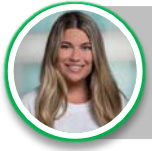
Kristen Peon
Sales Manager Assistant
krispeo@cdw.com
(312) 705-8722

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

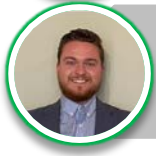
Samuel Humanchuk
Account Representative
sam.humanchuk@cdwg.com
(312) 547-2826

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

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

 |

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

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

Account Managers

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

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

CDW Education

K12 Leadership & Inside Account Managers

Regional Leaders

K12 Regional Leaders West

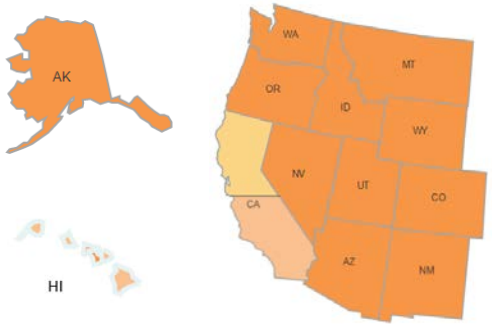
David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435

TBH
Sales Manager – CN
K12 California North
Email: Phone:
Home Office

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

Valerie Hanrahan
Sales Manager – CS
K12 California South
Email: valeban@cdw.com Phone: (312) 547-2711
Home Office: Chicago, IL



TBH
Field Sales Manager – California
Email: Phone:

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

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

Mary Boland
Sales Operations Supervisor
maritor@cdwg.com
(312) 705-0626

David Anderson
Sales Manager Assistant - K12
david.anderson@cdw.com
(617) 804-4435

Valerie Hanrahan

Sales Manager – CS
K12 West
Email: valeban@cdw.com
Phone: (312) 547-2711
Home Office: Chicago, IL

Account Managers

Adam Slater
Executive Account Manager
adamsla@cdw.com
(480) 270-7108

Anthony Dierickx
Account Manager
anthdie@cdwg.com
(312) 705-4061

Astrid Saed
Account Manager
astrsae@cdwg.com
(312)-547-4899

Charleen Chu
Executive Account Manager
charchu@cdwg.com
(312) 705-9033

Christopher Zingler
Executive Account Manager
chrizin@cdwg.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

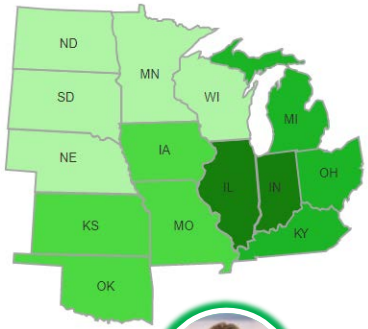
K12 Regional Leaders Central

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

 |

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

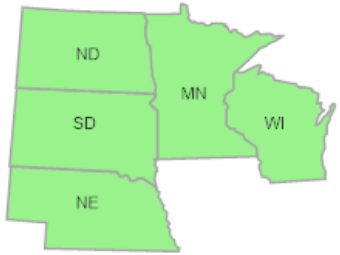
CDW Education

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

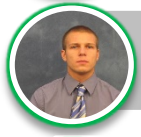
Mayank Srivastava
Executive Account Manager
joelhot@cdwg.com
(312) 547-2953

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@cdwg.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@cdwg.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

CDW 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

Megan Peterson
ATAE – KS/MO
chris.schwerin@cdwg.com
(312) 547-2817

Dave Donarski
ATAE - MN
davedon@cdwg.com
(612)-704-6000

Rafal Libelt
ATAE - IL
rafalib@cdwg.com
(312)-451 4108

Mark Silversten
ATAE– N & Central OH
marksil@cdwg.com
(440)-591-7718

Ryan Parvis
ATAE - IL
ryanpar@cdwg.com
(847)-371-5514

TBH
ATAE– WI

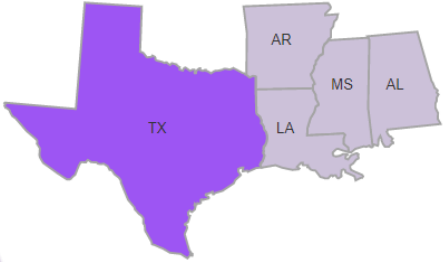
Steve Morrissey
ATAE - IN
steve.morrissey@cdwg.com
(847)-465-6000

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:

 |

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

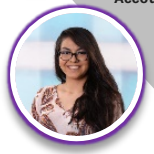
Gustavo Diaz
Account Representative
gustavo.diaz@cdwg.com
(312) 547-2611

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

Account Managers

Michael Swartz
Sales Manager – TE
K12 South
Email: michswa@cdwg.com
Phone: (312) 705-9596
Home Office: Chicago, IL

Jim Donato
Account Manager
jimmdon@cdwg.com
(312) 547-2798

Alec Campbell
Account Manager
aleccam@cdwg.com
(312) 705-6942

Corey Grempka
Executive Account Manager

Becky Bradley
Sr. Account Manager

CoreyandBecky@cdw.com
Corey: (312) 705-9518
Becky: (312) 705-9070

Kevin Tamras
Account Manager
kevitam@cdwg.com
(312) 705-0209

Alyssa Teague
Account Manager
alystea@cdw.com
(312)-705-9574

Melissa Zamin
Account Manager
melizam@cdw.com
(312) 705-8947

Ashley Zimdars
Account Manager
ashlzim@cdwg.com
(312) 705-0996

Jake Miles – TE
Account Representative
jake.miles@cdwg.com
(847) 968-0702

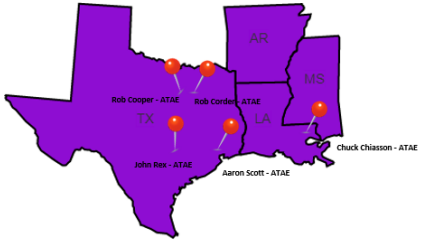
Swetal Thakkar
Account Representative
Swetal.Thakkar@cdwg.com
(312) 705-0193

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

 |

K12 Keystone Region

Danielle Lodovico
Sales Operations Supervisor
danilod@cdw.com
(203) 851-7196

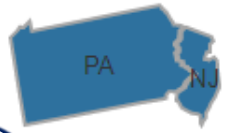
Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071

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

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

Mike Pinto
Sales Manager – AT
K12 Southeast Atlantic
Email: mikepin@cdw.com Phone: (203) 851-7150
Home Office: Shelton

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

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

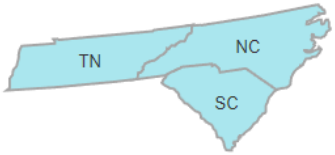
Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071

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

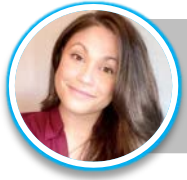
Todd Short
Executive Account Manager
toddsho@cdw.com
(312) 705-9047

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

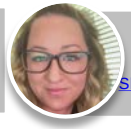
Adrienne Griffith
Sales Manager Assistant
adrgrif@cdw.com
(203) 851-7071

CDW Education

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

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

Robert DeBartolo
Sales Manager – Residency
K12 Chicago
Email: robedeb@cdw.com Phone: (847) 968-9388
Home Office: Chicago, IL

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

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

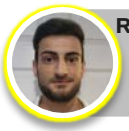
Anthony Brown - NE
Account Representative
tony.brown@cdwg.com
(203) 851-7032

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

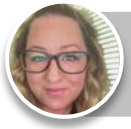
Giovanni Trocchia-KY
Account Representative
gio.trocchia@cdwg.com
(203) 851-7293

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

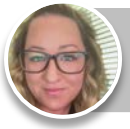
Richard Sakofsky - PAC
Account Representative
rich.sakofsky@cdwg.com
(480) 270-7006

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

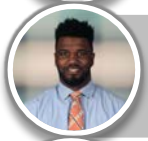
Jon Grey
Supervisor – Digital EdTech
Email: jongray@cdw.com
Phone: (203) 851-7133
Home Office: Shelton

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

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

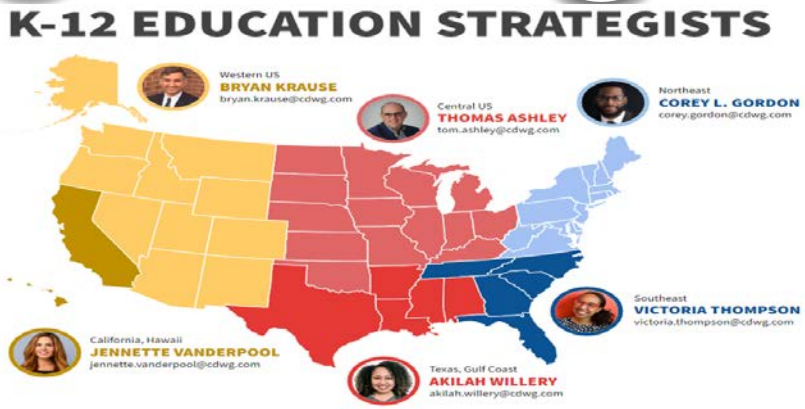
Jennette Vanderpool
K12 Education Strategist – West-Cal
j.diamond-vanderpool@cdwg.com
(847) 465-5600

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

Infrastructure Modernization Team

Keegan Morrison
Manager – Systems
Email: keegan.morrison@amplifiedit.cdw.com
Phone: (847) 465-6000

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

Mike Reorowicz
Sales Manager – West
Email: mikereo@cdwg.com
Phone: (312) 547-2196
Home Office: Chicago, IL

Jordan Harrison
Sr. Sales Operations Supervisor
jordhar@cdw.com
(847) 968-9937

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

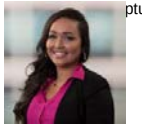
Lisa Missana
Assistant

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

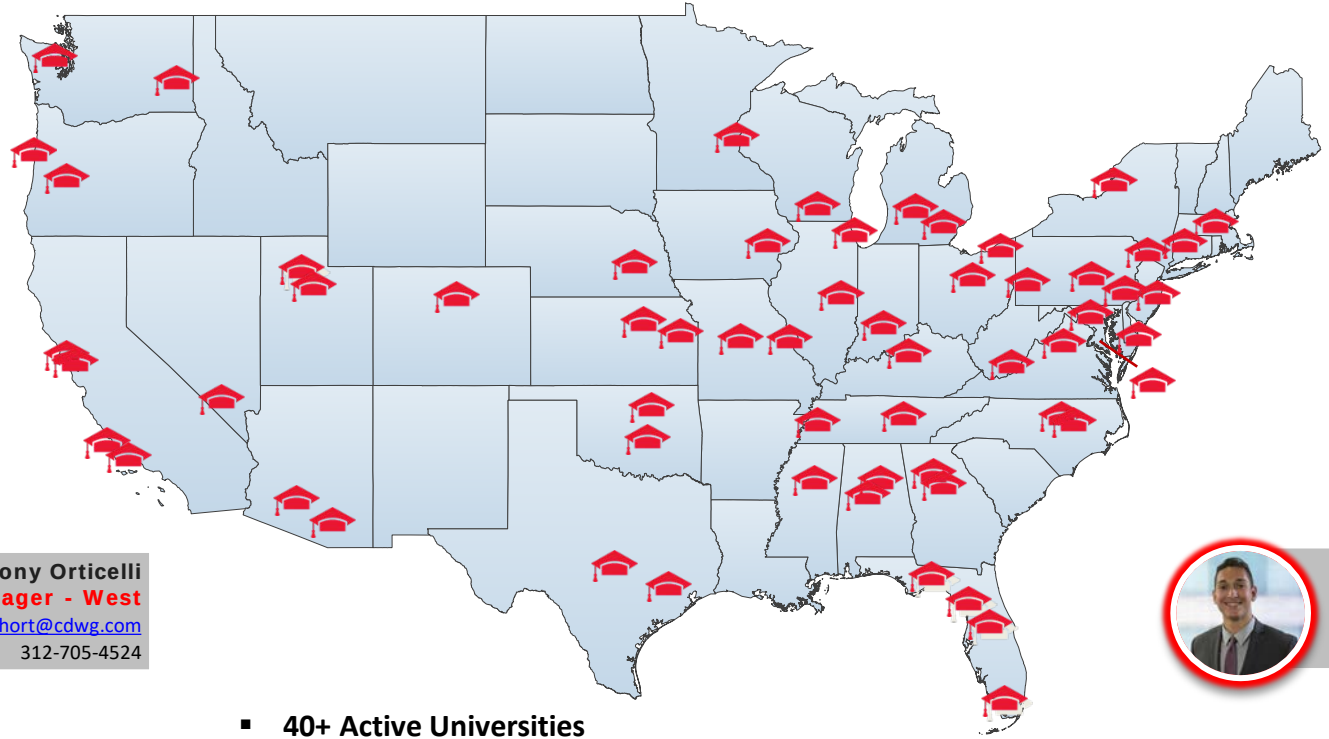
Cassie Floersch
Associate Manager – HiEd
Email: cassflo@cdw.com Phone: (312) 705-8836
Home Office: Chicago, IL

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

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

Table of Contents

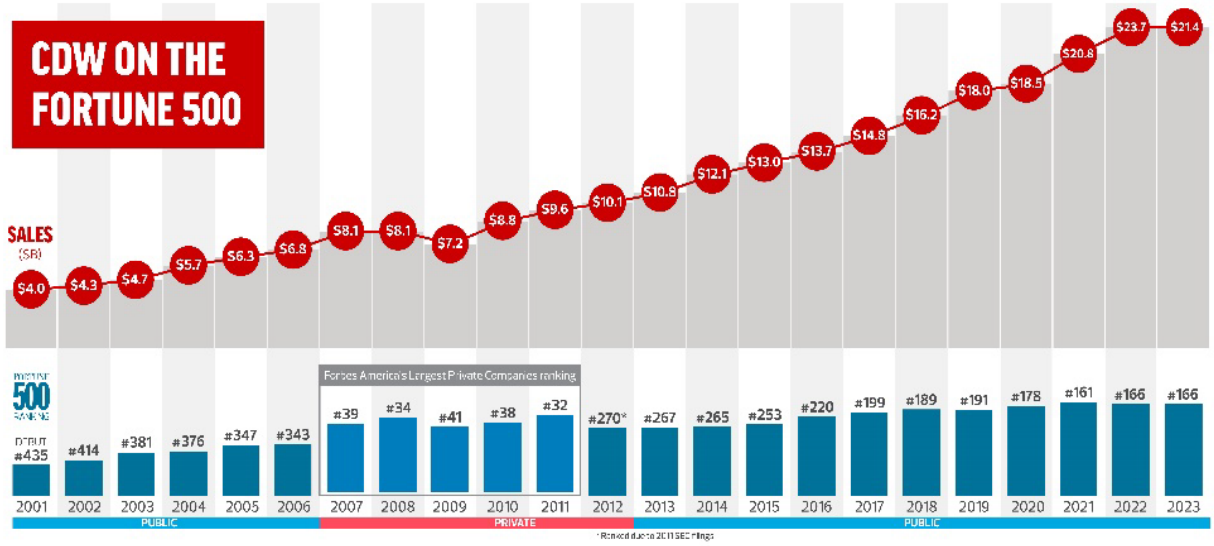
CDW Government Overview

- **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

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.

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.



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.

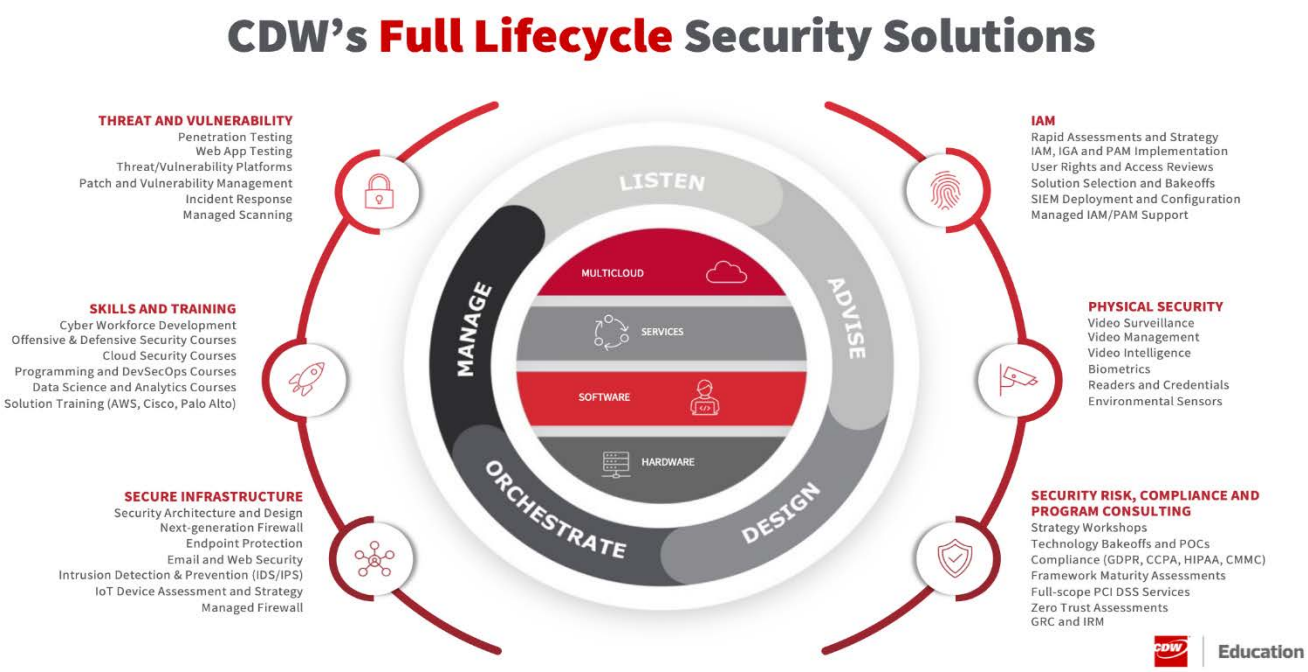
450,000-square-foot distribution center in IL

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 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.

- **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

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.

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**

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.

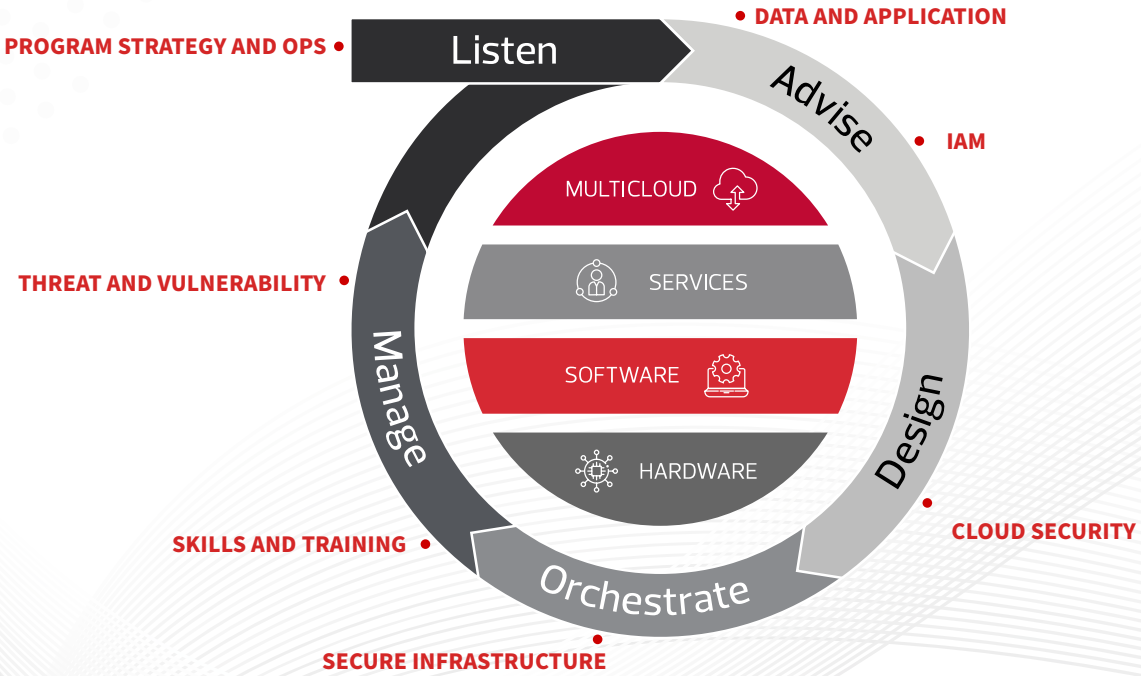
CDW.com/cybersecurity | CDW 800.808.4239

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

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