THIS MONTH'S FOCUS

CDSE Contributes to Annual NITAM Campaign

By Isaiah Burwell

An insider threat may use authorized access, wittingly or unwittingly, to do harm to the security of the United States. Threats can result in damage through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities. **National Insider Threat Awareness Month (NITAM)** is an annual, month-long campaign during September that brings together thousands of security professionals and policy makers to educate government and industry about the risks posed by insider threats and the role of insider threat programs. Each year, the Under Secretary of Defense for Intelligence & Security (USD(I&S)), the National Insider Threat Task Force, and the Defense Counterintelligence and Security Agency (DCSA) partner with other stakeholder organizations to build off previous successes and expand the impact and audience of the NITAM campaign. CDSE assists with this expansion through developing and marketing insider threat training resources.

CDSE offers four insider threat training products, covering everything from the basics of insider threat indicators and reporting processes to developing and managing insider threat programs. New insider threat professionals may find it beneficial to take the courses in the order outlined below due to the content progression building upon foundational knowledge. **Insider Threat Awareness INT101.16**, provides a thorough understanding of how insider threat awareness is an essential component of a comprehensive security program. The course covers

common insider risk indicators and promotes reporting concerning behaviors. Next, the **Insider Threat Program Operations Personnel Curriculum INT311. CU** course provides specialized training for analysts and other operations personnel working in insider threat programs within DOD components, federal agencies, and industry. An alternative second course, **Insider Threat Program Management Personnel Curriculum INT312.CU**, provides specialized training for personnel managing insider threat programs. The final course, **Establishing an Insider Threat Program for Your Organization INT122.16**, is designed for individuals designated as the organizational insider threat program manager.

CDSE also assembled an **insider threat toolkit** which contains an extensive list of eLearning, webinars, shorts, and other resources. The toolkit provides a link to the **case study library**, a repository that highlights individuals charged with crimes having an adverse impact on national security. Case studies are two-page summaries of insiders who become insider threats, the crimes they committed, and how they were brought to justice.

The NITAM website is updated every September with the latest news and highlights on insider threat products. It contains a section for the insider threat-related events, such as workshops and conferences.

There are numerous ways to make a difference in insider threat awareness. The NITAM website recommends promoting awareness, establishing a hub, training the workforce, and recognizing indicators and reporting, as ways to counter insider threats. With CDSE's contributions, NITAM will continue to expand its reach and better educate security professionals.

NATIONAL INSIDER THREAT AWARENESS MONTH

7th Annual NITAM

This September marks the seventh annual NITAM, as well as an opportunity to elevate the overall security posture, strengthen insider threat programs, and ensure a trusted workforce.

For ideas on how to participate in the month-long campaign, check out the newly launched **NITAM site** - updated for 2025 with FAQs, events and helpful resources. Resources include games, case studies and items such as **Human Resources & Insider Threat short**, and **DITMAC DOD Insider Threat Reporting Portal**.

This year's theme, "Partnering for Progress" highlights the power of collaboration. By actively promoting teamwork and sharing information among different departments and with external partners, organizations can significantly enhance their ability to detect, prevent, and respond to insider threats, ultimately creating a more secure and resilient environment.

COUNTERINTELLIGENCE

The Intersection of Fraud and Counterintelligence

Tom Gentle, the CDSE counterintelligence curriculum manager, is also a Certified Fraud Examiner (CFE) by the **Association of Certified Fraud Examiners** (ACFE). He uses his knowledge, experience, and network to develop fraud-related content for CDSE.

In 2002, Gentle served as a counterintelligence special agent, conducting and overseeing counterespionage and counterterrorism investigations involving financial analysis. After transitioning to the private sector, he oversaw a team of analysts who conducted financial analyses in support of investigations and operations. In 2015, he pursued CFE certification. As an active member of the ACFE and CI curriculum manager, Gentle incorporates information from ACFE's extensive network into CDSE training and resources.

The CDSE **Counterintelligence Awareness toolkit** includes the "Counterintelligence and Fraud Concerns" course, a poster, and a case study. The products address foreign intelligence entities and adversaries using illicit fraud activities to acquire access to personnel, information, systems, and facilities. These same threat actors also attempt to secure funding to conduct illicit activities.

CDSE collaborates with the CI Partnership Branch, CI and Insider Threat Directorate, DCSA to deliver fraud and CI related webinars. On Sept. 22, DCSA will host a "**Shadow Banking and Financial Fraud: Exploring North Korea's Fraud and Sanctions Evasion Schemes**" webinar. The webinar will provide an overview of North Korea's development of a mass-scale fraud triangle, creating a patchwork of need,
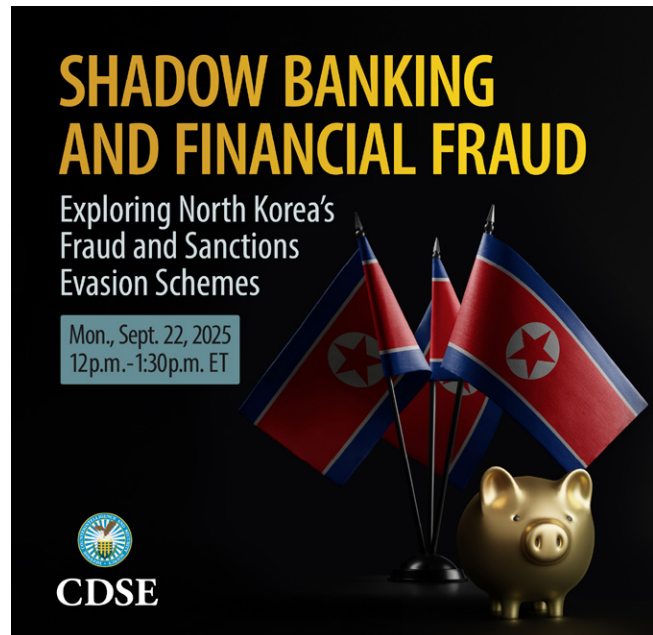
opportunity, and rationalization that drives illicit activity. The regime relies on a network of domestic and overseas operatives to obtain financing, evade sanctions, and move money throughout the global financial system. The webinar will provide real-world examples of fraud, money laundering, and conspiracies that help enrich the regime, as well as red flags and risk indicators across business sectors.

Gentle's ACFE network, combined with his passion for educating security professionals on fraud indicators, are instrumental in developing CDSE curriculum and furthering CI awareness.

PERSONNEL VETTING

Overview of Federal Personnel Vetting e-Learning Course

If you hold the APC or DP/APC, or perform or support National Security, Suitability, or HSPD-12 Credentialing adjudications, please check out "**Overview of Federal Personnel Vetting**" e-Learning.

This course provides training which aligns with Trusted Workforce (TW) 2.0 transformational changes to the Security, Suitability, and Credentialing (SSC) enterprise. Registration is restricted to students with a .gov or .mil email address. Taking this course satisfies gap training requirements for those who previously took PS001.18 and PS101.01 or PS101.10 prior to April 2025.

New Personnel Vetting (PV) Job Aids

Personnel Vetting released four new job aids:

- **Financial Considerations: Military Resources**. **The Financial Considerations job aid** summarizes the requirement for financial readiness training for the military. The program assists in resolving financial distress before it becomes a security concern as identified in the financial consideration guideline listed in SEAD 4. The job aid outlines Command and Leadership responsibilities, effective options, and lists available resources including non-profit debt management programs, federally approved counseling agencies, as well as DOD and military financial readiness programs.

- **PV Scenarios: Continuous Vetting**. Continuous Vetting (CV) is one of the five personnel vetting scenarios and is a near real-time review of a covered individual's background. This **trifold job aid** answers your questions about CV including how CV works, the benefits of CV, and who is subject to CV.

- **PV Scenarios: Upgrades, Transfer of Trust, and Re-Establishment of Trust**. This **trifold job aid** provides a description of three of five vetting scenarios along with the common requirements and outcomes of each. These vetting scenarios apply to current and former trusted insiders and include upgrades, transfer of trust (ToT), and re-establishment of trust (RoT).

- **National Security Adjudication**. National Security Adjudication is an examination of an individual's life to determine if that individual is an acceptable security risk and to make a trust determination. This **job aid** provides an overview of the national security adjudicative process; defining whole person concept, identifying the 13 national security adjudicative guidelines, and the adjudicative factors used in evaluating the relevance of an individual's conduct.

Click **here** to download, print, and distribute these new job aids to your security workforce today!

INSIDER THREAT

Insider Threat Detection and Analysis Course

Are you looking to enhance your skills in identifying and mitigating potential insider threats? Secure your spot now for the upcoming virtual session on Sept. 22-26, 2025.

This 5-day course provides students with the skills to apply critical thinking and structured analytic techniques to potential insider threat indicators, in alignment with National Insider Threat Task Force standards. Students will leverage holistic data and critical pathway theory, understand and apply relevant Executive Orders, DOD, and Intelligence Community (IC) authorities, and ensure constitutional and privacy rights are protected during data collection. Additionally, participants will master the end-to-end process of responding to potential threats, from initial intake to mitigation, including mandated reporting requirements.

Prerequisites have been updated to enhance accessibility. 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). The new prerequisite requirement is the completion of five eLearning courses which require 75 percent less time than the previous prerequisites.

Course and registration information can be found **here**.

September 2025 CDSE Monthly Vigilance Campaign

September's vigilance campaign focuses on NITAM and includes an **Insider Threat Fact Finding short**. This security short provides information on recognizing potential risks, reporting potential risks or unusual activity or actions from coworkers to insider threat program officials, and more!

Available Now: Human Resources and Insider Threat Short

This all new **Human Resources and Insider Threat short** replaces the previous short of the same name providing an overview of the role human resources (HR) personnel play on an insider threat hub team and the importance in mitigating insider threats. The short provides insight into the HR pillar during an insider threat investigation and provides foundational knowledge relevant to insider threat hub activities.

Structured as an interview with an experienced HR expert from an active insider threat team, the short allows learners to choose questions and obtain real-world explanations and answers.

Coming Soon: Supervisor and Command Leader Awareness of Insider Risk (INT215)

A new course titled "Supervisor and Command Leader Awareness of Insider Threat Risk" is under development to be released soon. The course will provide realistic scenarios and examples of insider threat behavior and how organizational culture, proactive engagement, and leadership actions play a role in risk mitigation. The course will be posted to **cdse.edu** once available.

PHYSICAL SECURITY

Enhance Your Security Expertise: New Intro to Physical Security Training (PY011.16)

Coming this fall, enhance your security expertise with the "Introduction to Physical Security (PY011.16)" E-learning course. The course will provide the tools and knowledge you need to learn how to apply security in-depth principles and contribute to a stronger security posture. This eLearning course can be taken at any time, and is geared to DOD civilians, military personnel, and defense contractors, covers physical security planning, implementation, and countermeasures to deter, delay, detect, deny, and defend against attacks.

FY 2025 UPCOMING COURSES

Registration Now Open

CDSE courses are a great way to gain security knowledge, awareness and expand skill sets. Secure your spot now as classes fill quickly! Available Instructor-Led Training (ITL) and Virtual Instructor-Led Training (VILT) courses are listed below.

Cybersecurity
Assessing Risk and Applying Security Controls to NISP Systems (CS301.01)
  • September 22 - 26, 2025 (Linthicum, Md.)

Insider Threat
Insider Threat Detection Analysis VILT (INT200.10)
  • September 22 - 26, 2025 (Virtual)

Meet Joshua Huettner, Insider Threat Instructor

By Tammi Bush

Joshua Huettner is a seasoned cybersecurity and intelligence leader with over 22 years of experience in cyber operations, intelligence planning, and risk mitigation across government and defense sectors. He currently serves as an insider threat instructor at the Center for Development of Security Excellence (CDSE), where he has been for a year and a half. In this role, he combines deep operational insight with a strong passion for education, developing and delivering advanced training programs that strengthen insider threat awareness and support the security readiness of the Department of Defense (DOD) and its mission partners.

Through his instructional work, Huettner directly supports CDSE's mission to advance the security posture of the DOD and Federal workforce by equipping personnel with the knowledge and tools needed to prevent, detect, and mitigate insider threats. His training products help build a culture of vigilance across diverse agencies, ensuring that security professionals are prepared to address evolving risks in real time.

"Teaching is where I find the greatest purpose — transforming complex threats into clear, actionable knowledge that empowers our workforce to stay one step ahead," Huettner said. He takes pride in creating engaging, mission-aligned content that reinforces the principles of proactive security and national defense.

Throughout his career, Huettner has held critical roles with the FBI, U.S. Navy, and various defense organizations, leading efforts in counterintelligence, cyber threat analysis, and cybersecurity policy. His operational background informs his instruction, bridging strategic concepts with practical application. He has managed multinational cyber planning efforts, led incident response operations, and developed tactics for insider threat detection and cyber defense.

"One of the most rewarding aspects of this work is partnering with such a diverse range of agencies and organizations — all working toward the shared goal of protecting our national security," he adds. This collaborative approach reflects CDSE's broader mission of enabling integrated and resilient security practices across the enterprise.

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

CDSE CONTACT LIST

training, education, and certifications for security professionals across the federal government and industry.

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