CDSE
LEARN. PERFORM. PROTECT.

SETA PULSE

VOLUME 7 ISSUE 9 | September 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

Protecting Our Potential: September is National Insider Threat Awareness Month

As the Department of War (DoW) and federal security landscape rapidly evolves, we must recognize that our greatest vulnerabilities often originate from within. September marks National Insider Threat Awareness Month (NITAM), a critical time for security practitioners across the enterprise and cleared industry to refocus on the early detection and proactive mitigation of insider risks.

This year's theme, "Protect Our Potential," centers on recognizing behavioral indicators and fostering a robust culture of reporting. While technology and physical security are vital components of our defense, our most effective countermeasure remains an educated and vigilant workforce.

The Strategic Value of SETA

An effective Insider Threat program does not exist in a vacuum; it is driven by comprehensive Security Education and Training Awareness (SETA). As security practitioners, your SETA programs are the first line of defense. Consistent, high-quality training transforms the workforce from passive bystanders into active defenders.

When personnel understand the "why" behind security protocols, they are far more likely to identify the subtle behavioral anomalies that precede a kinetic event, unauthorized disclosure, or act of espionage. SETA empowers employees to trust their instincts and utilize established reporting channels without fear of reprisal.

Recognizing the Indicators and Early Intervention
Insider threats manifest in various ways, ranging from unintentional negligence and data spills to deliberate sabotage and workplace violence. By continuously training our personnel on common behavioral indicators, we enable early intervention. Warning signs often include:

- Unexplained or sudden affluence.
- Working odd hours without authorization or a clear mission requirement.
- Inappropriate interest in matters outside the scope of one's duties.
- Unexplained travel to foreign countries.

Early intervention saves lives, secures mission-critical data, and often provides the individual in crisis with the help they need before a catastrophic event occurs.

2026 DCSA Security Conference
Further expanding on these themes, insider threat discussions will be embedded throughout the 2026 DCSA Security Conference, held virtually Sept. 14-18. Consistent with this year's NITAM theme, sessions throughout the week will cover a variety of advanced insider threat topics, offering practitioners new strategies to safeguard their facilities and personnel.

Take Action
We encourage all security professionals to review their current SETA materials and prepare to integrate this year's NITAM resources. View the NITAM page and access campaign resources **here**.

CDSE & DCSA NEWS

Countdown to Collaboration: 2026 Virtual DCSA Security Conference

We are just days away from kicking off the 2026 DCSA Security Conference. Join us for actionable insights, collaborative problem-solving, and expert-led discussions.

The schedule is structured into tracks dedicated to the unique needs of security professionals. Review the specialized tracks below and **register** for the days that directly align with your operational 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)*

SPēD Program Modernization Update

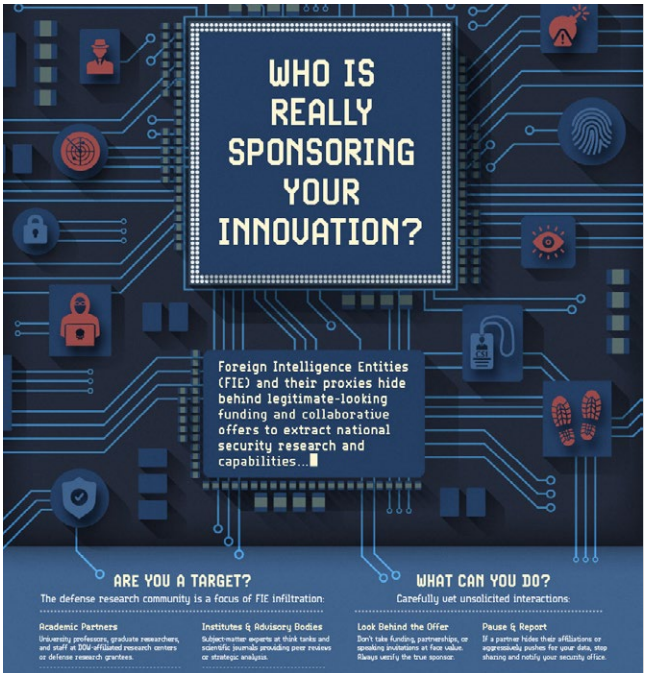
As part of the ongoing SPēD program modernization, we are currently executing several Role-Based Certification (RBC) pilots designed to standardize and enhance security training across the Defense Security Enterprise. These pilots focus on delivering a streamlined learner experience that seamlessly integrates core training with final assessments, allowing successful participants to earn their certification and a new digital badge in one consolidated step.

Moving forward, the program will continue to evolve by rolling out updated Performance and Competency Models, simplifying the registration process, and establishing clear pathways for credential maintenance. We are actively incorporating learner feedback from these initial pilots to ensure the new RBCs effectively meet the needs of our security professionals.

COUNTERINTELLIGENCE

New Poster: Who's Really Sponsoring Your Innovation?

The new **Who's Really Sponsoring Your Innovation poster** highlights how foreign intelligence entities exploit research funding and collaborative offers to target cutting-edge academic and industrial innovation. View all available security posters **here**.



CUI Training Frequency Reduced

In a move to restore mission focus, the Department of War changed the frequency of mandatory Controlled Unclassified Information (CUI) training from an annual to a biennial (every two years) requirement. CUI training, materials, and policy will be updated to adhere to this change.

INSIDER THREAT

When "Offboarding" Goes Wrong: Darnell Albert-El Case Study

What happens when an IT Director with special access gets fired? For Virginia-based logistics firm TRANSMARX LLC, it turned into a costly lesson in insider threat management.

In February 2008, Darnell Albert-El was hired as the company's IT Director, granting him privileged administrator-level access to the entire corporate network, including their Georgia-hosted website. Just four months later, Albert-El's employment was terminated—but they failed to properly secure his access.

Fueled by anger over his firing, Albert-El used his personal computer and active admin credentials to log back into the company's web server. In a matter of minutes, he executed a series of malicious commands that deleted approximately 1,000 critical website files, causing $6,707 in immediate losses.

Following a thorough investigation by the FBI, Albert-El confessed to the digital sabotage. His retaliation scheme ultimately earned him 27 months in federal prison and a court order to pay $6,700 in restitution.

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

BTAC Bulletin

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

INDUSTRIAL SECURITY

Updated eLearning Course: Introduction to Industrial Security (IS011.16)

CDSE updated its most popular industrial security course! The one-hour **Introduction to Industrial Security** eLearning course teaches National Industrial Security Program (NISP) requirements, roles, and contracting processes. Ideal for facility security officers and industrial security specialists, this concise training clarifies critical contractor obligations in both government and private facilities. **Register today** to secure your facility's compliance.

EDUCATION

Register Now: Fall 2026 Education Semester

The semester runs from Sept. 14, 2026 – Jan. 18, 2027.

CDSE delivers education courses to prepare security professionals to master tomorrow's national security challenges. Whether you are entering the security enterprise or looking to expand your security expertise, CDSE provides practical, mission-focused learning that directly supports your professional growth. Registration closes Sept. 7.

Learn more about the courses being offered **here**. Register via **STEPP** or contact the **CDSE Education Division** for more information.

PERSONNEL VETTING

New Security Shorts

"**Reporting Requirements for the Continuous Vetting of the Trusted Workforce**"
Designed to keep individuals sharp and compliant, this short highlights reporting requirements outlined in Appendix C of the Federal Personnel Vetting Management Standards that service members, civilians, and contractors must follow. This training supports individuals subject to personnel vetting as well as security practitioners across the Security, Suitability, and Credentialing (SSC) enterprise.

"**Elements of Federal Personnel Vetting**"
Provides an overview of the 12 elements of Federal personnel vetting as described in the Federal Personnel Vetting Guidelines and introduces the security practitioners' role in each element.

"**Continuous Vetting for Non-Sensitive Public Trust**"
Provides a high-level overview of the purpose of continuous vetting (CV) for non-sensitive public trust (NSPT) positions, the policies driving the shift to CV, and the role federal agencies play in managing CV for the NSPT population.

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**.

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

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

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

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

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

Special Access Programs
Introduction to Special Access Programs (SA101.01)
- Sept. 8 - 11, 2026 (El Segundo, Calif.)

UPCOMING WEBINARS

View all upcoming CDSE events **here**.

How to Prevent Tragedy: Insights from School Shooter, Jon Romano
Sept. 10, 2026 | 1 to 2:30 p.m. ET

Supercharging the DIB: Threats and Opportunities for the DOW Battery Supply Chains
Sept. 24, 2026 | 1 to 2:30 p.m. ET

VIGILANCE CAMPAIGN TOOLKIT

JOB AIDS

Insider Threat Indicators & Reporting
Industrial Security | Link

Personnel Vetting Scenarios: Continuous Vetting
Personnel Vetting | Link

SHORTS

The Triple Threat: Counterintelligence, Cybersecurity, and Insider Threat
Counterintelligence | Link

Insider Threat Fact Finding
Insider Threat | Link

Law Enforcement and Insider Threat
Insider Threat | Link

CASE STUDIES

Peter Debbins Case Study
Insider Threat | Link

POSTERS

See What Others Miss
Insider Threat | Link

Infamous Spies: Peter Debbins
Insider Threat | Link

Protecting Our Potential
Insider Threat | Link

WEBINARS

Understanding Basic Malware
Cybersecurity | Link

Physical Security Posture: Security-in-Depth (SID)
Physical Security | Link

VIDEOS

Alleged Directed Falsification (ADF)
Personnel Vetting | Link

SAP Security Incident: Bad Start
Special Access Programs | Link

Turning People Around, Not Turning Them In S1/E2: "Check Out My New Ride"
Insider Threat | Link

eLearning

Unauthorized Disclosure (UD) of Classified Information and Controlled Unclassified Information (CUI)
Information Security | Link

Risk Management for DOD Security Programs
General Security | Link

Games

The Adventures of Earl Lee Indicator
Insider Threat | 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