CDSE
LEARN. PERFORM. PROTECT.

SETA PULSE

VOLUME 7 ISSUE 7 | July 2026

CDSE SETA Pulse

The CDSE Security Education Training and Awareness (SETA) Pulse is an official monthly newsletter published by the Security Training Directorate Outreach and Engagement Office. Editorial content is the responsibility of the Center for the Center for Development of Security Excellence (CDSE) under the oversight of the DCSA Office of Communications and Congressional Affairs.

Leadership

Joseph M. Tonon, Ph.D.
Director, DCSA

Audrey Gutierrez
Director, CDSE

Editorial Staff

Cashmere He
Chief Content Officer

Jenise Kaliszewski
Tammi Bush
Content Contributors

Marc Pulliam
Content Designer

Contact Us

CDSE Security Training Directorate
938 Elkridge Landing Road, Linthicum, MD 21090
https://www.cdse.edu
dcsa.ncr.cdse.mbx.cdse-communications@mail.mil

Center for Development of Security Excellence

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

SETA FOCUS

Role-Based Certification Pilot Evolves Security Workforce

By Tammi Bush

The Center for Security Excellence (CDSE) launched the Role-Based Certifications (RBC) program, evolving the Security Professional Education Development (SPēD) initiative. The new Department of War (DoW) training sets a benchmark for the security workforce to strengthen national defense.

The RBC framework shifts security certification from an agnostic knowledge test to structured learning progression, which leads to an RBC to validate on-the-job competency. Open to all security DoW civilians, military personnel, and contractors in direct support of DoW, the program expands skill sets, standardizes training, and defines professional excellence across the Defense Security Enterprise (DSE).

"RBCs combine foundational prerequisites (eLearning) with application-based instructor-led training and a comprehensive assessment to ensure every certified professional is equipped to meet the demands of their role and the mission of the DoW," said Glenn Stegall, CDSE deputy director.

By equipping security professionals with practical skills, the DoW ensures its workforce serves as effective advocates who mitigate risks and apply critical countermeasures during strategic and tactical planning. The initiative underscores the DoW's commitment to building an adaptable security workforce.

"This is an important first step to rebuilding our professionalization pipeline and helping to standardize the security workforce. Previously, we had training agnostic certifications that served to validate that people had the knowledge, skills, and abilities to do a job for a specific role," said Audrey Gutierrez, CDSE director. "Now, we're taking another look at that with an authentic adult learning and community building approach, and going back to our stakeholders to develop in lockstep a pipeline that truly scaffolds development up to those standard levels of competency."

The framework will roll out in phases, prioritizing critical security disciplines. Five certifications will be launched by March 2027. The program begins with the Information Security RBC pilot, focusing on the Information Security (InfoSec) role, from July 26 to Aug. 23. This phase sharpens core competencies in risk mitigation, classification management, and incident response.

A working group of certification holders shaped the new program to focus on specific job roles and career

milestones. For current SPēD certification holders (as of March 2025), expiration dates are automatically extended to March 2027.

"The SPēD Evolution is more than a certification update -- it's a commitment to standardize security training, sustain capability standards, and empower every member of the security workforce to be an effective advocate for security in DoW planning and operations," Stegall said.

CDSE & DCSA NEWS

Registration Coming Soon for 2026 Virtual DCSA Security Conference

Join us virtually this September for five days of cutting-edge insights, collaborative problem-solving, and expert-led discussions. This year's conference is designed to maximize value by dedicating specific days to the unique needs of security professionals.

To ensure you experience the most relevant and impactful programming, the week is organized into focused tracks. Review the schedule below and register for the days that best align with your mission and professional focus:

DATES	FOCUSED PROGRAMMING	IDEAL AUDIENCE
Sept. 14 – 15	**Industrial Security Track:** Monday and Tuesday's sessions focus on specific topics, challenges, and compliance standards impacting Industrial Security.	Industrial Security Professionals
Sept. 16 – 18	**DOW and Federal Government Track:** Wednesday through Friday deliver strategic content tailored to military and government operations, interagency collaboration, and national defense priorities.	DoW personnel and Security Professionals in the federal government *(requires .gov, .mil, or government affiliated .edu email address to register)*

Visit the **conference website** or follow CDSE on socials for important updates on registration opening.

CDSE Launches New SETA eLearning Courses

By Katharine Rubinsky

In June, CDSE launched four new self-paced eLearning courses designed to deliver more effective and strategic Security Education, Training, and Awareness (SETA).

SETA is a comprehensive program designed to enhance the knowledge, skills, and behaviors of personnel regarding organizational security policies, procedures, and best practices.

These skills-based courses move beyond standard briefings to equip security training personnel of all experience levels with the practical knowledge to identify vulnerabilities and develop targeted solutions for their commands.

"The goal of these new courses is to further equip individuals responsible for SETA with a strong foundation in adult learning theory and data-driven instructional strategies," said Dr. Monica Minor-Exum, CDSE division chief. "By focusing on evidence-based approaches, we aim to help security professionals design and deliver training that leads to measurable improvements in performance and mission readiness."

The new courses include:

- **Training Delivery Methods (EA110.16)** Instructs participants on selecting the best training delivery options for specific audiences and objectives, exploring traditional, virtual and blended approaches.
- **Understanding Learning Objectives and Mapping Assessments (EA120.16)** Covers the creation of clear learning objectives and effective assessments, including instructional basics and the ABCD format.
- **The Fundamentals of ADDIE for Instructors (EA130.16)** Examines the ADDIE model of instructional design, teaching students to apply each phase to improve training materials and outcomes.
- **Instructor Presentation and Communication Techniques (EA140.16)** Provides strategies to engage audiences, remove communication barriers and deliver content confidently.

Interested personnel can learn more by visiting the **CDSE Education eLearning portal** and enroll directly through **STEPP**. Through SETA initiatives, CDSE remains committed to building a stronger, more secure defense community.

INSIDER THREAT

Insider Threat Detection Analysis Course (200.10)

The Insider Threat Detection Analysis Course (ITDAC) provides practical hands-on exercises for federal insider threat program analysts. The course equips participants with skills to master data analysis, critical pathway theory, and threat response to protect national security. Spaces are limited. Secure your spot today by visiting the **ITDAC page**.

Upcoming virtual sessions:

- July 13 - 17, 2026
- Aug. 17 - 21, 2026
- Sept. 21 - 25, 2026

Defense Contractor's Fraud Scheme: The Case of Craig Klund

How was a two-time convicted felon able to successfully compete for defense contracts and commit extensive fraud schemes?

Klund, a 58-year-old military contractor, was involved in deceptive and illegal financial practices, including fraud. Undeterred by two prior felony convictions, he executed a scheme to defraud the DOD by obtaining defense contracts under false pretenses. Klund pleaded guilty to several fraud-related charges and was sentenced to 10 years in prison, three years of supervised release, and ordered to pay nearly $436,000 in restitution.

Klund supplied defective parts to the military that had the capacity to harm military personnel and the public. Could this insider threat have been identified sooner? What mechanisms are in place to counter acquisition fraud in the DoW?

Read the case study for details of the crime, its operational impact, and the critical risk indicators that could have mitigated the harm.

New Insider Threat Security Shorts

Have 10 minutes to spare? Tune into three new security shorts to learn the impact insider threats have on the following topics:

- **Human Resources**
- **Cybersecurity**
- **Law Enforcement**

BTAC Bulletin

Learn about evolving security risks with the latest **Behavioral Threat Analysis Center Bulletin**. Each month, experts in counterintelligence, law enforcement, and behavioral science deliver authoritative analysis on insider threats.

INDUSTRIAL SECURITY

Getting Started Seminar for New Facility Security Officers (IS121.10)

The virtual Getting Started Seminar trains FSOs and security specialists to navigate complex requirements effectively and apply fundamental National Industrial Security Program (NISP) requirements.

Register now for the July 21 - 24, 2026 course.

CYBERSECURITY

Assessing Risk and Applying Security Controls to NISP Systems (CS301.01)

Gain critical training to manage cleared industry systems in the Assessing Risk and Applying Security Controls to NISP Systems course. Designed for ISSMs, ISSOs and FSOs, this course teaches the Risk Management Framework (RMF) through practical application.

Explore the curriculum and **register** for the Aug. 17 - 21 course in Linthicum, Md.

PERSONNEL VETTING

Personnel Vetting Management Course (PS126.10)

CDSE is offering a new Personnel Vetting Management course. This one-week virtual training equips security practitioners with the essential tools and processes to conduct end-to-end personnel vetting. This course is specifically designed to support security practitioners managing Individuals in national security sensitive positions.

Along with Trusted Workforce 2.0 requirements, participants will gain expertise across the entire vetting lifecycle to include federal personnel vetting program, background investigations, national security adjudications, continuous vetting, insider threat, and security review proceedings.

This course is offered exclusively to government and military personnel. Applicants must meet all eligibility requirements and complete prerequisites.

Register today for an upcoming virtual course.

- July 27 – 31, 2026
- Sept. 21 – 25, 2026

Fundamentals of National Security Adjudications VILT (PS101.10)

Gain the skills to identify security concerns and make personnel security determinations in CDSE's virtual course, "Fundamentals of National Security Adjudications" from July 20 - 24. **Register** today to secure your spot.

Personnel Vetting Training Videos

Part 4 of the Personnel Vetting Process is now available! This series of short videos covers personnel vetting from end-to-end, with part 4 focusing on the continuous vetting process. View all releases **here**.

PHYSICAL SECURITY

Physical Security and Asset Protection (PY201.10)

Master the skills needed to protect critical assets in the "Physical Security and Asset Protection" (PY201.01) course. This intensive course will teach you to apply the risk management process, develop robust security plans for facilities and justify recommendations to leadership. Gain the confidence to safeguard infrastructure and personnel by securing your seat in the upcoming Linthicum, Md. sessions. Limited seats available! **Register** today!

Register now for:

- Sept. 14 - 18, 2026

SPECIAL ACCESS PROGRAMS

Special Access Program (SAP) Courses

Special Access Program courses are tailored by skill level with practical exercises that bring the material to life, building confidence and skills to excel in your role. Review the course options, choose a course date below and register today!

Introduction to Special Access Programs (SA101.01)
- Aug. 4 - 7, 2026 (San Diego)
- Aug. 25 - 28, 2026 (Cincinnati)
- Sept. 8 – 11, 2026 (El Segundo, Calif.)

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

Back-to-Back SAP Training

Fast-track SAP expertise with the streamlined training path that pairs the introductory course and compliance inspections courses at one location over two consecutive weeks. Note: Successful completion of "Intro to SAPs" is a prerequisite for attending the "SAP Security Compliance Inspections" course.

Option 1 - San Diego
- **Intro to SAPs (SA101.01)**: Aug. 4 - 7
- **Orientation to SAP Security Compliance Inspections (SA210.01)**: Aug. 10 - 11

Option 2 – Cincinnati
- **Intro to SAPs (SA101.01)**: Aug. 25 - 28
- **Orientation to SAP Security Compliance Inspections (SA210.01)**: Aug. 31 - Sept. 1

FY 2026 UPCOMING COURSES

Registration Now Open

CDSE offers a variety of training through different platforms and mediums:

- **eLearning courses** are online, self-paced courses to fit your busy schedule.
- **In-person courses** are offered in Linthicum, Md. and various mobile training sites.
- **Virtual instructor-led courses** offer collaborative learning without travel.

Access the full schedule of upcoming courses **here**.

Cybersecurity
Assessing Risk and Applying Security Controls to NISP Systems (CS301.01)
- Aug. 17 - 21, 2026 (Linthicum, Md.)

General Security
DOD Security Specialist (GS101.01)
- Aug. 11 - 19, 2026 (Germany)
- Sept. 15 - 23, 2026 (Linthicum, Md.)

DOD Security Specialist (GS101.01)
- July 6 - Aug. 2, 2026 (Virtual)

Industrial Security
Getting Started Seminar for New Facility Security Officers (IS121.10)
- July 21 - 24, 2026 (Virtual)

Insider Threat
Insider Threat Detection Analysis Course (INT200.10)
- July 13 - 17, 2026 (Virtual)
- Aug. 17 - 21, 2026 (Virtual)
- Sept. 21 - 25, 2026 (Virtual)

Information Security
Activity Security Manager (IF203.10)
- July 26 - Aug. 23, 2026 (Virtual)

Personnel Vetting
Advanced National Security Adjudication (PS301.10)
- Sept. 21 - 25, 2026 (Virtual)

Fundamentals of National Security Adjudications (PS101.10)
- July 20 - 24, 2026 (Virtual)

Personnel Vetting Management Course (PS126.10)
- July 27 – 31, 2026 (Virtual)
- Sept. 21 – 25, 2026 (Virtual)

Physical Security
Physical Security and Asset Protection (PY201.01)
- Sept. 14 - 18, 2026 (Linthicum, Md.)

UPCOMING WEBINARS

View all upcoming CDSE events **here**.

Malice, Mental Illness, and Mitigation: Understanding the Role of Mental Illness in Targeted Violence
July 15, 2026 | 1300 -1430 ET

The Nexus Between Counterintelligence and Fraud
July 16, 2026 | 1200 -1330 ET

AI and Cybersecurity: Adversarial Techniques and Managing Risk
August 5, 2026 | 1000 -1100 ET

STAFF SPOTLIGHT

Staff Spotlight: Lydia Israel, Program Analyst

By Tammi Bush

Lydia Israel, a program analyst, has worked at CDSE for three years. Last month Israel proudly celebrated her 12-year federal service anniversary – spanning nine years of service with the U.S. Navy and three years with DCSA. Israel previously served as a U.S. Navy security manager before transitioning to project management at DCSA.

As a program analyst, Israel supports the Technology Liaison Division (TLD) within Security Training. Bridging the gap between DCSA and IT, she evaluates, monitors and resolves IT issues to optimize organizational effectiveness.

"I translate complex business needs into actionable IT solutions while tracking system performance and ensuring operational efficiency," Israel said. "My role is unique to the organization because I provide behind-the-scenes support as the designated point of contact for troubleshooting and executing IT initiatives specific to CDSE's mission."

She also manages software licenses and acquires software and support.

Staff can contact Israel for software licensing, platform integration, records management, and acquisition technology. However, rapidly evolving technology and policies present constant challenges. Israel noted that her primary focus is staying ahead of emerging technology while ensuring secure delivery to customers.

Ultimately, Israel aims to advance technology and improve organizational platforms to streamline the user experience.

"There is never a dull moment working in TLD," Israel said. "Because I often assist colleagues facing technical distress or capability gaps, I focus on delivering positive customer experiences. The focus of my job is to work with people who are in distress or are lacking some sort of capability to perform their job," she said. "Knowing this, I look forward to providing customer experiences and being able to help. I strive to contribute to meaningful outcomes that push the mission forward."

Outside of work, Israel tutors and mentors high school students and young adults with disabilities. A health and fitness enthusiast, she is training for her 16th half marathon. For relaxation, Israel enjoys cycling, reading at local parks, and traveling to visit family and friends.

VIGILANCE CAMPAIGN TOOLKIT

JOB AIDS

Derivative Classification
Information Security | Link

SHORTS

Defense In Depth
Cybersecurity | Link

GAME

Spot The Vulnerabilities
Industrial Security | Link

CASE STUDY

Xiaoqing Zheng Case Study
Insider Threat | Link

WEBINARS

Personnel Vetting Timely Topics - Continuous Vetting
Personnel Vetting | Link

SAP Visit Certifications FAQs
Special Access Programs | Link

POSTERS

Preparation-Mouse
Security Awareness | Link

CDSE Makes That Possible
Security Awareness | Link

eLEARNING COURSES

Counterintelligence Awareness and Reporting for DOD
Counterintelligence | Link

VIDEO

DOD Security Principles
General Security | Link

ILT

DOD Security Specialist
General Security | Link

Physical Security and Asset Protection
Physical Security | Link

Introduction to Special Access Programs
Special Access Programs | Link

VILT

Getting Started Seminar for New Facility Security Officers
Industrial Security | Link

Activity Security Manager (InfoSec)
Information Security | Link

Insider Threat Detection Analysis
Insider Threat | Link

Personnel Vetting Management
Personnel Vetting | Link

TOOLKIT

Physical Security Toolkit
Physical Security | Link

WEBSITE

Certification
Security Awareness | Link

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, D.C. 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

Professional Development 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