



**THIS
MONTH'S
FOCUS**

SAFETY TIPS FOR SAFE TRAVEL

DID YOU KNOW?

Tis' the season: phishing attacks spike during the holidays, with a 52 percent increase. (CISCO)

 CDSE – Center for Development of Security Excellence

 @TheCDSE

 Center for Development of Security Excellence

 Center for Development of Security Excellence

CDSE Pulse

Published by the Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) Outreach and Engagement Office.

DCSA Leadership

David M. Cattler Daniel J. Lecce
Director, DCSA *Deputy Director, DCSA*

Kevin Jones Erika Ragonese
Assistant Director, Security Training *Deputy Assistant Director, Security Training*

CDSE Leadership

Audrey Gutierrez Glenn Stegall
Director *Deputy Director*

Pulse Staff

Cashmere He Isaiah Burwell
Chief Content Officer *Content Writer*

Matthew Wright Marc Pulliam
Tammi Bush *Content Designer*
Content Contributors

Many DOD personnel and cleared contractors will travel for vacation during the holiday season. Whether traveling within the United States or overseas, personnel with security clearances are at the same risk for criminal activities as other travelers and are prime targets of Foreign Intelligence Services (FIS).

Personnel with access to classified information or who hold a sensitive position must report unofficial/official foreign travel prior to departure in accordance with agency/organization policy. Security professionals should educate their workforces about travel risks, how to mitigate them, and actions to take in the event of an issue. Individuals should learn about potential threats, how to minimize their risks, and what to do in the event of an incident. CDSE, the U.S. State Department, and the National Counterintelligence and Security Center (NCSC) have travel security resources. Many resources focus on foreign travel, but some of the threats (criminal activities/foreign intelligence targeting/etc.) and mitigation strategies also pertain to travel in the United States. These resources can raise travel-related security awareness within individuals and organizations.

A security briefing is one of the primary ways to educate DOD and cleared industry personnel regarding travel risks, mitigation strategies, and available travel resources. Security information related to travel can be given through a general security awareness briefing or travel briefing. CDSE

offers a Defensive Security Briefing and a Counterintelligence (CI) Foreign Travel Briefing. CDSE also has several security awareness travel posters that can be shared online or placed within facilities. Defensive travel briefings alert personnel to potential harassment, exploitation, provocation, capture, entrapment, or criminal activity. They also provide courses of action to mitigate adverse security and personal consequences. The briefings suggest passive and active measures to avoid becoming targets or inadvertent victims. The Defensive Security Briefing available through CDSE is taken from DODM 5105.21 - V3. This briefing provides information regarding Foreign Intelligence Services, terrorists/ criminals/mob violence, travel guidance, and reporting requirements.

The CDSE CI Foreign Travel Briefing is offered as a short, or 15-minute eLearning course (CI022.16). Both the methods assist DOD personnel and facility security officers (FSOs) working in cleared defense contractor facilities in developing their own tailored briefs. It contains an outline of





topics that are recommended for inclusion in a CI Foreign Travel Brief. Topics include Vulnerability Awareness, Personal Safety, Terrorist Threats, Assistance Contacts, and **“Before You Go.”**

Whether traveling in the United States or overseas, DOD personnel and cleared contractors should take the time to review available travel security resources to reduce their risk of being targets of FIS or criminal activity. Security professionals should raise awareness through briefings,

posters, and targeted messaging concerning travel risks and security tips to mitigate those risks. They should also inform their personnel about any responsibilities, such as notifying security officials before overseas travel, requirements to receive travel briefings and refresher training, and any reporting requirements after travel. The resources provided by CDSE, NCSC, and the U.S. State Department will help security professionals prepare their workforces and individuals prepare themselves to have safer and more secure travel experiences.

CDSE AND DOD TRAVEL SECURITY RESOURCES

[Defensive Security Briefing](#)

[CI Foreign Travel Briefing Course](#)

[Travel Reporting Poster](#)

[Know the Risks Poster](#)

[Packing Poster](#)

[Travel Poster](#)

[Counterintelligence Awareness Toolkit](#) (Foreign Travel and Visits Tab)

NCSC TRAVEL RESOURCES

[Travel Awareness Video](#)

[Human Targeting Video](#)

[Human Targeting and Travel Awareness Posters](#) | [Poster 2](#) | [Poster 3](#)

[Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position](#)

[Smart Traveler Enrollment Program \(STEP\)](#)

[Traveler’s Checklist Card](#)

[Travel Advisories](#)

[U.S. Embassy / Consulate Locator](#)

[Emergency Contact Information from the U.S. & Canada](#) (1-888-407-4747 | From Overseas - +1 202-501-4444)

[Emergencies](#)

[Lodging Safety](#)



CDSE SPRING 2025 EDUCATION COURSES

Expand your knowledge with CDSE! Registration is now open for CDSE Education classes for the 2025 spring semester. The 16-week semester runs from January 20, 2025 to May 18, 2025. The courses are asynchronous, online, tuition-free, and allow students the flexibility to collaborate with each other and instructors. Are you in need of professional development units (PDUs)? Students can earn 160 PDUs by completing these classes. CDSE Education Division also offers two 8-week courses: ED401.10, The Defense Security Enterprise: A National Security Enabler and ED203.10, Writing Incident Reports and Research Papers for DOD Security.

Enrollment fills quickly, so register early to secure a spot. [Learn more](#) and register via [STEPP](#).

Questions? Contact the [CDSE Education Division](#).



INSIDER THREAT DETECTION AND ANALYSIS COURSE

Insider threats are one of the biggest risks to national security. Learn the latest analytic techniques with CDSE's virtual instructor-led "Insider Threat Detection Analysis Course" (ITDAC) training. During this five-day course, attendees will apply critical thinking skills and applicable structured analytic techniques to potential insider threat indicators.

This course also allows learners to obtain and use holistic data in conjunction with the application of critical pathway theory. Some prerequisites apply. Register for courses [here](#). Below is the 2024 and 2025 course schedule:

Dec. 2-6, 2024 (Virtual)	May 12-16, 2025 (Virtual)
Jan. 13-17, 2025 (Virtual)	June 23-27, 2025 (Virtual)
Feb. 10-14, 2025 (Virtual)	July 21-25, 2025 (Virtual)
March 17-21, 2025 (Virtual)	Aug. 18-22, 2025 (Virtual)
April 7-11, 2025 (Virtual)	Sept. 22-26, 2025 (Virtual)



NEW SHORT COURSE SERIES ON LIFE CYCLE OF CONTROLLED UNCLASSIFIED INFORMATION RELEASED

CDSE has published the CUI Life Cycle Shorts series, consisting of four short courses. The shorts provide learners with specific “how-to” guidance, aligning with current policy requirements, on daily tasks that involve CUI. The shorts can help ensure the workforce has clear guidance on how to: create, identify, and designate CUI; safeguard CUI; share CUI, and decontrol and destroy CUI in accordance with DODI 5200.48 “Controlled Unclassified Information (CUI).” Visit CDSE’s Information Security [page](#) to learn more and to access this new training.

PERSONNEL VETTING NEED-TO-KNOW VIDEO

DCSA has released a “Need-to-Know” training video that explains the need-to-know concept as a component of authorized access to classified information. The video describes the responsibilities of security professionals and information holders, in addition to process, safeguarding measures and violations.



ACTIVITY SECURITY MANAGER COURSE

Don’t miss CDSE’s upcoming “Activity Security Manager” course. This mid-level, virtual instructor-led course provides students with a comprehensive understanding of how to apply and implement specific DOD Information Security policies and procedures to mitigate and manage risks associated with developing, managing, and evaluating a DOD Information Security Program (ISP). Students are anticipated to invest 40-60 hours over four weeks in a primarily asynchronous environment. The course is tailored for DOD civilian, military, and contractor personnel with primary duties as an activity security manager, information security program specialist, or manager within a DOD Component ISP. Students should have a functional working knowledge of the DOD ISP.

After taking this course, students can expect to implement the fundamental policies and requirements of the ISP, implement risk management to protect DOD assets, determine fundamental cybersecurity and information technology principles, and more. The first iteration will take place from February 2, 2025, to March 3, 2025. For more dates and information, check out the [CDSE website](#).



FY 2025 UPCOMING COURSES

Consider signing up for one of CDSE's instructor-led training (ILT) or VILT courses! Training is free, and the VILT eliminates travel expenses. Complete CDSE courses to earn PDUs toward maintenance of Security Professional Education Development (SPeD) Program certifications and credentials. Select courses have the American Council on Education (ACE) CREDIT recommendations that may earn transfer credits at participating universities.

Classes fill quickly, so get an early start in planning your security training for FY25. Access the training schedule today to learn more! Below is a list of available ILT/VILT courses.

Cybersecurity

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

- September 22 - 26, 2025 (Linthicum, MD)

General Security

DOD Security Specialist (GS101.01)

- March 4 - 13, 2025 (Linthicum, MD)
- April 8 - 17, 2025 (Linthicum, MD)
- September 9 - 18, 2025 (Linthicum, MD)

DOD Security Specialist VILT (GS101.10)

- November 18 - December 15, 2024 (Virtual)
- January 13 - February 9, 2025 (Virtual)
- May 12 - June 8, 2025 (Virtual)
- August 18 - September 14, 2025 (Virtual)

Industrial Security

Getting Started Seminar for New Facility Security Officers (FSOs) (IS121.01)

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

- January 14 - 17, 2025 (Virtual)
- April 8 - 11, 2025 (Virtual)
- August 5 - 8, 2025 (Virtual)

Information Security

Activity Security Manager VILT (IF203.10)

- February 2 - March 3, 2025 (Virtual)
- April 21 - May 18, 2025 (Virtual)
- July 28 - August 24, 2025 (Virtual)



Insider Threat

Insider Threat Detection Analysis VILT (INT200.10)

- January 13 - 17, 2025 (Virtual)
- February 10 - 14, 2025 (Virtual)
- March 17 - 21, 2025 (Virtual)
- April 7 - 11, 2025 (Virtual)
- May 12 - 16, 2025 (Virtual)
- June 23 - 27, 2025 (Virtual)
- July 21 - 25, 2025 (Virtual)
- August 18 - 22, 2025 (Virtual)
- September 22 - 26, 2025 (Virtual)

Personnel Security

Advanced National Security Adjudication VILT (PS301.10)

- December 9 - 19, 2024 (Virtual)
- March 3 - 13, 2025 (Virtual)
- June 2 - 12, 2025 (Virtual)
- September 8 - 18, 2025 (Virtual)

Fundamentals of National Security Adjudications (PS101.01)

Fundamentals of National Security Adjudications VILT (PS101.10)

- January 13 - 23, 2025 (Virtual)

(Continued on next page)



(Continued from previous page)

Personnel Vetting Seminar VILT (PS200.10)

- February 4 - 5, 2025 (Virtual)
- May 6 - 7, 2025 (Virtual)
- August 5 - 6, 2025 (Virtual)

Physical Security

Physical Security and Asset Protection (PY201.01)

- April 21 - 25, 2025 (Linthicum, MD)
- August 18 - 22, 2025 (Linthicum, MD)

Physical Security and Asset Protection VILT (PY201.10)

- March 10 - 28, 2025 (Virtual)

Special Access Programs

Introduction to Special Access Programs (SA101.01)

- March 4 - 7, 2025 (China Lake, CA)
- March 11 - 14, 2025 (Sunnyvale, CA)
- April 22 - 25, 2025 (Linthicum, MD)
- May 13 - 16, 2025 (Linthicum, MD)
- August 5 - 8, 2025 (Lexington, MA) (MIT)
- September 9 - 12, 2025 (Rolling Meadows, IL) (NGC)

Introduction to Special Access Programs VILT (SA101.10)

- December 2 - 10, 2024 (Virtual)
- June 2 - 10, 2025 (Virtual)

Orientation to SAP Security Compliance Inspections (SA210.0)

- February 19 - 20, 2025 (Linthicum, MD)
- August 11 - 12, 2025 (Lexington, MA)



SAP Mid-Level Security Management (SA201.01)

January 13 - 17, 2025 (Linthicum, MD)
July 14 - 18, 2025 (Linthicum, MD)

SAP Mid-Level Security Management VILT (SA201.10)

CDSE courses are intended for use by Department of Defense and other U.S. Government personnel and contractors within the National Industrial Security Program.

SECURITY ACADEMY "FEDERAL INVESTIGATOR TRAINING PROGRAM"

From October 18 to December 18, the Background Investigator Training team at the Security Academy is delivering the hybrid "Federal Background Investigator Training Program" instructor-led training to 22 DCSA Special Agents.

INVESTIGATOR FIELD VILT

The Security Academy is delivering the "Investigator Field" VILT from October 28 to December 27. The Background Investigations (BI) Training's Field Investigative Training Team is delivering a VILT to include four live, virtual training sessions and some 230 hours of additional structured on-the-job training preparing 36 BI Field Agents from across the country in a successful transition from a learning environment to live, independent casework.



CDSE NEW CASE STUDIES

On November 4, CDSE's Insider Threat team released **two new case studies** on Bryce Steven Pedicini and Jason M. Hines.

Pedicini, 27, was charged in May 2023 with attempted espionage and violation of a lawful general order. As a former U.S. Navy chief petty officer fire controlman previously assigned to the USS Higgins (DDG 76), Pedicini wrongly transported classified information while stationed at Yokosuka Naval Base, Japan. He was contacted by and shared national defense and classified information with an unknown representative from a foreign government, whom he engaged with under the guise of writing research papers. The foreign agent offered Pedicini money in exchange for writing the papers and providing classified information, increasing the payout based on the value and sensitivity of the information.

According to court records, Pedicini sent multiple documents from November 2022 to May 2023 and was sentenced to 18 years in military prison. The judge also reduced his rank to E-1 and issued a dishonorable discharge.

Hines, 44, was charged with fraud in July 2024, sentenced to 18 months in prison, with an additional 18 months of home confinement, and was ordered to forfeit \$2 million. Hines also agreed to pay restitution for \$5 million. Hines operated Direct Business Services International (DBSI), a New Jersey-based communications company, which services an array of international and domestic resellers and end users with business communications equipment and software licenses. DBSI was an authorized partner with Avaya Direct International (ADI) and would purchase a surplus of license keys to resell on the open market.

Hines conspired with ADI to sell pirated ADI software licenses for proprietary telephone equipment manufactured by Avaya. Hines' co-conspirator, Brad Pearce, was a long-time employee of Avaya. He secretly used his system administrator privileges to generate tens of thousands of unauthorized license keys that he sold to Hines. In turn, Hines would sell them to his global network of resellers and end users. Ultimately, Hines and Pearce sold tens of thousands of pirated business telephone system software licenses, valued at over \$88 million.



CDSE NEWS

CDSE offers an email subscriber news service to get the latest CDSE news, updates, and information. You may be receiving the Pulse through your subscription, but if you were forwarded this newsletter from another source and would like to subscribe to the Pulse, Insider Threat Bulletins, or the Weekly Flash, visit our [news page](#) and sign up or update your account today.

