CDSE
LEARN. PERFORM. PROTECT.

SETA PULSE

VOLUME 7 ISSUE 6 | June 2026

CDSE Pulse

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

DCSA Leadership

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

Col. Brooke Carr
Acting Chief of Staff, DCSA

CDSE Leadership

Audrey Gutierrez
Director

Glenn Stegall
Deputy Director

Dr. Shafiah Firoz
Division Chief, DOW Security Training

Dr. Monica Minor-Exum
Division Chief, Credentialing & Certification Division

Pulse Staff

Cashmere He
Chief Content Officer

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

SETA FOCUS

June Vigilance Campaign: Securing Controlled Unclassified Information

CDSE is launching a new monthly vigilance campaign of Security Education, Training and Awareness (SETA) products to equip security practitioners including security managers, facility security officers and other professionals across the Department of War security enterprise, with curated training resources.

June's inaugural campaign spotlights the critical importance of securing Controlled Unclassified Information (CUI). Handling any form of controlled information carries significant responsibilities, and every employee must understand their duty to safeguard sensitive information.

To support this effort, CDSE provides immediate access to tools ranging from eLearning and job aids to real-world case studies. These ready-to-use resources empower the Defense Security Enterprise to reinforce vigilance and strengthen readiness across the workforce.

Understanding CUI

Controlled Unclassified Information (CUI) requires strict safeguarding and dissemination controls under applicable laws, regulations, and government-wide policies. While not formally classified, the unauthorized disclosure of CUI could damage national security, individual privacy, and other government interests. Examples of CUI include, but are not limited to, law enforcement information, financial data, and personal privacy information.

The CUI Life Cycle

Security professionals must manage CUI through five distinct stages:

- **Create, Identify, and Designate**: Recognize and designate information as CUI in accordance with regulatory guidance.
- **Safeguard**: Protect CUI from unauthorized access and disclosure.
- **Share**: Disseminate CUI only to individuals with an authorized, lawful government purpose via approved methods.
- **Decontrol**: Remove CUI controls when the information no longer requires safeguarding, adhering to DOW records management procedures.
- **Destroy**: Properly destroy CUI to prevent its recovery.

Your Role in Protecting CUI

Every individual handling CUI must actively protect it. Key responsibilities include:

- **Marking**: All CUI must be marked with "CUI" in the banner and footer of documents, and a CUI Designation Indicator block must be present on the first page.
- **Safeguarding**: Store CUI in a controlled environment, and do not leave it unattended where unauthorized individuals may see it.
- **Destroying**: Destroy CUI using approved methods, such as cross-cut shredding, to ensure it is unreadable, indecipherable, and irrecoverable.

Access SETA Resources

CDSE offers a wealth of SETA resources to help organizations seamlessly implement CUI best practices. Security practitioners can access these tools directly by clicking **here** and view this month's full vigilance campaign on the final page of this publication.

By leveraging CDSE materials and actively integrating the practices into daily operations, every security professional can protect CUI to strengthen security and safeguard critical operations.

INSIDER THREAT

Insider Threat Detection Analysis Course (200.10)

Designed for federal insider threat program analysts, the Insider Threat Detection Analysis Course (ITDAC) is an intensive training that provides hands-on, real-world exercises. Participants will master data analysis, critical pathway theory, and threat response to effectively protect national security from within. Spaces are limited. Secure your spot today by visiting the **ITDAC page**.

Upcoming Virtual Sessions:

- June 8 - 12, 2026
- July 13 - 17, 2026
- Aug. 17 - 21, 2026
- Sept. 21 - 25, 2026

From USC Graduate to Convicted Spy: The Case of Hao Zhang

How did two university friends orchestrate a massive theft of U.S. trade secrets?

Hao Zhang, a 41-year-old Chinese national, used his position within U.S. companies to systematically funnel sensitive data to China. Convicted on 26 counts—including economic espionage and theft of trade secrets—Zhang was sentenced to 18 months in prison and ordered to pay $476,835 in restitution.

Could this insider threat have been identified sooner?

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

Infamous Spies Poster Series

Promote security awareness in the workplace with the "Infamous Spies" poster series. New releases detail **Peter Debbins** and **Ana Montes**, and their respective espionage cases. Posters are **available for download**.

BTAC Bulletin

Stay ahead of 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)

Master the National Industrial Security Program (NISP) and elevate your security program.

The virtual "Getting Started Seminar for New Facility Security Officers" trains incoming FSOs and DOW specialists to navigate complex requirements successfully.

Register now for the July 21 - 24, 2026 virtual class.

CYBERSECURITY

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

Assessing Risk and Applying Security Controls to NISP Systems provides critical training for those managing cleared industry systems. Participants, including ISSMs, ISSOs and FSOs, master the Risk Management Framework (RMF) through actionable guidance and practical application.

By demystifying complex contractor requirements, the training ensures security programs maintain both compliance and resilience. This curriculum bridges the gap between regulatory theory and operational security. **Explore the curriculum and sign up**.

- Aug. 17 - 21, 2026 (Linthicum, Md.)

PERSONNEL VETTING

Personnel Vetting Management Course (PS126.10)

CDSE is now offering a brand new Personnel Vetting Management course. This one-week training runs from 8 a.m. to 4:30 p.m. ET and equips security practitioners with the essential tools and processes to conduct end-to-end personnel vetting. The curriculum specifically supports those managing eligibility for classified access or sensitive positions.

The training incorporates Trusted Workforce 2.0 requirements. Participants will gain expertise across the entire vetting lifecycle to include federal personnel vetting program, background investigations, 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.

- June 8 – 12, 2026
- July 27 – 31, 2026
- Sept. 21 – 25, 2026

PHYSICAL SECURITY

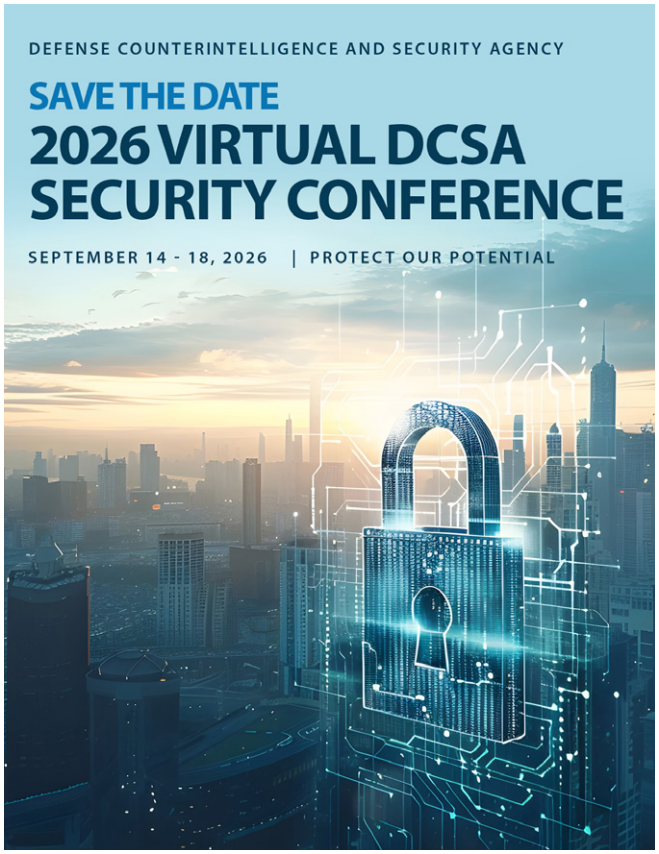
Physical Security and Asset Protection

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:

- June 8 - 12, 2026
- Sept. 14 - 18, 2026

CDSE & DCSA NEWS



Save the Date: 2026 Virtual DCSA Security Conference

By Cashmere He

The Defense Counterintelligence and Security Agency (DCSA) will host the 2026 Virtual DCSA Security Conference on Sept. 14-18.

This year's conference marks a major milestone as a consolidated initiative bringing together stakeholders from across the security spectrum. For the first time, the event unifies the Department of War and industry partners through a cohesive conference experience, fostering collaboration and a shared commitment to protecting our nation's competitive advantage and technological edge.

We invite security professionals, leaders, and practitioners to join us for a week of integrated security training, policy updates, and mission-critical briefings. We will officially launch the registration portal and release the full agenda later this summer. For more information, visit **CDSE News**.

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.)

To attend one of the wraparound options, register for each course individually.

Wraparound Course Offering

To maximize learning, consider a wraparound option where the "Intro to SAPs" course is followed by the "SAP Security Compliance Inspections" course at the same location in back-to-back weeks. Attendance for the second course depends upon successful completion of the first 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)
- June 8 - 12, 2026 (Virtual)
- 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. 14 - 24, 2026 (Virtual)

Fundamentals of National Security Adjudications (PS101.10)
- July 20 - 28, 2026 (Virtual)

Personnel Vetting Management Course (PS126.10)
- June 8 – 12, 2026 (Virtual)
- July 27 – 31, 2026 (Virtual)
- Sept. 21 – 25, 2026 (Virtual)

Physical Security
Physical Security and Asset Protection (PY201.01)
- June 8 - 12, 2026 (Linthicum, Md.)
- Sept. 14 - 18, 2026 (Linthicum, Md.)

UPCOMING WEBINARS

View all upcoming CDSE events **here**.

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

STAFF SPOTLIGHT

Staff Spotlight: Margaret Brady, Training Specialist and Course Manager

By Tammi Bush

Margaret Brady, a familiar face at the Center for Development of Security Excellence (CDSE), recently transitioned to the role of training specialist and course manager. After nearly four years supporting the mission as a contractor, her move to federal service marks a new chapter supporting the Department of War and broader security missions.

In her new role, Brady oversees General Security courses, most notably the flagship Security Specialist Course. Her role encompasses the entire educational development lifecycle, from initial concept and ongoing maintenance to eventual retirement. Instructors deliver the curriculum through a mix of eLearning, in-person sessions, and mobile training iterations.

Security training profoundly impacts the security posture across every branch of the military and amongst industry partners. By facilitating mandatory annual training -- including the highly attended "OPSEC Awareness for Military Members, DOD Employees and Contractors" -- the General Security team ensures personnel consistently reinforce and modernize critical security protocols.

Staying ahead of continuous policy changes across different teams can be challenging, Brady said. Adapting to these shifts requires flexibility and continuous awareness of the evolving security landscape.

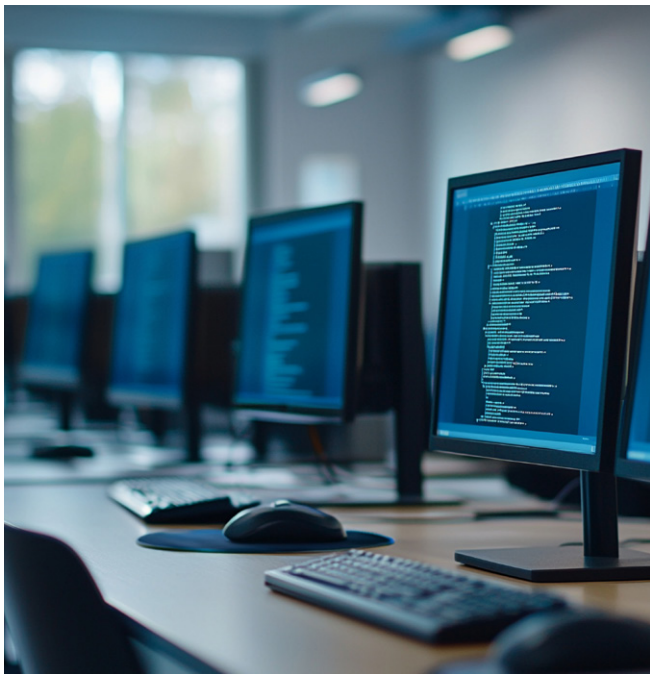
Training a diverse range of security professionals, including foreign nationals, is the most rewarding part of the job, Brady added.

"This exposure provides a unique, macro-level perspective on what security means globally," Brady said. "Furthermore, the strong sense of camaraderie within CDSE—where mutual respect and teamwork are paramount—creates a supportive environment that bolsters the larger mission."

Brady focuses on actively growing and evolving course offerings. The General Security team proactively adapts to the shifting needs of security training with several exciting projects on the horizon.

Currently, the team is developing a foundational security course tailored for international students. This new curriculum parallels the Security Specialist Course while diving deeper into the fundamental reasoning behind security practices. Additionally, the team will take the Security Specialist Course on the road this summer, conducting mobile training in Germany.

Beyond the daily rigors of course management and security training, Brady often sits courtside. A dedicated volleyball fan and parent, she spends much of her free time cheering on her daughter, who competes for a national-level club team based in Baltimore. This June, they will travel to Orlando, Fla. to compete in the Junior National Championships for the third consecutive year.



VIGILANCE CAMPAIGN TOOLKIT

JOB AIDS

Understanding Espionage and National Security Crimes
Counterintelligence | **Link**

Security Incident Job Aid
Industrial Security | **Link**

CUI Training Template
Information Security | **Link**

SHORTS

CUI Life Cycle Short #1: Create/Identify and Designate CUI
Information Security | **Link**

CUI Life Cycle Short #2: Safeguarding Part 1 - Marking CUI
Information Security | **Link**

CUI Life Cycle Short #3: Safeguarding Part 2 and Sharing
Information Security | **Link**

CUI Life Cycle Short #4: Destroying and Decontrolling CUI
Information Security | **Link**

Parts of a Physical Security Plan
Physical Security | **Link**

Special Access Programs: Markings
Special Access Programs | **Link**

GAME

Adjudicative Guidelines Word Search
Personnel Vetting | **Link**

CASE STUDY

Aldrich Ames Case Study
Insider Threat | **Link**

WEBINARS

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

Transmission or Transportation of Classified Materials by Industry
Industrial Security | **Link**

Kicking Off a CUI Awareness Campaign
Information Security | **Link**

POSTERS

Infamous Spies: Aldrich Ames
Insider Threat | **Link**

Packing
Security Awareness | **Link**

eLEARNING COURSES

Risk Management Framework (RMF) Implement Step (CS104.16)
Cybersecurity | **Link**

Introduction to Risk Management (GS150.06)
General Security | **Link**

VIDEO

Packaging Classified Documents
Information Security | **Link**

TOOLKIT

Controlled Unclassified Information (CUI) Toolkit
Information 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