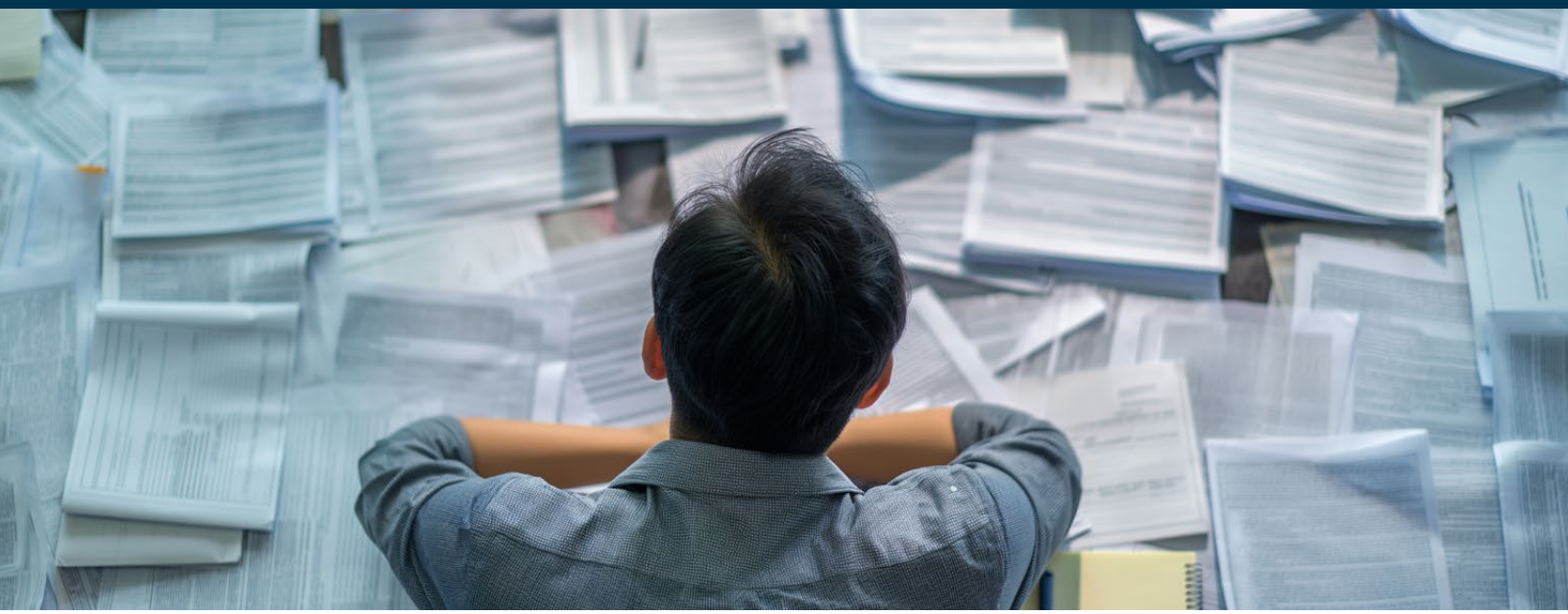
CDSE
LEARN. PERFORM. PROTECT.

PULSE

VOLUME 6 ISSUE 6 | JUNE 2025



CDSE Pulse
Published by the Security Training Directorate Outreach and Engagement Office for the Center for Development of Security Excellence (CDSE).

DCSA Leadership
David M. Cattler, *Director, DCSA*
Daniel J. Lecce, *Deputy Director, DCSA*
Kevin Jones, *Assistant Director, Security Training*
Erika Ragonese, *Deputy Assistant Director, Security Training*

CDSE Leadership
Audrey Gutierrez, *Director*
Glenn Stegall, *Deputy Director*

Pulse Staff
Cashmere He, *Chief Content Officer*
Isaiah Burwell, *Content Writer*
Jenise Kaliszewski, Tammi Bush, *Content Contributors*
Marc Pulliam, *Content Designer*

Center for Development of Security Excellence
CDSE – Center for Development of Security Excellence
@TheCDSE
Center for Development of Security Excellence

THIS MONTH'S FOCUS

CDSE has What you Need for CUI

By Isaiah Burwell

There are numerous threats to information the United States Government wants to protect. The safeguards used to protect this information and control who has access to it is what keeps the Nation safe. However, not all of this information is classified. CDSE offers various resources to educate security professionals about Controlled Unclassified Information (CUI), as well as Personnel Vetting (PV).

CUI, as defined in part 2002.14 of Title 32, CFR, is information the Government or an entity creates or possesses, for or on behalf of the Government that a law, regulation, or Government-wide policy requires an agency to handle using safeguarding or dissemination controls. The Office of the Secretary of Defense (OSD) and Department of Defense (DOD) Components' heads must ensure personnel receive initial and annual refresher CUI education and training, maintain documentation of this training for audit purposes, and report Component training completion data to the Under Secretary of Defense for Intelligence and Security (USD(I&S)) annually or as directed.

CDSE's **CUI toolkit** is an all-encompassing recourse for CUI training and resources. The eLearning "**DOD Mandatory Controlled Unclassified Information (CUI) Training**," which is accessible through the toolkit, is the mandatory training course for all DOD personnel with access to CUI. The course provides information on the 11 training requirements for accessing, marking, safeguarding, decontrolling,

and destroying CUI, along with the procedures for identifying and reporting security incidents. This course also fulfills CUI training requirements for industry personnel. There are two platforms that house this training, the Security Awareness Hub and STEPP. In addition to the mandatory course, the CUI toolkit also includes Life Cycle of CUI shorts that explain how CUI is created, marked, shared, and destroyed. Other resources include a CUI Marking Job Aid, a Procurement Toolbox, and an FAQ video. These resources explain CUI, but how can the Government ensure only reputable people have access to CUI?

CDSE's **PV toolkit** is a virtual warehouse for materials such as courses, job aids, posters, and shorts. The eLearning courses alone include Introduction to CAC credentialing, Introduction to National Security Adjudication, and Introduction to Personnel Security. The job aids in the toolkit provide guidance for topics such as continuous vetting, re-establishment of trust, and reporting requirements. There are also over 20 security shorts, including one for each of the 13 adjudicative guidelines.

CUI and PV are interconnected programs that keep the Nation safe. CUI offers guidance to protect important information, and PV ensures that those following CUI's guidance are trustworthy. Both programs work in harmony to keep valuable information away from the Nation's adversaries.

DCSA NEWS

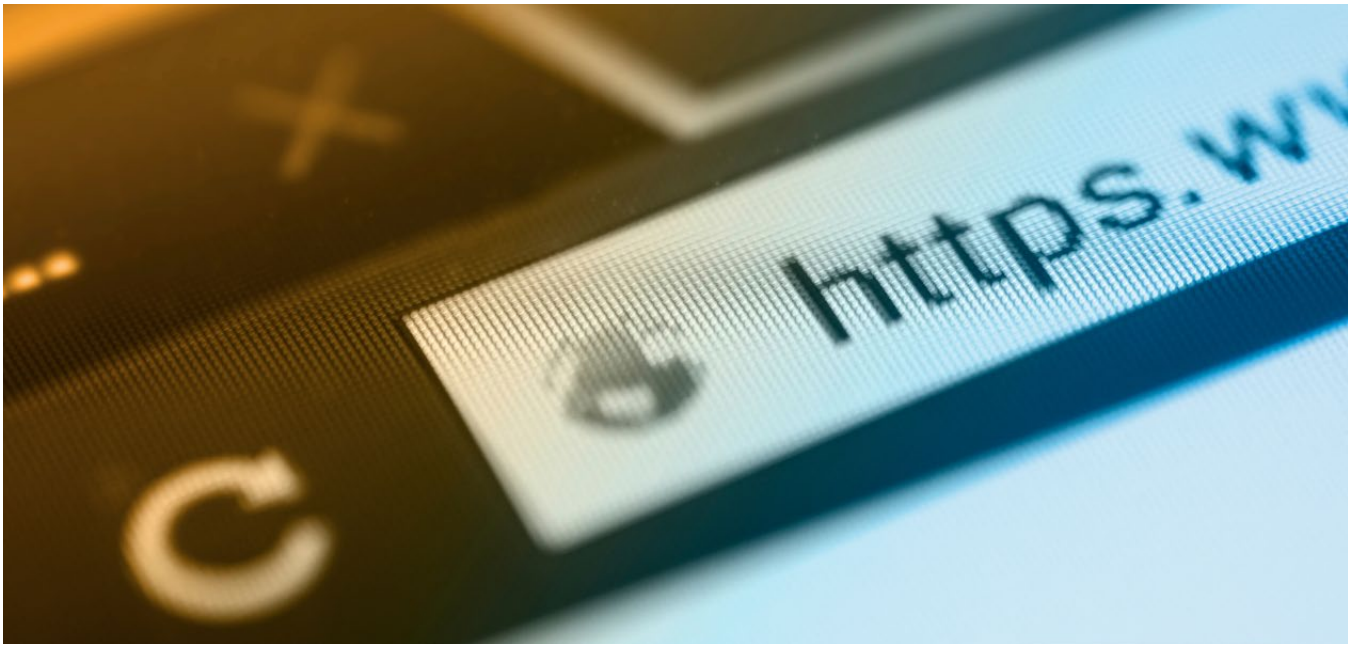
DCSA to Update Security Training URLs

The Security Training, Education, and Professionalization Portal (STEPP) and the Security Awareness Hub (SAH) will be updating the URLs for all training resources, effective June 30, 2025.

This update is part of an ongoing effort to enhance the security and functionality of these platform's online resources. The current URLs will be deactivated on June 30, so users will need to update links if they are bookmarked.

What does this mean for you?

- Both STEPP and SAH will have new URLs on June 30, 2025.
- New STEPP link: **https://securitytraining.dcsa.mil/** will replace https://cdse.usalearning.gov/
- New SAH link: **https://securityawareness.dcsa.mil/** will replace https://securityawareness.usalearning.gov/
- Current URLs will be deactivated on June 30, 2025.
- Users will need to update URL links only if they are bookmarked.

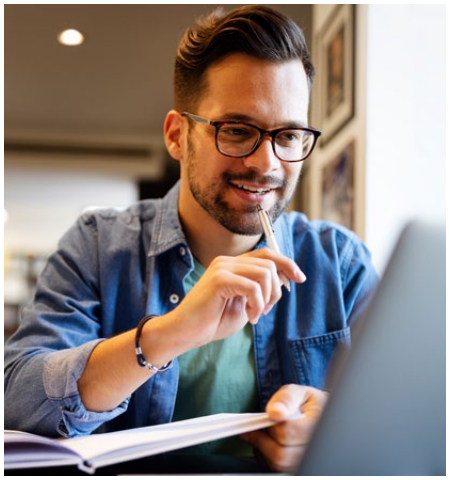


EDUCATION & TRAINING

CDSE Education Division's 8-week Courses

This fall, two 8-week tuition-free virtual instructor-led courses will be offered, starting August 18 through October 12: **Writing and Communication Skills in the Security Environment** (ED202.10) and **The Security Triangle: Security, Law Enforcement, and Intelligence** (ED402.10). The courses are worth 80 PDUs to maintain a **Security Professional Education Development (SPēD)** certification. Register to secure your spot in these courses today!

For more detailed information about these courses, visit CDSE Education at **www.cdse.edu/education**.



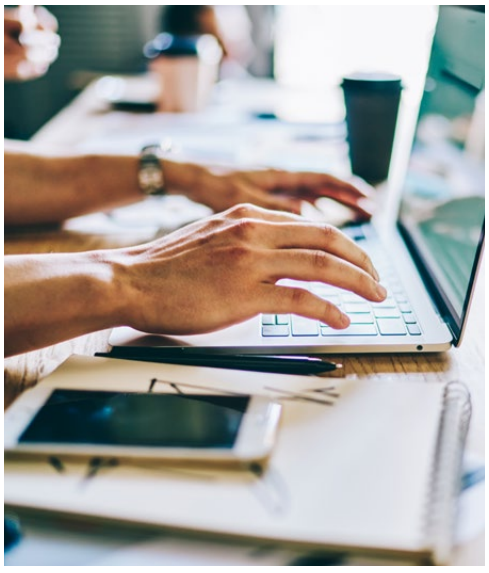
CDSE Education Division's 16-week Courses

Registration opened June 18 in the STEPP system for the fall semester of the Education Division's 16-week courses. The courses will run from August 18 to December 14, 2025.

The 16-week courses focus on strategic thinking, collaborative leadership, and effective thinking. The courses are graduate-level and worth three credit hours.

In addition to earning 160 Professional Development Units (PDUs) for completing a course, learners are able to use the courses toward maintenance of their **Security Professional Education Development (SPēD) certification** upon completion.

CDSE Education Division's Post-Baccalaureate Certificate (PBC) Program



CDSE Education Division's Post-Baccalaureate Certificate (PBC) program offers graduate-level courses designed to expand DOD security specialists' knowledge on the security profession and prepare them for leadership positions and responsibilities.

The five asynchronous, post-baccalaureate security certificates are in Risk Management, Security Leadership, Security Management, Security (Generalist), and Systems and Operations at no cost to students.

Read more about the PBC program **here**. For more information or to apply, click **here**.

PERSONNEL VETTING

New Personnel Vetting (PV) Job Aids

PV Scenarios: Continuous Vetting. Continuous Vetting (CV) is one of the five personnel vetting scenarios and is a near real-time review of a covered individual's background. This trifold job aid answers your questions about CV including how CV works, the benefits of CV, and who is subject to CV.

National Security Adjudication. National Security Adjudication is an examination of an individual's life to determine if that individual is an acceptable security risk and to make a trust determination. This job aid provides an overview of the national security adjudicative process; defining the whole person concept, identifying the 13 adjudicative guidelines, and the adjudicative factors used in evaluating the relevance of an individual's conduct.

PV Scenarios: Upgrades, Transfer of Trust, and Re-Establishment of Trust. This trifold provides a description of three of the five vetting scenarios, along with the common requirements and outcomes of each. These vetting scenarios apply to current and former trusted insiders and include upgrades, transfer of trust (ToT), and re-establishment of trust (RoT).

Click **here** to download, print, and distribute to your security workforce today!

Personnel Vetting Seminar

CDSE is presenting the virtual instructor-led "**Personnel Vetting Seminar**" on August 5-6. This seminar addresses the requirements associated with the reform of the Federal Government's personnel vetting system, known as TW 2.0. This course aids personnel vetting practitioners in DOD, Federal agencies, and private industry to understand TW 2.0 requirements, identify gaps between current and future procedures, and support implementation. The seminar covers end-to-end personnel vetting operations, including the Federal Background Investigations Program, National Security Adjudications, and Continuous Vetting in a collaborative environment. The course consists of two half-days and targets U.S. Government security practitioners, military personnel, cleared industry Facility Security Officers, and other Federal personnel performing personnel vetting security-related duties and for personnel executing security programs for cleared industry.

COUNTERINTELLIGENCE

New Counterintelligence Case Study: Jareh Sebastian Dalke

The Counterintelligence team has released a new case study, "**Jareh Sebastian Dalke**." This job aid highlights attempted espionage by Dalke, a former U.S. Army enlisted soldier who worked as a civilian information systems security designer at the National Security Agency (NSA). He held a top-secret clearance and maintained access to sensitive compartmented information.

Dalke began working at NSA on June 6, 2022, and shortly thereafter requested a 9-month leave of absence to care for a family member's medical condition. On June 28, 2022, following a denial of his extended leave request, Dalke resigned and was officially terminated July 1, 2022.

However, during his short 4-week tenure at NSA, Dalke printed and improperly retained three classified documents. Dalke was 32 years old at the time of sentencing and pleaded guilty on October 23, 2022, to six counts of attempting to transmit classified National Defense Information to an agent of the Russian Federation. He was sentenced to 262 months in prison.

FY26 Counterintelligence Curriculum Theme: Innovation

What would happen if the Nation's secure communications and encryptions were rendered useless through disruption or total compromise? How would leaders and warfighters communicate securely? Now, imagine the same happening to financial systems and networks to include compromise of the blockchain that serves as the transactional foundation for all digital assets. That would be catastrophic to national security and economy. These are the potential scenarios the Nation faces from foreign intelligence entities and adversaries as they work to gain the quantum computing and AI advantage.

Quantum computing and artificial intelligence (AI) require innovative approaches to provide training and awareness of these complex and critical topics. The CDSE CI training and awareness team will be incorporating quantum computing into the FY26 CI curriculum in addition to expanding its content related to AI, fraud, and behavioral science.

Foreign intelligence entities and adversaries are working to take the lead in ***quantum computing*** and AI. That includes employment of illicit activities to acquire quantum computing and AI technology or access to personnel, facilities, systems, and/or information. Quantum computing has applications that hold the promise of significant advancements across multiple domains to include AI, cryptography, and financial modeling. AI can be used to enhance data pattern recognition and accelerating AI development.

The CDSE CI team has already incorporated AI-related products into its curriculum to include a video short, a webinar, and another webinar scheduled for July 17, 2025. The curriculum will continue to expand its AI content in the remainder of FY25 and into FY26, especially as AI intersects quantum computing. Cryptography can necessitate the development of quantum encryption methods, especially with respect to secure and encrypted systems. Training and awareness about quantum computing and the domain of cryptography will provide the Defense Security Enterprise and warfighters with an overview of the threats and risks posed by foreign intelligence entities and adversaries. Illicit activities conducted by foreign intelligence entities and adversaries can be used to fund activities that target U.S. personnel and interests. CDSE will host a webinar on this topic with the Department of Treasury on September 18, 2025. Not only has there been an increase in online and digital financial transactions, but there has also been an increase in the use of digital assets.

Quantum computing may be used as a potential method to access or compromise financial and digital assets and the blockchain, which is the digital, distributed, and often public ledger that records transactions across many computers. Each "block" contains data, and blocks are linked cryptographically, making it difficult to alter or tamper with individual blocks without affecting the entire chain. This decentralized and transparent system ensures that transactions are secure and verifiable. The CI curriculum will address the threats and risks posed by foreign intelligence entities and adversaries' potential use of quantum computing to harm personnel, facilities, information, and systems. With the FY26 theme of "Innovation", CDSE will provide relevant, informative, and interesting products in the upcoming year, adding to its already-innovative products on AI, fraud, and behavioral science.

On May 22, 2025, CDSE addressed the relevance of behavioral science to counterintelligence in a collaborative webinar with the DCSA CI Partnership Branch and Behavioral Threat Analysis Center, Defense Insider Threat Management and Analysis Center. The webinar titled, "Psychology and Counterintelligence: A Mission Critical Intersection," had more than 1,000 registered webinar participants from government and industry.

More information and resources about the Counterintelligence Training and Awareness Curriculum and CDSE can be found by accessing the CDSE website **here**.

New Counterintelligence Poster: "Lawful Dealings, Unlawful Aims"

A new CI poster has been released, "**Lawful Dealings, Unlawful Aims**." The poster is intended to explore how legitimate business dealings are frequently used as a vehicle for an illicit activity that enables the theft of technology and innovation. CI professionals have a responsibility to help key stakeholders understand and identify these risks and implement mitigations.

New CI Job Aid: CI Driving Discussions About Critical Assets

The Counterintelligence team has released a new job aid, "**CI Driving Discussions About Critical Assets**."

This job aid explores how organizations in government, industry, and academia are targeted by motivated adversaries seeking to steal, exploit, manipulate, or sabotage their sensitive or valuable information, infrastructure, and/or assets. While CI professionals are responsible for identifying and mitigating these respective organizational risks, doing so can be a challenge without a clear understanding of what each organization deems most vital.

INDUSTRIAL SECURITY

Industrial Security Basics Course (IS122.16)

Interested in learning more about the National Industrial Security Program? Gain a better understanding of the NISP with CDSE's refreshed **Industrial Security Basics** eLearning course. Students will learn about the industrial security basics, including the purpose of regulatory documents that form the basis of the NISP, the primary roles within it, and the authorities that oversee its operation. Recommended participants include DOD Security Specialists with Industrial Security responsibilities, DCSA Industrial Security Representatives, and DCSA Industrial Security Headquarters Personnel. Increase your industrial security knowledge today!

INFORMATION SECURITY

Marking Syntax Short (IFS0048)

The DOD Security Training branch's information security team published a new version of the **Marking Syntax Short** on May 5. This new version of the security short addresses needed updates to ensure the classification security marking guidance is aligned with both DOD and IC regulatory guidance. The security short also implemented strategic minor quality improvements to enhance learner engagement and learning transfer of the content.

FY25 COURSES

Upcoming FY25 Courses

CDSE's instructor-led training (ILT) or virtual instructor-led training (VILT) courses are a great way to earn professional development units (PDUs) and maintain Security Professional Education Development (SPēD) Program certifications and credentials.

Secure your spot now as classes fill quickly! Available ILT/VILT courses are listed below.

Cybersecurity
Assessing Risk and Applying Security Controls to NISP Systems (CS301.01)
- September 22 - 26, 2025 (Linthicum, Md)

Industrial Security
Getting Started Seminar for New Facility Security Officers (FSOs) VILT (IS121.10)
- August 5 - 8, 2025 (Virtual)

Information Security
Activity Security Manager VILT (IF203.10)
- July 28 - August 24, 2025 (Virtual)

Insider Threat
Insider Threat Detection Analysis VILT (INT200.10)
- June 23 - 27, 2025 (Virtual)
- July 21 - 25, 2025 (Virtual)
- August 18 - 22, 2025 (Virtual)
- September 22 - 26, 2025 (Virtual)

Personnel Security
Personnel Vetting Seminar VILT (PS200.10)
- August 5 - 6, 2025 (Virtual)

Physical Security
Physical Security and Asset Protection (PY201.01)
- August 18 - 22, 2025 (Linthicum, Md)

Special Access Programs
Introduction to Special Access Programs (SA101.01)
- August 5 - 8, 2025 (Lexington, Ma) (MIT)
- September 9 - 12, 2025 (Rolling Meadows, Il) (NGC)

Orientation to SAP Security Compliance Inspections (SA210.0)
- August 11 - 12, 2025 (Lexington, Ma)

SAP Mid-Level Security Management (SA201.01)
- July 14 - 18, 2025 (Linthicum, Md)

CDSE & DCSA NEWS

American Council on Education (ACE) to Conduct Virtual Site Visit at CDSE

Leadership from the Center for Development of Security Excellence (CDSE) welcomed the Sweden Delegation to the Security Training Directorate, in Linthicum Md. for a day of learning sessions on May 7. The Sweden Delegation conducted reciprocal security site visits throughout the National Capital Region and met with senior leaders from Defense Technology Security Administration, the Office of the Under Secretary of Defense for Intelligence & Security - Physical Security, Defense Counterintelligence and Security Agency, and Raytheon.

DCSA Security Academy Delivered the "Investigator Field Course" VILT

From March 16 to 24, the BI Training's Investigator Training team delivered a VILT to include four live, virtual training sessions and roughly 230 hours of additional structured on-the-job training. The training helped to prepare 31 BI Field Agents from across the country for a successful transition from a learning environment to live, independent casework.

STAFF SPOTLIGHT

Meet Lisa Brumfield, new Special Access Program (SAP) Instructor

Lisa Brumfield is the new Special Access Program (SAP) instructor, effective May 5. A former Industrial Security Specialist instructor on the Industrial Security team and an Air Force veteran, she has spent over 23 years working in security.

Brumfield said the opportunity to transition back into SAP is a full circle moment – just 13 years ago, she sat in the SAP course as a student aspiring to be an instructor.

"It makes me smile and reminds me that you have to go for what you want and make it happen," she said. "I'm excited to join the SAP team and getting spun up again on SAP."

Brumfield explained that knowledge is power, and she is getting reacquainted with new policy changes and regulations to ensure she is fully educated on SAP updates and how to pass those on to students.

"I'm so glad to be reintroduced to SAP. The goal is to protect national security and let new folks coming in know about their responsibilities and that it starts with them," she said. "I am of the mindset of educating before something happens versus after the fact, so SAPs are an even more critical part of the mission. In the SAP world, it is the extra layer of security, and for the players involved you want to drive home the goal of national security - there's such a delicate balance and protection is so critical."

In the evolving security landscape, Brumfield stresses the important role SAPs play in combating our adversaries.

"Our adversaries are getting smarter, and we have to be three steps ahead and know which way they're coming and thwart it. Education is key to that," she said.

Security education has always been of utmost importance to Brumfield. She is a member of NCMS, The Society of Industrial Security Professionals and during her tenure she served on the Board of Directors as the Controlled Unclassified Information (CUI) Chairperson. Brumfield is passionate that security education is key, and government and industry go hand-in-hand.

"I continue to gain knowledge about the security field every chance I get, and I attend every security conference and try to help out behind the scenes. I'm happy to pay it forward and for people coming into the SAP program, it is such a crucial time in our country. Everything must be above board when it comes to SAPs."

ABOUT DCSA

The Defense Counterintelligence and Security Agency (DCSA) provides industrial security engagement and counterintelligence support to secure the trustworthiness of the U.S. government's workforce, contract support, technologies, services, and supply chains.

Our Role
We protect America's trusted workforce, trusted workspaces, and classified information. To do so, we have two fundamental missions: personnel security and industrial security. Supporting these two core missions are counterintelligence and insider threat and security training. For over 50 years, our agency has used each of these missions to meet the threats of our nation's adversaries.

How We Serve
DCSA is the largest investigative service provider in the federal government, supporting over 100 federal entities. We oversee 12,500 cleared facilities under the National Industrial Security Program (NISP). We rely on the following directorates to ensure the security of our nation's technologies and information.

Personnel Security
We deliver efficient and effective background investigations, continuous vetting, and adjudications. In doing so, we safeguard the integrity and trustworthiness of the federal and contractor workforce. We conduct background investigations for 95% of the federal government, including 105 departments and agencies. We also adjudicate 70% of the federal government's adjudicative determinations.

Industrial Security
At DCSA, we oversee 12,500 cleared facilities under the National Industrial Security Program (NISP). We make sure companies are protecting their facilities, personnel, and associated IT systems from attacks and vulnerabilities.

Counterintelligence and Insider Threat
Counterintelligence and insider threat supports both our personnel security and industrial security missions. Counterintelligence focuses on foreign insider threat while insider threat is focused on internal threat. In this mission center, we identify and stop attempts by our nation's adversaries to steal sensitive national security information and technologies.

Security Training
Our agency is comprised of nationally accredited training centers. These centers provide security training, education, and certifications for security professionals across the federal government and industry.

CDSE CONTACT LIST

Mailing/Postal Address
938 Elkridge Landing Road
Linthicum, Md 21090

STEPP (Learning Management System) Help Desk
Submit an online support request ticket or call the Help Desk at 202-753-0845 within the Washington, DC area or toll free at 833-200-0035 on weekdays from 8:30 a.m. to 6:00 p.m. Eastern Time.

508 Compliance and Accessibility
cdseaccessibility@mail.mil

Certification Division/SPēD Project Management Office
dcsa.spedcert@mail.mil

Education Division
dcsa.cdseeducation@mail.mil

Outreach and Engagement Office
dcsa.ncr.cdse.mbx.cdse-communications@mail.mil

Training Division
dcsa.cdsetraining@mail.mil

Webinars
dcsa.cdsewebinars@mail.mil

Webmaster
dcsa.cdseweb@mail.mil

Still not sure whom to contact?
dcsa.ncr.dcsa-cdse.mbx.cdse-front-office@mail.mil