



**THIS
MONTH'S
FOCUS**

INSIDER THREAT AWARENESS

DID YOU KNOW?

The total average cost of an insider risk increased in 2023 to \$16.2 million per organization (taking an average of 86 days to identify and contain).

Source: Ponemon 2023 Insider Threat Report, 2023 Cost of Insider Risks Global Report

 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

Glenn Stegall
Acting Director

Pulse Staff

Cashmere He Isaiah Burwell
Chief Content Officer *Content Writer*

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

INSIDER THREAT AWARENESS

In October 2011, the President issued Executive Order (E.O.) 13587 establishing the National Insider Threat Task Force (NITTF), under joint leadership of the Attorney General and the Director of National Intelligence. As part of the E.O., the President directed federal departments and agencies, with classified networks, to establish insider threat detection and prevention programs. The E.O. directs the NITTF to assist agencies in developing and implementing their insider threat programs. In November 2012, following an extensive interagency coordination and vetting process, the President issued the National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs via a Presidential Memorandum.

September was designated as National Insider Threat Awareness Month NITAM in 2019. During NITAM, federal agencies, departments, industry collaborate to emphasize the importance of preparing the workforce to deter, detect, and mitigate threats posed from trusted insiders. Throughout the month, various events and materials are produced, allowing audiences to learn more about threats posed by insiders, insider threat programs, and supporting through reporting.

The theme for this year's NITAM is Deter, Detect, Mitigate. The Defense Personnel and Security Research Center's (PERSEREC) Threat Lab held the fifth annual Insider



Threat Social and Behavioral Sciences Summit (InT SBS Summit) on August 27 and 28 to kick-off NITAM. The Summit focused on Detection, which is about identifying and investigating signs or actions that could signal an insider threat, using a blend of technology, psychology, and procedural checks.

Additionally, the Defense Counterintelligence and Security Agency (DCSA) Conference for Insider Threat was held on September 9 and 10. The conference was hosted by the DOD Insider Threat Management and Analysis Center (DITMAC) and the Department



of Homeland Security Insider Threat Program. Industry security leaders, decision-makers, and experts gathered in Arlington, Virginia to discuss insider threat awareness.

NITAM and the conferences are necessary to help individuals and organizations understand the possible severity of an insider threat. For instance, John Beliveau II was a Naval Criminal Investigative Service (NCIS) supervisory special agent who disclosed sensitive law enforcement reports to a CEO who was the target of a criminal fraud investigation. By providing this sensitive law enforcement information, Beliveau helped the CEO

perpetrate a massive fraud scheme on the U.S. Navy to evade and prevent criminal investigations. Beliveau pleaded guilty on December 17, 2013 to bribery and the conspiracy to commit bribery, and was sentenced to 12 years in prison. He was also ordered to pay \$20 million in restitution to the U.S. Navy. This is just one example of the damage an insider threat can cause.

It is important to deter, detect, and mitigate insider threats so situations like this don't happen again. There is still more work to do, and numerous ways for individuals to contribute to NITAM on both small and large scales.

NATIONAL INSIDER THREAT AWARENESS MONTH 2024

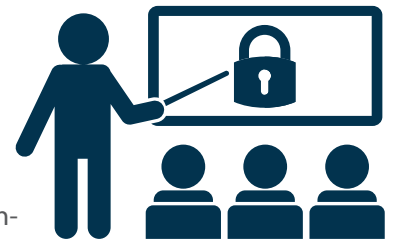
This year's National Insider Threat Awareness Month (NITAM) theme is "Deter, Detect, Mitigate." The DCSA Conference for Insider Threat, which was held on September 9 and 10, was a part of a month-long campaign throughout September that brought together thousands of U.S. security professionals as well as Government and industry policy makers from around the globe to educate on insider threat risks and the critical role of insider threat programs.

This year's [website](#) had a whole new look and was focused on increasing awareness and reporting insider threats across the workforce with job aids, case studies, posters, webinars, videos, games and much more! The conference was a great success with over 367 in-person attendees and 1731 virtual participants. If you missed it and were not able to attend, please be on the lookout for the conference recordings, which will be shared upon completion following the conference.



INSTRUCTOR-LED CYBERSECURITY COURSE AT CDSE IN DECEMBER

CDSE is offering an instructor-led course on Assessing Risk and Applying Security Controls to NISP Systems (CS301.01) in December. This tuition-free course runs



December 2-5 in Linthicum, MD. Students should have completed enrollment (prerequisites and registration) by November 15.

The target audience for this training includes Information System Security Managers (ISSMs), Information System Security Officers, and Facility Security Officers (FSOs) involved in the planning, management, and execution of security programs for cleared industry. This five-day course provides students with guidance on applying policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the risk management framework process.

Go [here](#) to learn more, register, and view the required prerequisites.



INSIDER THREAT FACT FINDING SHORT

The Insider Threat Fact Finding Short is now **live**. The new short is focused on enhancing the understanding of the interconnected, multi-disciplinary approach used by insider threat programs to collect multiple data points from divergent sources and to combine them in ways that regard the “whole person” when detecting and assessing potential risk.



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. Below is the 2024 and 2025 course schedule:

- Oct. 21-25, 2024 (Virtual)
- Nov. 18-22, 2024 (Virtual)
- Dec. 2-6, 2024 (Virtual)
- Jan. 13-17, 2025 (Virtual)
- Feb. 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)
- Aug. 18-22, 2025 (Virtual)
- Sept. 22-26, 2025 (Virtual)

Register for the ITDAC course.

INSIDER THREAT FEATURED JOB AIDS

Check out CDSE’s new job aids! This month features the **Counterintelligence Authorities for Insider Threat Programs Job Aid**.

This job aid outlines the (EO) 13587 – structural reforms to improve the Security of Classified Networks and the responsible sharing and safeguarding of classified information. The EO was established in October 2011 by President Barack Obama to implement an insider threat detection and prevention program consistent with guidance and standards developed by an Insider Threat Task Force.

The job aid also outlines the National Insider Threat Policy Presidential Memorandum 2012, the National Defense Authorization Act (NDAA) of 2018 and DOD policy.

This month’s feature also includes the **Potential Risk Indicators: Foreign Considerations Job Aid**. Foreign associations and interests can pose a risk to national security when they result in divided or conditional U.S. allegiance. Foreign adversaries seek to exploit vulnerabilities within DOD through infiltration, coercion, or recruitment of personnel. Cleared individuals have a responsibility to report any foreign associations to ensure integrity and national security.

Individuals at risk of becoming insider threats, and those who ultimately cause harm, often exhibit warning signs, or potential risk indicators (PRI). A PRI could include a variety of predispositions such as stressors, choices, actions and behaviors to include dual citizenship (past or present), foreign travel patterns, familial ties and more. While these PRI’s can present potential risks to national security, they are not inherently indicative of malicious intent.





INDUSTRIAL SECURITY LAUNCHES NEW ELEARNING COURSE, POSTERS AND WEBINARS

On August 20, the Industrial Security team released the updated eLearning course, **Acquisitions and Contracting Basics**, in the National Industrial Security Program (NISP) IS123.16. This course provides students with a high-level overview of acquisitions and contracting basics, including the acquisition framework, security requirements and guidance, contract administration, security-related contractual documents, and the fundamental NISP roles and responsibilities.

On August 19, the Industrial Security team released two new security posters, "Know Security! No Incidents!" and "Get in Sync with Security." The posters are available for you to **download** and promote security awareness in the workplace.

Two new Industrial Security webinars are now available. The first webinar, *Security Rating Criteria Requirements*, **can be accessed here**. DCSA subject matter experts provide

an overview of the refined security rating criteria being implemented on October 1, 2024. This refinement consolidates the two lists of criteria used under the current process into a single list known as the "Gold Standard" and creates a common understanding of definitions and requirements.



The second new Industrial Security webinar, *Introduction to the Security Rating Score*, is **now available**. DCSA subject matter experts introduce the refined security rating process which will be implemented on October 1, 2024. These refinements incorporate a security rating score and a common set of definitions for criteria within the four security posture categories.

THE SECURITY TRIANGLE: SECURITY, LAW ENFORCEMENT, AND INTELLIGENCE COURSE

CDSE's Education Program released its newest virtual instructor-led course, **ED402, The Security Triangle: Security, Law Enforcement (LE), and Intelligence**. It focuses on the three components of the security triangle (security, LE, and intelligence). Through the review of case studies, this course explores how the DOD security professional collaborates with and supports LE and intelligence communities to prevent future security failures. This new eight-week course runs between October 14 and December 15 and is open to all federal civilians and military personnel (active and reserve) with or without an undergraduate degree. The course is unavailable to contractors. Students will receive 80 professional development units (PDUs) upon successful completion. Visit the course webpage to learn more and the Security Training, Education, and Professionalization Portal (STEPP) to register.





PERSONNEL VETTING SEMINAR

CDSE is presenting the Virtual-led Personnel Vetting Seminar on November 19-21. This seminar addresses the requirements associated with the reform of the Federal Government's personnel vetting system, known as Trusted Workforce 2.0 (TW 2.0). Its purpose is to aid personnel vetting practitioners in DOD, federal agencies, and private industry to understand TW 2.0 requirements, identify gaps between current and future procedures, and support implementation. The seminar covers end-to-end personnel vetting operations, including the federal background investigations program, National Security Adjudications, Continuous Vetting, and Insider Threat analysis in a collaborative environment.

This three-and-a-half day course is intended for U.S. Government security professionals, military personnel, cleared industry Facility Security Officers (FSOs), and other federal personnel performing personnel vetting security-related duties and for personnel executing security programs for cleared industry. Visit the [course page](#) to learn more and register.



UPCOMING WEBINARS

Sign-up is available for the following **upcoming live webinars**:

Security Professional Trusted Workforce 2.0 Gap Training

September 17, 2024
1:00 p.m. to 2:30 p.m. ET

Counterintelligence and Insider Threat Curricula Overview

September 19, 2024
12:00 pm to 1:00 pm ET

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.

