CDSE
LEARN. PERFORM. PROTECT.

SETA PULSE

VOLUME 7 ISSUE 8 | August 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

August Vigilance Campaign: Anti-Terrorism Awareness

The Center for Development of Security Excellence (CDSE) is launching a series of monthly vigilance campaigns to support the Department of War (DoW) and the broader Defense Security Enterprise (DSE). Each campaign delivers curated Security Education, Training, and Awareness (SETA) products to bolster mission readiness among security practitioners.

In alignment with anti-terrorism month, August's campaign highlights anti-terrorism awareness and threat recognition. Defending personnel, facilities, and information requires constant vigilance; all personnel must understand how to recognize and mitigate evolving threats. To support these efforts, CDSE highlights existing products and resources – ranging from job aids and toolkits to case studies - designed for immediate application.

Understanding the Threat Landscape
Anti-terrorism encompasses defensive measures that reduce vulnerability to terrorist acts. Since terrorism does not exist in a vacuum, terrorism often intersects with other security disciplines and is preceded by observable behaviors. Related threats include radicalization, insider threats, targeted violence, and foreign influence (Adjudicative Guideline B).

Mitigating these threats requires a multi-layered approach:

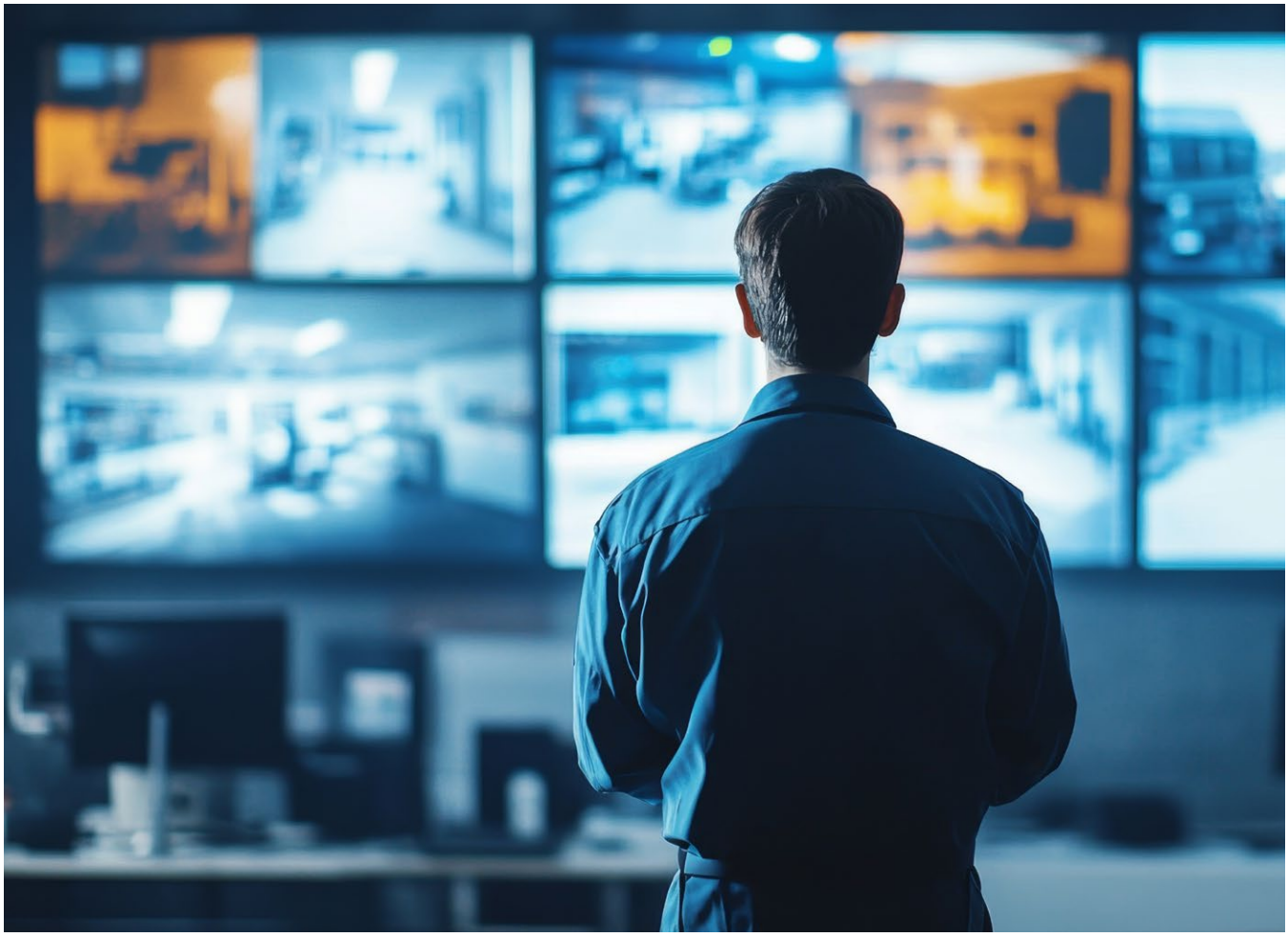
- Awareness & Identification: Recognizing the behavioral indicators and psychological processes precede radicalization or an attack.
- Physical Security: Implementing countermeasures and robust physical security plans to protect facilities and personnel.
- Preparedness: Maintaining **active shooter awareness** and crisis response readiness.
- Reporting: Adhering to reporting requirements, such as the NISP Reporting Requirements, to ensure threats are elevated to the proper authorities immediately.

Your Role in Anti-Terrorism
Every individual within the DSE has an obligation to protect our nation. Key responsibilities include:

- Reporting suspected activity: If you see something, say something. Report suspected terrorism directly to the **FBI**. Immediate reporting saves lives.
- Maintaining vigilance: Familiarize yourself with the behavioral indicators of extremism, targeted violence, and foreign preference.
- Enhancing defenses: Review and update physical security plans. *Note: Updated CDSE physical security products will be released by the end of the fiscal year.*

SETA Resources Available
CDSE provides comprehensive resources to implement anti-terrorism best practices. In addition to core anti-terrorism training, CDSE offers targeted violence toolkits, physical security job aids and case studies (such as the cases of **Mark Steven Domingo** and **James Frank**).

Access these resources at **https://www.cdse.edu**. Review the final page of this publication for this month's complete vigilance campaign product list. Leveraging these products ensures security practitioners remain equipped to defend personnel, safeguard critical information, and secure the nation.



CDSE & DCSA NEWS

Register Now: 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.

Visit the **registration portal** today to select your track and secure your attendance!

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)*

COUNTERINTELLIGENCE

New Quantum Computing Short

CDSE recently posted the latest counterintelligence security short titled, **"Counterintelligence and the Quantum Computing Race."** The five-minute short is the first CDSE course catalog product on the topic of quantum computing, its potential capabilities and the risks it poses.

The short gives an overview of quantum computing and the long-term implications for those who gain or lose technological advantage. In addition, the short provides context on the advantages of quantum computing as well as the significant counterintelligence concerns and implications of the risks threat actors potentially pose.

INSIDER THREAT

Insider Threat Detection Analysis Course (200.10)

Sharpen your technical edge as a federal insider threat program analyst with practical hands-on exercises in the "Insider Threat Detection Analysis" Course (ITDAC)! 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:

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

The Spy in the Sunset: Theft of Trade Secrets Case Study

Would you notice if a colleague was stealing your organization's most sensitive technology hidden inside a digital photo of a sunset?

For years, Xiaoqing Zheng, a 59-year-old engineer, exploited his position of trust to carry out a sophisticated campaign of economic espionage. He was systematically copying over 19,000 proprietary files to personal USB drives and utilizing software to maintain 400 unauthorized encrypted documents on his desktop. When security protocols were heightened, Zheng began using steganography to hide secret technical code within the binary data of a sunset photograph before emailing it to himself.

Following an FBI raid in 2018, Zheng confessed and was sentenced to 24 months in prison and fined $7,500 for conspiring to steal trade secrets.

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

When it comes to safeguarding our critical data, everyone has a role to play — and insider risks are a challenge we must face together.

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

CDSE Training and Updates for Industry

Watch the recorded **CDSE Training Product Updates for Industry webinar** to learn about new and updated products beneficial to cleared industry. This 30-minute webcast covers the benefits of an active security training program and provides a navigation demonstration for **cdse.edu**.

Clearances in Industrial Security: Putting it All Together (IS125.16)

"Clearances in Industrial Security: Putting it All Together," is a new eLearning course that provides a high-level overview of personnel security clearances, facility clearances, and foreign ownership, control, or influence (FOCI). This one-hour course is geared to DoW security specialists with industrial security responsibilities and DCSA industrial security personnel. **Register** today!

INFORMATION SECURITY

DoW Initial Orientation and Awareness Training (IF140.16) eLearning Course

The "DoW Initial Orientation and Awareness Training" (IF140.16) eLearning course launched on June 29. The course is designed to consolidate foundational security awareness processes, procedures, and core principles, specifically aligning with the requirements outlined in DODM 5200.01, Volume 3, Enclosure 5. DoW components retain sole authority to determine which of their specific annual mandatory training requirements are fulfilled by completing this course.

This course is a repurposed version of the previous "DoD Initial Orientation and Awareness Training" eLearning course. This new version of the course incorporates specific feedback from Defense Security Enterprise stakeholders and presents learners with a challenge to move beyond mere compliance and become a proactive champion for security awareness. **Register** today!

Updated: Controlled Unclassified Information (CUI) Life Cycle Short

A revised version of the Information Security short, "**CUI Life Cycle short #2, Safeguarding Part 1- Marking CUI**" is available.

The updated short provides guidance to safeguard CUI adhering to marking requirements outlined in the DOD Information Program and DODI 5200.48. The short is the second in a series of four shorts designed to provide DoW personnel with the "how-to" of common tasks related to protecting and handling CUI.

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.

GENERAL SECURITY

DOD Security Specialist Course (GS101.01)

Elevate your expertise in risk management and learn the fundamentals of security practices in industrial, personnel, information, and physical security disciplines with the "DOD Security Specialist" course.

This course is offered exclusively to DoW government, military, and contractor security personnel. Applicants must meet all eligibility requirements and complete prerequisites. **Register** for an upcoming course:

- Aug. 11 – 19 (Wiesbaden, Germany)
- Sept. 15 – 23 (Linthicum, Md.)

New Security Awareness Job Aid

Sharpen your instincts and pave the way for a stronger security culture in the workplace with the new **Security Awareness job aid**! This job aid outlines the 5-R Security Awareness Framework which serves as tool to move beyond compliance and safeguard our Nation's security.

EDUCATION

Register for Fall 2026 Semester of CDSE Tuition-Free Education Courses

Register for Fall 2026 CDSE Education courses which will run from Sept. 14, 2026, to Jan. 18, 2027. Courses fill quickly, so please register early to secure your spot for the fall semester. The courses, led by subject matter experts (SME) in defense security, will build competencies in strategic thinking, analytical thinking, effective communication, and collaborative leadership.

The courses are asynchronous online, tuition free, and allow students flexibility to collaborate with each other and SME instructors. During the 16-week courses, students will engage in collegiate-level reading, research, and writing assignments. Students can earn 160 Professional Development Units (PDUs). You can learn more about the courses being offered and register **here**.

For additional information, contact the CDSE Education Division at: **dss.ncr.dss-cdse.mbx.cdse-education@mail.mil**.

PERSONNEL VETTING

Personnel Vetting Management Course (PS126.10)

Explore Trusted Workforce 2.0 policy changes and requirements with the "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.

Designed to support security practitioners managing Individuals in national security sensitive positions, participants will gain insight of the complete 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 the upcoming virtual course:.

Register for the next virtual course, which will be held: Sept. 21 – 25, 2026.

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 Course (PY201.10)

Master the skills needed to protect critical assets in the "Physical Security and Asset Protection" 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 session. **Register** now for Sept. 14 - 18, 2026 (Linthicum, Md.)!

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. 25 - 28, 2026 (Cincinnati)
- Sept. 8 – 11, 2026 (El Segundo, Calif.)

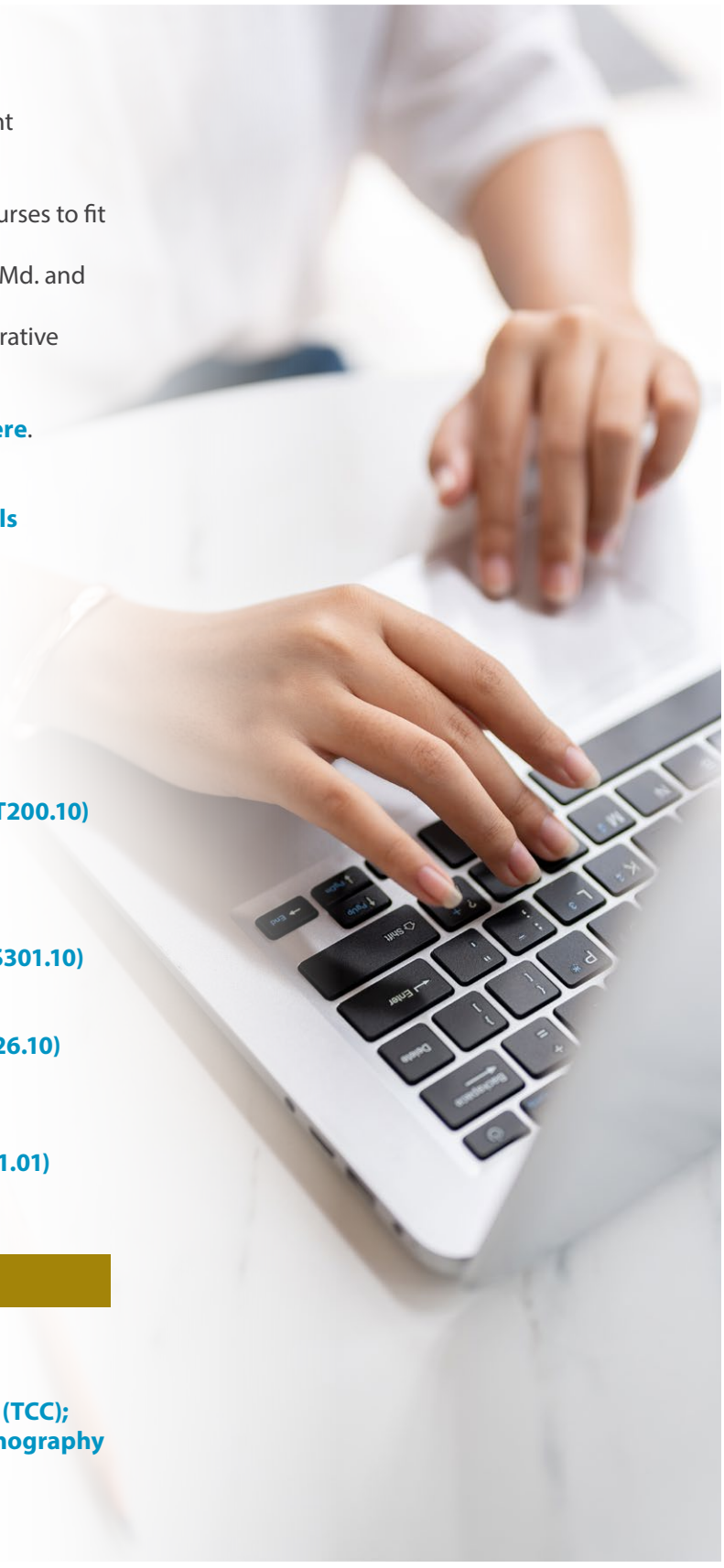
Back-to-Back SAP Training

Join CDSE in Cincinnati to fast-track SAP expertise with the streamlined training path that pairs the introductory course and compliance inspections courses over two consecutive weeks. *Note: Successful completion of "Intro to SAPs" is a prerequisite for attending the "SAP Security Compliance Inspections" course.*

- **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.)

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

UPCOMING WEBINARS

View all upcoming CDSE events **here**.

Understanding the True Crime Community (TCC); Youth Targeted Violence and Weapons Iconography
August 6, 2026 | 1:00 - 2:30 p.m. ET

STAFF SPOTLIGHT

Staff Spotlight: Caleb Armstrong, Supervisory Visual Information Specialist

By Tammi Bush

For nearly two decades, Caleb Armstrong, supervisory visual information specialist, has worked in Security Training at DCSA. Armstrong oversees the Creative Services branch comprised of graphic designers and audiovisual engineers.

Managing an award-winning creative team is a complex balancing act requiring knowledge spanning art direction, brand management, graphics, animation, filmmaking, and IT operations.

Beyond creative direction, the role demands diplomacy, property custodianship, and navigating the nuances of third-party vendors. Armstrong's primary goal is to ensure his team has what they need to be successful, comfortable, and safe. He indicated that watching team members transform an abstract requirement into a tangible, high-quality product is "akin to magic."

"I don't think anybody would disagree with me on this, but policy is dry and technical. Its quality is fraught with complexity and the fluid nature of it is inherently chaotic. The level of abstraction involved in breaking these things open, in this culture and with haste, is a quality that the creatives on the team excel at," Armstrong said. Armstrong's team turns complex ideas into simple, comprehensive visual products, ultimately ensuring that personnel can efficiently execute their roles.

"We integrate. We simplify. We enable. We beautify and amplify," Armstrong said.

Though Generative AI has recently disrupted the creative space, Armstrong asserts the final execution still relies entirely on the designer's expertise. He particularly enjoys watching his team transform a requirement into a well-crafted product. When an idea takes hold, Armstrong notices a palpable energy that becomes infectious.

"The most enjoyable part of my job is interacting with my team. I'm fortunate that I've somehow come to be surrounded by some of the most intelligent, creative, passionate, and diligent people that I've ever worked with. Not a day goes by where I don't learn from my team members and colleagues. Everything that I take away from them informs my role as a supervisor and reminds me that I still have more to learn," Armstrong said.

Outside of the office, Armstrong is a self-proclaimed "old-school nerd." When he isn't hitting the gym, you can find him reading comic books, watching movies, or playing board and video games. His favorite way to unwind is spending quiet time at home with his wife, dogs, and close friends.

VIGILANCE CAMPAIGN TOOLKIT

JOB AIDS

Behavioral Indicators and Insights for Countering a Possible Terrorist Attack
Counterintelligence | Link

Implementing Effective Physical Security Countermeasures Job Aid
Physical Security | Link

Insider threat and Extremist Activity Within the DOD
Insider Threat | Link

SHORTS

Active Shooter Awareness
Physical Security | Link

Adjudicative Guideline B: Foreign Influencer Awareness
Personnel Vetting | Link

Parts of a Physical Security Plan
Physical Security | Link

Security Incidents Reporting Short
Information Security | Link

CASE STUDIES

Frank James Case Study
Counterintelligence | Link

Mark Steven Domingo Case Study
Insider Threat | Link

POSTERS

Behavioral Indicators and Insights for Countering a Possible Terrorist Attack
Security Awareness | Link

Know the Risks
General Security | Link

WEBINARS

Behavioral Indicators and Insights for Countering Terrorism
Insider Threat | Link

Radicalization to Terrorism: Psychological Processes and Research Updates
Insider Threat | Link

SAP Visit Certifications FAQs
Special Access Programs | Link

VIDEOS

Ransomware
Cybersecurity | Link

eLEARNING COURSES

Antiterrorism Officer (ATO) Level II GS109.16
Physical Security | Link

NISP Reporting Requirements IS150.16
Industrial Security | Link

TOOLKITS

Insider Threat Target Violence Toolkit
Insider Threat | Link

Physical Security Planning Toolkit
Physical Security | 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