CDSE DIRECTOR'S CORNER

Standing Strong: CDSE Director Sets Focus on Community, Connection, and Communication

By Tammi Bush

Audrey Gutierrez
(Photo by Joseph DeLuco)

"This year for me and for CDSE is going to be about reinvigorating the community, ensuring there's no daylight between CDSE and the professionals we serve," expressed the Center for Development of Security Excellence (CDSE) Director Audrey Gutierrez.

In her first year as director for CDSE, part of the Defense Counterintelligence and Security Agency's (DCSA) Security Training (ST) operating component, the organization received 11 awards and recorded more than 5.5 million course completions. Gutierrez reflected on accomplishments and highlights from the year and shared her goals for 2026, her appreciation for CDSE's ability to not only weather the storm, but also to rise above challenges as the premier provider of integrated security training services.

During a year marked by Government reform initiatives for increased efficiency that included leadership transitions, organizational realignments,

CDSE BY THE NUMBERS

5.5M
Course Completions

2.3M
DoW Security Training Credentials Provided

500K
Students Covering Over 40 DoW and non-DoW Institutions

and growing expectations, CDSE successfully navigated challenges collectively as a team by actively engaging and educating the community responsible for protecting national security.

"We've had continued strong enrollment during workforce uncertainty, which tells us that our content remains relevant, and it remains highly valuable, and we continue to get positive qualitative feedback from our customers. When we're seeing high satisfaction, sustained demand, repeat engagement through both the numbers and the qualitative feedback, we know we're delivering the right training to the right audience at the right time," Gutierrez said.

Defining a single target audience by job title or population is inherently complex, so CDSE measures success through several reinforcing indicators rather than relying on a single metric but using both qualitative and quantitative measures.

"In terms of qualitative, we have annual curriculum review meetings across security disciplines where curriculum managers are sitting down with stakeholders and talking about what's working and where we can improve," Gutierrez said.

Ensuring a close, transparent relationship with the security professionals CDSE serves is critical for success. In 2025, Gutierrez embraced the "people first" leadership philosophy by focusing on flow to guide how she listens and how she leads, believing it can unlock motivation and innovation.

"In turn," she explained, "people are more apt to spend time in their areas of strength, push decision-making down to the lowest appropriate level, and, most importantly, trust subject matter experts to lead, innovate, and adapt."

She firmly believes in using flow to align individuals' strengths, autonomy, and purpose, which in a practical sense means optimizing roles and responsibilities.

"Flow directly supports a culture of continuous learning because autonomy fuels intrinsic motivation, that is all over the research," Gutierrez said. "That philosophy then extends into the classroom so it's like a double dip because we are teachers walking the talk and, in the classroom, it encourages experimentation and innovation in instructional design and methodology."

This type of learning environment, driven by the flow mindset, is what Gutierrez believes sets the stage for people to ask questions, make mistakes, and adjust accordingly – ultimately creating an organization and learning environment where growth, adaptability, and innovation are the norm.

In 2026, Gutierrez's new vision will focus on community, connection, and communication. She plans to shift the focus to reengage and partner with the security community. These efforts will include an increase in strategic communication, stronger two-way engagement to highlight innovation across the enterprise, and further opportunities for stakeholder collaboration.

Gutierrez credits CDSE staff for exemplifying the fundamental pillars of resilience, professionalism, grit, and an unwavering commitment to the mission. In times of uncertainty, clear and open communication is the light that guides us forward. She believes the moments of flux provide the true measurement of strength.

Communication alone is not the solution, but it fosters a sense of community. Gutierrez expressed that it is the foundation upon which we build a sense of community – internal teams, valued external partners, and everyone our work touches. Building connection and a unified community fuels collaboration, inspires innovation, and reinforces purpose, she added.

Gutierrez praised CDSE's accomplishments throughout 2025, particularly for remaining focused and flexible as the threat environment continued to evolve.

Among the top achievements was CDSE's flagship effort for Security Professional Education Development (SPēD) modernization, continuing Trusted Workforce 2.0 implementation, and positioning CDSE for the future of role-based credentials. Additionally, CDSE strengthened stakeholder engagement, ensuring offerings remained relevant while expanding mobile and on-site training options.

"We are changing at an accelerating pace and so we are going to continue supporting the warfighter by remaining agile, leaning into anticipation and innovation," Gutierrez said. "We will be actively embracing AI and emerging technology, continuously scanning the threat and operational environments, and staying closely aligned with stakeholder needs. Supporting the warfighter requires anticipation, not reaction."

DCSA's Security Training is setting the foundation of a fully successful security enterprise and Defense Industrial Base (DIB), equipping security professionals with the skills, knowledge, and ability to secure the trustworthiness of the U.S. Government workforce, the integrity of cleared contractor support, and the uncompromised operation of technologies, services, and supply chains. With ST's commitment to security education, comes advancing the mission and strengthening national security as a premier provider of integrated security services.

Defined by an accelerating pace of change, modern warfare requires organizations to be proactive and innovative.

It is no longer enough to react; CDSE must proactively invest in technologies, cultivate talent that enables us to foresee future challenges, and develop groundbreaking

solutions to ensure the warfighter has the decisive edge both today and tomorrow, expressed Gutierrez. For those new to the field or in the pipeline, Gutierrez reminds that while the landscape is constantly shifting, the mission and expertise have never been more important. National security is a stabilizing force in a turbulent world, and stability and clarity are more vital now than ever.

"As a new security professional, you are joining a field where the mission matters deeply, and that cuts across the turbulence in the environment. Yes, the environment is rapidly evolving, but you're going to rapidly evolve with it, and your growth and adaptability, the degree to which you can attain those things, is going to directly impact national security," she said.

A security career is one that rewards curiosity, integrity, and continuous learning in what Gutierrez calls "the sweet spot."

"We are going to continue to exist to support security professionals at every stage, whether just starting out or stepping into a leadership role; you're not just entering a job, you're joining a community of professionals protecting the nation, and it goes back to that theme of community of practice that I really want to double down on this year."

With the start of the new year, Gutierrez is prepared to champion open communication, embrace the security community, and deepen connections that bind us. Together, we are not just resilient – we are stronger, more united, and ready for whatever comes next, Gutierrez said.

The journey, and what it takes to get there, reminds Gutierrez of Elton John's 1983 song "I'm Still Standing," an anthem celebrating strength and resilience in the face of adversity.

CYBERSECURITY

Instructor-Led Training: Assessing Risk and Applying Security Controls to National Industrial Security Program (NISP) Systems (CS301.01)

The cybersecurity team is offering a new training, "**Assessing Risk and Applying Security Controls to NISP Systems**." This course provides guidance on applying policies to protect information delineated by the Risk Management Framework (RMF) process and a comprehensive review of contractor requirements under the NISP.

The target audience for this training includes information system security managers (ISSMs), information system security officers (ISSOs), and facility security officers (FSOs) involved in the planning, management, and execution of security programs for cleared industry.

In-person courses will be offered at Linthicum, Md., on the following dates:

- Feb. 2-6, 2026
- May 4-8, 2026
- Aug. 17-21, 2026
- Register via STEPP **here**.

PERSONNEL VETTING

Overview of Federal Personnel Vetting e-Learning

Stay current on personnel vetting reform with the "**Overview of Federal Personnel Vetting**" e-Learning course.

Geared toward adjudicators and individuals performing national security adjudicative functions, this course aligns with Trusted Workforce (TW) 2.0 transformational changes to the security, suitability, and credentialing (SSC) enterprise. Registration is restricted to students with a .gov or .mil email address. The course satisfies gap training requirements for those who previously took PS001.18 and PS101.01 or PS101.10 prior to April 2025.

INSIDER THREAT

FY26 Insider Threat Detection Analysis Course (ITDAC) Schedule Released

The FY26 schedule for the "**Insider Threat Detection Analysis Course** (INT200.10)" (ITDAC), has been released. This course, specifically designed for insider threat analysts, applies critical thinking skills and analytic techniques to potential insider threat indicators.

The course uses simulated cases to analyze reports, gather information and build context, as well as to develop effective mitigation strategies.

The virtual course will be offered on the following dates:

- Feb. 9-13, 2026
- March 16-20, 2026
- April 13-17, 2026
- May 11-15, 2026
- June 8-12, 2026
- July 13-17, 2026
- Aug. 17-21, 2026
- Sept. 21-25, 2026

To register, click **here**.

INFORMATION SECURITY

Activity Security Manager InfoSec VILT Course Schedule for FY26 (IF203.10)

The January iteration of "Activity Security Manager for InfoSec" VILT kicks off on Jan. 25 and runs through Feb. 22. **Registration** closes Jan. 14.

This mid-level four-week course covers application and implementation of security policies and procedures to mitigate and manage risks associated with developing, managing, and evaluating the Information Security Program (ISP).

This course is for civilian, military, and contractor personnel with primary duties as an activity security manager, information security program specialist, or manager within a component ISP. Students are expected to have a functional working knowledge of the ISP.
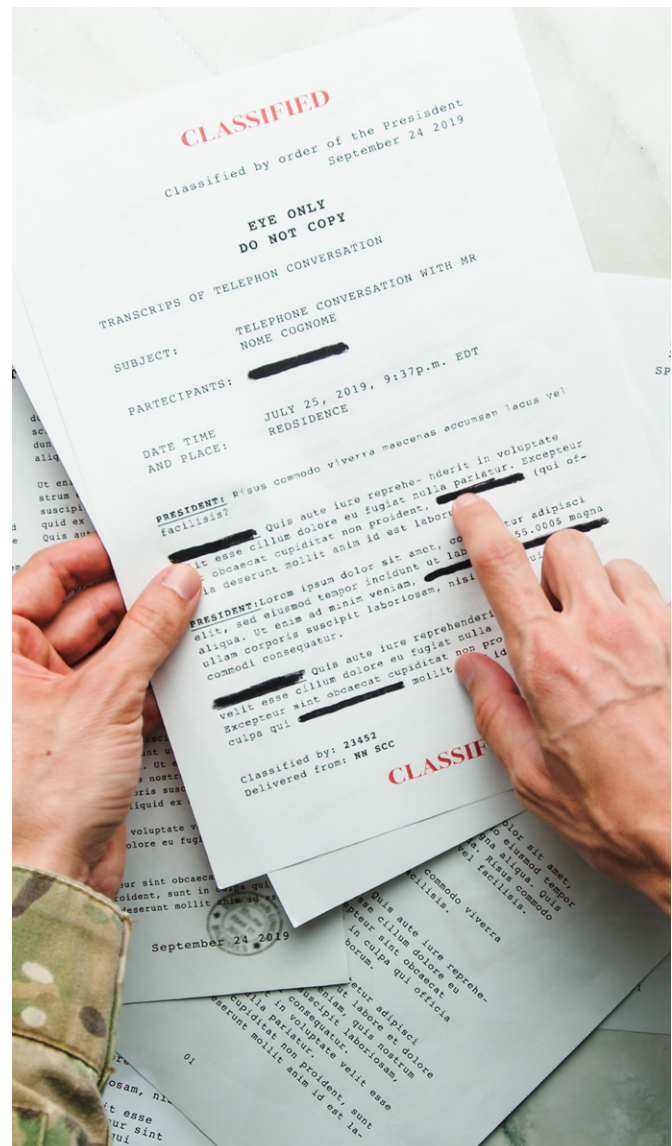
Streamline Workflow with Expert Job Aids

Marking Syntax for U.S. Classified Information job aid supports civilian, military and contractor personnel in correctly in applying marking syntax to classified information in accordance with regulatory guidance.

Original Classification Authority (OCA) Desktop Reference outlines the steps in the original classification process that OCAs must adhere to when determining classification decisions.

NOFORN/RELTO: A Quick reference Guide to Two Dissemination Controls job aid provides an overview of how and when to properly apply the NOFORN and RELTO dissemination control markings in accordance with regulatory guidance.

Transmission and Transportation for DOD IF107.16

An all new "Transmission and Transportation for DOD" course is now available. This two-hour course offers a comprehensive scenario-based learning opportunity that covers authorized procedures, methods, and dissemination requirements for transmitting and transporting classified information in accordance with regulatory guidance. **Register** today to take this course.

BEHAVIORAL THREAT ANALYSIS CENTER

BTAC Bulletin

The Behavioral Threat Analysis Center (BTAC) Bulletin is a monthly newsletter offering timely and relevant insider threat guidance and resources.

The bulletin is produced by a multidisciplinary team of experts in threat assessment/threat management, law enforcement, counterintelligence, behavioral science, employee management relations, and cybersecurity.

View the latest BTAC Bulletin **here**.

Beyond The Bulletin Podcast

DOD Insider Threat Management and Analysis Center (DITMAC) has released a new podcast "Behavioral Threat Analysis Center – Beyond the Bulletin." Tune in for the **interview**, led by DITMAC Director James Shappell, with Peter Lapp and Dr. Kristin Schneider, where they discuss the vision for the BTAC, the Bulletin, and the podcast.

SPECIAL ACCESS

FY26 Special Access Programs Course Calendar Released

The FY26 Special Access Program (SAP) training calendar is available. The "Introduction to Special Access Programs (SAPs)" course provides an overview of security requirements outlined in the DOD Special Access Program Security Manual 5205.07, as well as incorporates practical student course exercises for new SAP security professionals. **In-person** and **virtual** training options are available.

In-Person Course Schedule

- March 3 - 6, 2026 (Korea)
- March 10 - 13, 2026 (Hawaii)
- April 21 - 24, 2026 (Linthicum, Md.)
- May 12 - 15, 2026 (Linthicum, Md.)
- Aug. 4 - 7, 2026 (San Diego, Calif.)
- Aug. 25 - 28, 2026 (Cincinnati, Ohio)

VILT Course Schedule

- June 1 - 9, 2026 (Virtual)

UPCOMING WEBINARS

The Impacts of Artificial Intelligence and Emerging Technologies on the Cybersecurity Landscape

Jan. 14, 2026 | 11:00 am to 12:00 pm ET

Artificial Intelligence (AI) Risks and Threats to National Security

Jan. 22, 2026 | 1:00 pm to 2:30 pm ET

Misconduct to Resolution: Planning to Prevent Unintended Consequences

Jan. 29, 2026 | 1:00 pm to 2:30 pm ET

FY 2026 UPCOMING COURSES

Registration Now Open

CDSE courses are a great way to gain security knowledge, gain awareness, and expand skill sets. Secure your spot now as classes fill quickly! **Available** instructor-led training (ILT)/VILT courses are listed below.

Cybersecurity
Assessing Risk and Applying Security Controls to NISP Systems (CS301.01)
   • Feb. 2 - 6, 2026 (Linthicum, Md.)
   • May 4 - 8, 2026 (Linthicum, Md.)
   • Aug. 17 - 21, 2026 (Linthicum, Md.)

General Security
DOD Security Specialist (GS101.01)
   • Feb. 3 - 11, 2026 (Redstone Arsenal, Ala.)
   • March 17 - 25, 2026 (Linthicum, Md.)
   • June 2 - 10, 2026 (Linthicum, Md.)
   • Aug. 11 - 19, 2026 (Germany)
   • Sept. 15 - 23, 2026 (Linthicum, Md.)

DOD Security Specialist VILT (GS101.01)
   • Jan. 5 - Feb. 1, 2026 (Virtual)
   • April 6 - May 3, 2026 (Virtual)
   • July 6 - Aug. 2, 2026 (Virtual)

Industrial Security
Getting Started Seminar for New Facility Security Officers VILT (IS121.10)
   • March 24 - 27, 2026 (Virtual)
   • May 12 - 15, 2026 (Virtual)
   • July 21 - 24, 2026 (Virtual)

Information Security
Activity Security Manager VILT (IF203.10)
   • Jan. 25 - Feb. 22, 2026 (Virtual)
   • April 19 - May 17, 2026 (Virtual)
   • July 26 - Aug. 23, 2026 (Virtual)

Insider Threat
Insider Threat Detection Analysis Course VILT (INT200.10)
   • Feb. 9 - 13, 2026 (Virtual)
   • March 16 - 20, 2026 (Virtual)
   • April 13 - 17, 2026 (Virtual)
   • May 11 - 15, 2026 (Virtual)
   • June 8 - 12, 2026 (Virtual)
   • July 13 - 17, 2026 (Virtual)
   • Aug. 17 - 21, 2026 (Virtual)
   • Sept. 21 - 25, 2026 (Virtual)

Personnel Vetting
Advanced National Security Adjudication VILT (PS301.10)
   • June 1 - 11, 2026 (Virtual)
   • Sept. 14 - 24, 2026 (Virtual)

Fundamentals of National Security Adjudications VILT (PS101.10)
   • April 20 - 29, 2026 (Virtual)
   • July 20 - 29, 2026 (Virtual)

Physical Security
Physical Security and Asset Protection (PY201.01)
   • Feb. 2 - 6, 2026 (Linthicum, Md.)
   • April 6 - 10, 2026 (Linthicum, Md.)
   • May 11 - 15, 2026 (Linthicum, Md.)
   • June 8 - 12, 2026 (Linthicum, Md.)
   • Sept. 14 - 18, 2026 (Linthicum, Md.)

Physical Security and Asset Protection VILT (PY201.10)
   • Feb. 23 - March 13, 2026 (Virtual)

Special Access Programs
Introduction to Special Access Programs (SA101.01)
   • March 3 - 6, 2026 (Korea)
   • March 10 - 13, 2026 (Hawaii)
   • April 21 - 24, 2026 (Linthicum, Md.)
   • May 12 - 15, 2026 (Linthicum, Md.)
   • Aug. 4 - 7, 2026 (San Diego, Calif.)
   • Aug. 25 - 28, 2026 (Cincinnati, Ohio)

Introduction to Special Access Programs VILT (SA101.10)
   • June 1 - 9, 2026 (Virtual)

Orientation to SAP Security Compliance Inspections (SA210.01)
   • Feb. 18 - 19, 2026 (Linthicum, Md.)
   • Aug. 31 - Sept. 1, 2026 (Cincinnati, Ohio)

SAP Mid-Level Security Management (SA201.01)
   • July 13 - 17, 2026 (Linthicum, Md.)

Staff Spotlight: Nicholas Stephanadis, Counterintelligence Instructor

By Tammi Bush

Nicholas Stephanadis is a seasoned intelligence leader with over 20 years of experience in counterintelligence (CI), insider threat, and risk management across government, industry, academia, and non-profits. Serving as a CI instructor at CDSE over the past year and a half, he empowers security professionals with CI principles that have a profound impact on a variety of job functions.

Through his instructional work, Stephanadis directly supports CDSE's mission to advance the security posture of the DOW and federal workforce by ensuring personnel have a working understanding of foreign intelligence threats, the broad array of risks posed, and the role every individual has in mitigating risk. He strives to develop training products to address evolving CI concerns, both technical and non-technical.

"To some, the foreign intelligence threats may seem unrealistic," Stephanadis said. "Our objective is twofold—not only educate on the reality of the risks, but ensure students come away understanding they have a significant role in helping combat these risks. We all do."

Stephanadis spent the first decade of his career in the U.S. Intelligence Community at the nexus of CI and critical infrastructure protection efforts. He subsequently shifted to private industry, spending eight years holding operational and leadership roles in CI and insider threat programs within the aerospace and defense sector.

"Knowledge is meant to be passed along. And it's that exchange that I find really gratifying," he adds.

In 2012, Stephanadis founded a Defense Intelligence Agency team focused solely on providing CI support to defense critical infrastructure. He is a member of the Intelligence and National Security Alliance (INSA) and serves on its Insider Threat Subcommittee. In 2022, Stephanadis founded SpotStone, an organization that engages with government, industry, and academia to understand and mitigate human-enabled risk.

For fiscal year 2026, CDSE's CI team is incorporating three content areas into the curriculum: adversarial targeting of technology, quantum computing, and fraud. These new content areas will be included in eLearning, case studies, job aids, posters, and webinars. The CI team also provides CI training and awareness instruction in four CDSE courses that include the "Fundamentals of National Security Adjudications," "DOD Security Specialist Course," "Getting Started Seminar for New Facility Security Officers," and the "Mid-Level Special Access Program Manager's Course." The CI team hosts two CI webinars annually and collaborates with the CI Partnership Branch, DCSA, on four quarterly webinars. Learn more about the CI curriculum here.

In his free time, Stephanadis stays busy as a father of two daughters and enjoys being outside, learning music and playing musical instruments.

Stephanadis explained that what attracted him to the CI field is the impact and strategic nature of the work.

"The most rewarding piece of this type of work is to pass along important nuggets to people that can mitigate and have an impact," he said. "The ease with which people can get their hands on and the amount of information available online is always a concern. There are even more opportunities to do this work than ever before."

CDSE NEWS

CDSE NEWS: Defense Security Training Council

Prior to retiring, former DCSA Director David Cattler signed an action memo "Improving Alignment Among Security Certification Programs" instructing Security Training to:

1. Align the Adjudicator Certification Governance Board with the Security Professional Education Development (SPēD) Program and Department of Defense Security Training Council (DSTC), and

2. Align the Certified Insider Threat Professional Governance Council with the SPēD Program and DSTC.

The SPēD Program Management Office is executing plans of action to revise each charter to improve security certification alignment, streamline decision making, and increase oversight.

In addition, a Fiscal Year 2025 (FY25) annual Department of Defense Security Skill Standards (DS3) review was conducted between March and June of 2025 utilizing subject matter expert feedback to update the DS3 v10.0 published in 2024. The Department of Defense Security Skills Standards (DS3) Version 10.1 serves as a critical component of the security accreditation and certification program and defines the competencies and knowledge required of security practitioners. It serves as the foundation for education, training, and certification. The latest version includes minor administrative updates and revised policy.

Leaders from DCSA on the Airwaves

FORT MEADE, Md. – Leaders from the Defense Counterintelligence and Security Agency (DCSA) take to the airwaves! U.S. Army Chaplain Napoleon Bradford (left) joins Audrey Gutierrez (center), Director of the Center for Development of Security Excellence (CDSE), and Cashmere He (right), DCSA's Outreach and Engagement Branch Chief for Security Training, co-anchor the DCSA Deeper Dive newscast at the Defense Media Activity on Dec. 11. *(Photo by Christopher Gillis, Defense Counterintelligence and Security Agency)*

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