CDSE
LEARN. PERFORM. PROTECT.
PULSE
VOLUME 6 ISSUE 4 | APRIL 2025

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

DCSA Leadership
David M. Cattler, *Director, DCSA*
Daniel J. Lecce, *Deputy Director, DCSA*
Kevin Jones, *Assistant Director, Security Training*
Erika Ragonese, *Deputy Assistant Director, Security Training*

CDSE Leadership
Audrey Gutierrez, *Director*
Glenn Stegall, *Deputy Director*

Pulse Staff
Cashmere He, *Chief Content Officer*
Isaiah Burwell, *Content Writer*
Matthew Wright, 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

THIS MONTH'S FOCUS

Grand Theft Cargo: Analyzing the Supply Chain's Top Threat

By Isaiah Burwell

April is National Supply Chain Integrity Month, a time to educate ourselves on the current threats to the mechanisms that deliver our Nation's goods. Cargo theft, which accounts for billions of dollars in losses every year, was the theme of a recent supply chain-related congressional subcommittee hearing. While laws take time to pass, CDSE already offers numerous resources for security professionals to keep themselves and their organizations up-to date on supply chain security.

On February 27, U.S. Senator Todd Young (R-Ind.), Chairman of the Subcommittee on Surface Transportation, Freight, Pipelines, and Safety, convened a subcommittee hearing titled, "Grand Theft Cargo: Examining a Costly Threat to Consumers to the U.S. Supply Chain."

The hearing focused on the rise in cargo theft, specifically on crimes within the supply chain like brokering scams, fraudulent trucking companies, and train robberies by highly organized gangs. The hearing examined potential solutions, including increased coordination and enforcement by Federal agencies like the Federal Motor Carrier Safety Administration (FMCSA) and the Department of Homeland Security (DHS) to stop these criminal enterprises.

Since the COVID pandemic, cargo theft has surged to new heights across the country. Once carried out mainly by crude criminals, the rise of e-commerce has expanded this crime domain to include sophisticated domestic and international groups from China, Eastern Europe, and Mexico.

Young said cargo theft is difficult to spot and stop because it takes so many forms. Homeland Security Investigations estimates that the loss of cargo theft "accounts for $15-35 billion annually."

The chairman garnered bipartisan support for his agenda. "I don't believe

that these issues — law enforcement or addressing cargo theft — should be partisan in any way. Crimes in our freight supply chain can harm consumers, small businesses, transportation workers and our economy," said Sen. Gary Peters (D-Mich.), the subcommittee's ranking member.

Freight industry stakeholders attending the hearing endorsed several bills designed to protect the freight workforce and improve the flow of freight. One measure is the Household Goods Shipping Consumer Protection Act, which would boost certain guidelines at the FMCSA to help reassure individuals about consumer protections. Congress would use its resources to protect the supply chain with bills, but CDSE has already used its resources to protect the supply chain through education products.

CDSE's **Supply Chain Threat Awareness course** encompasses and defines Supply Chain and Supply Chain Risk Management (SCRM). Students will learn what potential threats are posed by Foreign Intelligence Entities (FIE), criminals, and strategic competitors, as well as various risk mitigation strategies/ countermeasures. CDSE's **Counterintelligence Awareness Toolkit** also contains a section on SCRM. This section features more CDSE-created content, such as job aids, eLearning courses, and webinars. The section also provides links to supply chain policy documents, as well as documents highlighting threat awareness and best practices.

Cargo shipping is the most tactile aspect of our supply chain. Our modern technological advancements will not mean much if we cannot safely transport items across the country. CDSE's SCRM products are great ways for the average security professional to keep up to date on the threats and needs of the supply chain so that we may protect it together.

CDSE Supply Chain Integrity Resources

Supply Chain Threat Awareness course

Counterintelligence Awareness Toolkit

Software Supply Chain Attacks Job Aid

Deliver Uncompromised Toolkit

CISA and NCSC Supply Chain Integrity Resources

NCSC Supply Chain Threats

NCSC Supply Chain Risk Management for Industry & Academia

CISA Supply Chain Risk Management Essentials

CISA Information and Communications Technology Supply Chain Security

2025 Virtual DCSA Security Conference for Industry

The virtual DCSA Security Conference for Industry will take place on April 23-24 from 10:00 am to 4:30 pm. This unclassified event will focus on the theme "The Power of Partnership: Trust in People, Facilities, Systems, and Data." The conference will be held virtually via Adobe Connect and is geared to a maximum of 3,000 industry security professional, Facility Security Officers (FSO), Assistant FSOs, Directors of Security, Insider Threat Program Senior Officials, Information System Security Managers, Senior Management officials, and mission support personnel.

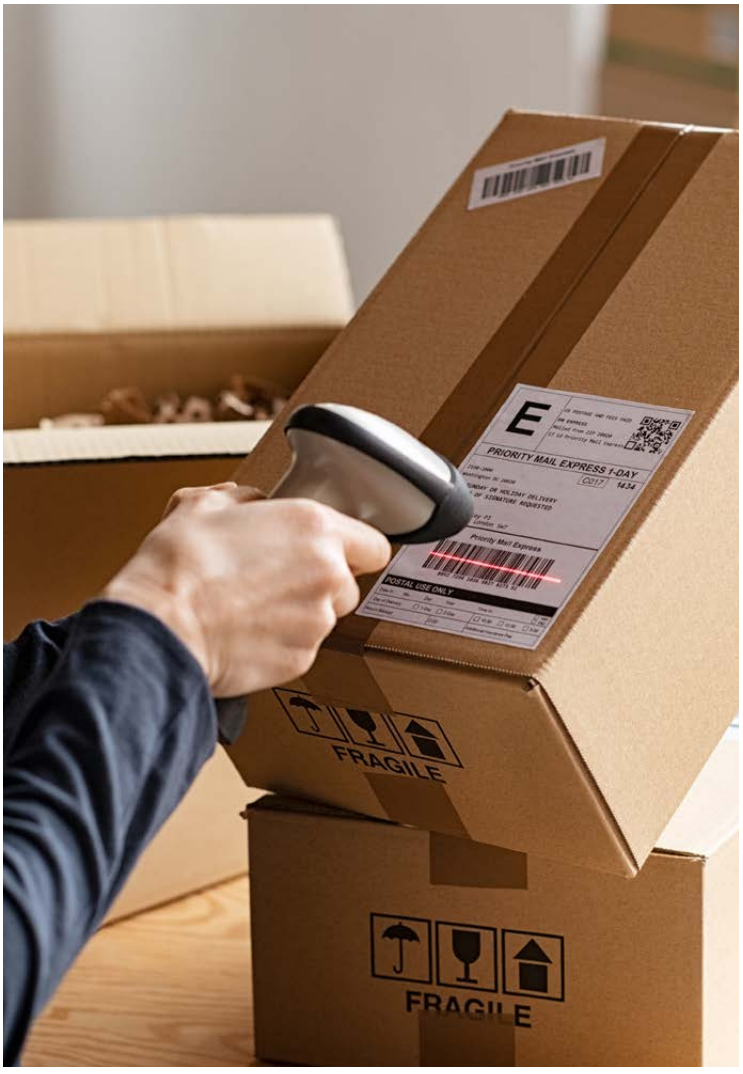
This two-day conference will cover a variety of session topics and panel moderated discussions. **Register** to secure your conference spot.

COUNTERINTELLIGENCE, CYBERSECURITY, INSIDER THREAT

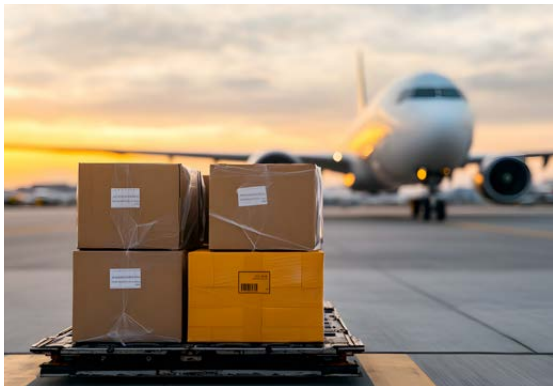
Insider Threat to Supply Chains Job Aid

Supply chain security is a critical component of any organization that focuses on risk management of external suppliers, vendors, logistics, and transportation. It involves ensuring products are not tampered with or not stolen during the production, storage, transportation, or delivery processes. What some organizations overlook are vulnerabilities of risks during this process. Insider threat risks can be intentional but may not always be malicious. For example, an insider threat risk may be caused by an employee unintentionally exposing information or disregarding protocols.

Organizations can be proactive in identifying and mitigating supply chain insider risks. The **Insider Threat to Supply Chains Job Aid** provides common examples of insider threats in supply chains, mitigation steps to identify potential risks, and best practices for preventing insider threat incidents. The job aid is also in the **Insider Threat Toolkit** under the Cyber Insider Threat/User Activity Monitoring category. The toolkit offers a variety of information on topics within the Insider Threat landscape including information in areas such as training, awareness, vigilance, research, fraud, and reporting, to name a few. Security professionals can use the toolkit resources to perform their role in the Insider Threat field.



Supply Chain Awareness Month



April is Supply Chain Awareness Month and the CDSE Counterintelligence (CI) Team has added a new Supply Chain Awareness product, a CI short titled, "Supply Chain and Counterintelligence Due Diligence," which is available on the CI Toolkit. This is an overview product that highlights the importance of CI due diligence in the acquisition and supply chain process.

Other CI Supply Chain Awareness products include job aids, posters, and webinars are available in the CI toolkit.

Insider Threat Detection and Analysis Course

Want to sharpen your skills by identifying insider threat indicators? Secure your spot now for the next open session on April 21-25, 2025.

This 5-day course enables attendees to apply critical thinking skills and applicable structured analytic techniques to potential insider threat indicators. Participants will work with CDSE experts to obtain and use holistic data with the application of critical pathway theory. Additionally, learners will be taught how to apply Executive Orders, DOD, and Intelligence Community (IC) authorities in data gathering, receive instruction on constitutional and privacy rights, and will learn the processes for conducting and reporting response actions from intake of an initial potential threat to mitigation of the threat.

Prerequisites for the ITDAC have been updated to make the course more accessible. Effective immediately, candidates are no longer required to complete the Insider Threat Program Operations Personnel Curriculum INT311.CU or the Insider Threat Program Management Personnel Curriculum INT312.CU. Instead, there are five eLearning courses, which require 75 percent less time to complete than the previous prerequisites.

The 2025 course schedule is as follows:

May 12-16, 2025 (Virtual)
June 23-27, 2025 (Virtual)
July 21-25, 2025 (Virtual)
Aug. 18-22, 2025 (Virtual)
Sept. 22-26, 2025 (Virtual)

Register for the ITDAC course and view the full list of prerequisites.

INDUSTRIAL SECURITY

Registration is Now Open for the Getting Started Seminar for FSOs at the NCMS Annual Training Seminar

CDSE will be hosting the Getting Started Seminar (GSS) for Facility Security Officers (FSOs) at the NCMS Annual Training Seminar on June 9, 2025! This course is not only a great way to get started as a new FSO, but also a way for experienced FSOs to keep informed on industrial security guidance and emerging trends. Students will work in collaboration with other security professionals, exploring security topics through practical exercises. Topics include the DD 254, insider threat, reporting requirements, counterintelligence, security and contractor reviews, security training and briefings, and personnel security.

Please **pre-register** and complete the pre-requisites. Registration closes on May 16, 2025, and only registered participants will be allowed to attend. Proof of registration (emailed by CDSE) and a photo ID will be required for class entry. You must be registered for the NCMS Annual Training Seminar to attend this GSS. *Please note that walk-ins will not be allowed*. GSS fills up fast, so register today!

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

The Getting Started Seminar for New Facility Security Officers (FSOs) is a virtual-led training course that allows new FSOs and security personnel the opportunity to learn and apply fundamental National Industrial Security Program (NISP) requirements in a collaborative environment. If you are an FSO, contractor security personnel, DOD Industrial Security Specialist, or anyone else working in the security environment, register to attend one of our upcoming iterations:

April 8-11, 2025
August 5-8, 2025

EDUCATION

New CDSE Education Division Courses

In 2024, the Center for Development of Security Excellence (CDSE) Education Division developed two new 8-week virtual instructor-led education courses for security professionals, *ED402.10 The Security Triangle: Security, Law Enforcement, and Intelligence* and *ED401.10 The Defense Security Enterprise: A National Security Enabler.*

The *ED402.10* course, first successfully offered in the Fall 2024 semester, focuses on the three components of the security triangle (security, law enforcement (LE), and intelligence). Through the analytical review of three case studies, the Washington Navy Yard Shooting (2013), the Khobar Towers Bombing (1996), and the Fort Hood Shooting (2009), students explore how DOD security professionals collaborate with and support the LE and intelligence communities to prevent future security failures.

The *ED401.10* course, offered in the Spring 2025 semester, provides security professionals with a foundational understanding of the core security principles and the role of security as a mission enabler in achieving the broader goals of the DOD. The course treats Security Management as a doctrine and discusses examples of how security successes and failures have historically bolstered and undermined the DOD mission. To enhance student learning and develop collaborative leadership skills, this course innovatively used the Security, Training, Education, and Professionalization Portal (STEPP) Wiki application in the virtual learning classroom to develop a collaborative case study on the Robert Hanssen espionage case.

Both courses are open to all U.S. Government civilian employees and U.S. military service members with or without a college degree. Students will earn Professional Development Units (PDUs) upon completing either of these courses, which can be used to maintain their Security Professional Education Development (SPēD) certification. To learn more about these courses and other CDSE Education courses, click **here**.

PERSONNEL VETTING

Personnel Security: Fundamentals of National Security Adjudications VILT PS101.10

In this 7-day virtual instructor-led course held from July 22-30, learners will evaluate information obtained through an investigation package, identifying any potential issues in the information for mitigation and resolution. Learners will also identify potential security concerns and risks based upon the application of the national security adjudicative guidelines. Through case review, learners will determine eligibility based upon practical application of adjudicative methodology for final national security adjudicative determinations.

The course teaches students how to identify security concerns by utilizing National Security Adjudicative Guidelines to make a personnel security determination. Students will be introduced to the whole person concept, different types of background investigations, designated sensitive positions, and personnel security policies and regulations. In addition, students will also learn how to evaluate a portion of a person's life to reasonably determine whether his/her future behavior will be consistent with national security.

This course is intended for DOD and Federal civilians (GS/GG 5-7 level) who adjudicate eligibility for assignment to sensitive positions and/or access to collateral and Sensitive Compartmented Information (SCI) program information or DOD/DOD Intelligence Community (IC) Government Civilian/Military personnel (non-adjudicators) who perform duties to support national security adjudications. Nominations for attendance must be approved and made through training coordinator or designee. Check cdse.edu for more information on dates and location.

Requirements:

- Clearance Requirements: N/A
- Attendance Requirement: Full-time attendance and participation in all sessions.
- Exam Requirements: Students must earn 162 points out of 215, a 75 percent grade average, on course exams and performance exercises.

Credits Recommended/Earned:

- ACE Credit Recommendation: (**What's this?**): three semester hours, upper division baccalaureate degree category.
- Professional Development Units (PDUs) per SPēD: PDUs are determined by length of course and IAW with current Certification Maintenance Guidelines.

SPECIAL ACCESS PROGRAMS

Introduction to Special Access Programs (SAPs)

CDSE will offer the Intro to SAPs Course May 13-16 in Linthicum, MD. This course addresses the basic requirements to implement security for a DOD SAP. This course will cover DoDM 5205.07, DoDI 5205.11, and DoDM 5205.07 vols 1-4, as well as how to perform duties as a SAP security professional. This course will focus on providing entry level SAP security professionals the tools needed to implement DOD policies in their programs. The course covers security enhancements such as the SAP Nomination process, SAP facility construction requirements, Risk Management Framework, and other security enhancements as outlined in the DOD policy.

This 3-and-a-half-day course targets new U.S. Government SAP security professionals to include civilian, contractor, military, as well as those in other Federal agencies that work with DOD SAPs. Visit the **course page** to learn more and register.

Orientation to Special Access Program (SAP) Security Compliance Course

CDSE will offer an Orientation to SAP Security Compliance course May 19-20 in Linthicum, MD. This course addresses the processes and procedures for conducting compliance inspections for DOD SAPs. This course will cover the DoDM 5205.07 vols. 1-4 and provide students with an opportunity to provide ratings in a mock team inspection.

The 2-day course targets SAP security professionals with an understanding of fundamental SAP security practices and a firm grasp of the DoDM 5205.07 vols. 1-4 to apply this knowledge during the mock inspection portion of the course. Visit the **course page** to learn more and register.

FY25 COURSES

UPCOMING FY25 COURSES

Interested in earning professional development units (PDUs) toward maintenance of Security Professional Education Development (SPēD) Program certifications and credentials? CDSE's instructor-led training (ILT) or virtual instructor-led training (VILT) courses are the perfect opportunities for you to receive free training online. Select courses even have the American Council on Education (ACE) CREDIT recommendations that can earn you transfer credits at participating universities.

Classes fill quickly, so start planning now for your FY25 security training. 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)

INDUSTRIAL SECURITY
Getting Started Seminar for New Facility Security Officers (FSOs) VILT (IS121.10)
- August 5 - 8, 2025 (Virtual)

INFORMATION SECURITY
Activity Security Manager VILT (IF203.10)
- April 21 - May 18, 2025 (Virtual)
- July 28 - August 24, 2025 (Virtual)

INSIDER THREAT
Insider Threat Detection Analysis VILT (INT200.10)
- 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
Personnel Vetting Seminar VILT (PS200.10)
- 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)

SPECIAL ACCESS PROGRAMS
Introduction to Special Access Programs (SA101.01)
- 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)
- June 2 - 10, 2025 (Virtual)

Orientation to SAP Security Compliance Inspections (SA210.0)
- August 11 - 12, 2025 (Lexington, MA)

SAP Mid-Level Security Management (SA201.01)
- July 14 - 18, 2025 (Linthicum, MD)

STAFF SPOTLIGHT

Meet Douglas Whitman: Cybersecurity Curriculum Manager

Douglas Whitman

Douglas Whitman is the new Cybersecurity Curriculum Manager for the Center for Development of Security Excellence (CDSE) part of the Security Training Directorate within the Defense Counterintelligence and Security Agency (DCSA). He is responsible for the development and management of the Cybersecurity curriculum, toolkits, job aids, as well as the DOD Cybersecurity Awareness Training. Whitman has 11 years of experience in the educational field, first as a teacher, then later serving as a school administrator. He later pivoted to Cybersecurity to work as a Chief Information Security Officer for a community college before joining DCSA. Whitman's educational achievements include an undergraduate degree in Secondary Education, as well as two graduate degrees in Educational Leadership and Information Assurance & Cybersecurity.

The Cybersecurity Team has undergone a transformation over the past several months, welcoming an entirely new team dedicated to supporting the CDSE, DCSA, and DOD Cybersecurity training mission, as well as industry partners and stakeholders. This transition marks an exciting opportunity for fresh perspectives, innovation, and new collaboration opportunities. This new team is committed to building up on past and existing efforts to provide high- quality instruction and educational products. The Cybersecurity Team is currently reviewing existing products and training to ensure they meet the needs of our audiences, revising existing products, and identifying stakeholder training needs.

The Cybersecurity products consist of 102 products between two curricula, e-learnings, job-aids, toolkits, games, and more. The Cybersecurity team's top priority is development of their Instructor Led Training (ILT), Assessing Risk and Applying Security Controls to NISP Systems (CS301.01), for a September 2025 launch date. The team will develop many products to support the DOD mission between now and then, so stay tuned!

CDSE & DCSA NEWS

Safeguarding Trust Video

To defend national security, trust is at the forefront of everything DCSA and CDSE do to combat insider and foreign threats.

Working alongside industry partners, we inspect, control, and monitor access to classified information. We protect national security with investigators who vet military, civilian, government, and private sector personnel and safeguard against foreign and insider threats. Our training initiatives keep us informed and ahead of evolving threats. "**Safeguarding tomorrow, today**," video. Watch the video to learn more about

how DCSA is at the forefront of safeguarding trust in our federal workforce, in workspaces, and in classified IT systems and data.

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, DC 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

Education 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