



THIS MONTH'S FOCUS

Industrial Security Annual Planner: Tools for a more Secure Nation

By Isaiah Burwell

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 <i>Director, DCSA</i>	Daniel J. Lecce <i>Deputy Director, DCSA</i>
Kevin Jones <i>Assistant Director, Security Training</i>	Erika Ragonese <i>Deputy Assistant Director, Security Training</i>

CDSE Leadership

Audrey Gutierrez <i>Director</i>	Glenn Stegall <i>Deputy Director</i>
-------------------------------------	---

Pulse Staff

Cashmere He <i>Chief Content Officer</i>	Isaiah Burwell <i>Content Writer</i>
Matthew Wright Tammi Bush <i>Content Contributors</i>	Marc Pulliam <i>Content Designer</i>

Center for Development of Security Excellence

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

The Industrial Security Program is a multi-disciplinary security program focused on the protection of classified information developed by, or entrusted to, U.S. industry operating under the National Industrial Security Program (NISP). CDSE provides numerous training products to develop the industrial security skillset of both Government employees and industry professionals. One of the ways security professionals can learn about CDSE's offerings is by consulting the **Industrial Security Program Annual Planner**. This job aid serves as a supplemental tool to support and grow industrial security training and awareness within organizations throughout the year. One of the most diverse and valuable resources in the planner is the toolkits.

Toolkits are a one-stop access point for multiple resources within a security discipline. For instance, the **Facility Security Officer (FSO) toolkit** contains links to job aids, security shorts,

security training videos, webinars, and forms. FSOs play a crucial role in the NISP. They are the liaisons between industry and Government and have key responsibilities that include protecting classified information and ensuring compliance with the applicable National Security Program Operating Manual (NISPOM) security requirements. FSOs have a complex job, and they cannot do it alone. The **Deliver Uncompromised Toolkit** is a valuable resource for cleared individuals who share the obligation to protect national security.



The Deliver Uncompromised Toolkit contains sub-categories for other security disciplines, including counterintelligence, supply chain risk management, and cybersecurity risk management. Each subcategory contains its own list of documents, videos, and other resources. These tools educate security professionals on how to better protect the Nation's critical technology from our adversaries. Without them, our mission readiness, the safety and security of our warfighters, and the security of our citizenry are in jeopardy. In some areas, our adversaries have stolen technologies, improved them, and moved past us, giving them a technological edge. Protecting our technology is paramount to our mission, and that is why in addition to the Deliver Uncompromised toolkit, the **Cybersecurity toolkit** is so important.

The Cybersecurity Toolkit offers links to training, posters, security awareness games, eLearning, webinars, shorts, and policy guidance. There is also a section of the toolkit dedicated to social media policies, best practices, and job aids. These tools educate cleared professionals on how to have a safe online presence, the importance of which cannot be understated.

On Dec. 8, 2024, a state-sponsored Chinese hacking operation accessed third-party software to tap into desktop computers of U.S. Department of the Treasury



employees. Every cleared individual should be aware of the risks and use caution when online, because you never know if or when you could become an adversary's target.

Though this article highlighted the toolkits, their existence does not lessen the importance of the other resources in the Industrial Security Program Annual Planner. You can follow the 12-month schedule as is or customize it to fit your organization's needs. A new planner is released each year, and CDSE does not rely on the same content each time. New research and information bring change, and we continuously provide new posters, job aids, and other tools every year.

INSIDER THREAT

Insider Threat Detection and Analysis Course

Want to sharpen your skills in identifying insider threat indicators? Secure your spot now for the next open session on March 17-21, 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 and obtain and use holistic data in conjunction 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:

March 17-21, 2025 (Virtual)
 April 21-25, 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 and view the full list of prerequisites.

PERSONNEL VETTING

CDSE Personnel Security Training Discipline Name Change

On Jan. 29, 2025, the Personnel Vetting (PV) team updated CDSE's website to personnel vetting in all areas concerning PS training products and services. This change is an immense step consistent with Federal Personnel Vetting (FPV) reform and Trusted Workforce (TW) 2.0 implementation, as well as the future of our training products and services. CDSE's PV training catalog will develop to meet the needs of security practitioners and vetting management across the Security, Suitability, and Credentialing (SSC) enterprise with vested interest in all PV domains, no longer focusing mainly on personnel security. The Personnel Security (PS) Toolkit is now listed as the PV Toolkit. The update can be viewed [here](#).

New Personnel Vetting Process Webcast Series

Check out CDSE's newly released PV Webcast Series! This three-episode series introduces the process that a newly hired federal civilian, military member, or contractor will experience as part of the PV process. This series targets all federal and contractor employees who seek eligibility to access classified information or who are assigned to a sensitive position and need to understand their PV requirements and processes.



Tune in [here](#) for episodes one and two as we explore the Pre-investigation and Investigation stages of the PV Process.

Personnel Vetting Seminar

CDSE is presenting the "Virtual Instructor-led Personnel Vetting Seminar" on May 6-7. This seminar addresses the requirements associated with the reform of the Federal Government's personnel vetting system, known as TW 2.0. This course is intended 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, and Continuous Vetting in a collaborative environment. The course consists of two half-days and targets U.S. Government security practitioners, military personnel, cleared industry Facility Security Officers, other federal personnel performing personnel vetting security-related duties, and personnel executing security programs for cleared industry. Visit the [course page](#) to learn more and register.



Sensitive Compartmented Information (SCI) Refresher Training

The CDSE Special Access Program (SAP) team has released an updated version of the SCI Refresher training course. This short provides those with access to SCI information an eLearning course that their organizations can leverage to cover a vast majority of annual training topics required by DOD policy. This new version of the course includes a test out option for students. Click [here](#) to take the training.

Fundamentals of National Security Adjudications PS001.18

This **7-day course** provides entry to intermediate-level National Security Adjudicators with the essentials needed to assess an individual's loyalty, trustworthiness, and reliability. It also allows them to render trust determinations for an individual to be granted initial or continued eligibility to access classified information or to occupy a sensitive position. 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 application of the national security adjudicative guidelines.

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 if their future behavior would be consistent with national security.

This course is intended for Department of Defense (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 IC Government Civilian/Military personnel (non-adjudicators) who perform duties in support of national security adjudications. Nominations for attendance must be approved and made through a 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 per SP&D: PDUs are determined by length of course and IAW with current Certification Maintenance Guidelines.



PHYSICAL SECURITY

ICD 705 Physical Security Construction Requirements for SAPs SA501.16

The CDSE SAP team has released a new version of the Intelligence Community Directive (ICD) 705 Physical Construction Requirements for SAPs. This updated course presents the basic skills required to evaluate the ICD and SAP policies with regards to Special Access Program Facility (SAPF) construction. Due to the similarity in construction standards, this course can also be utilized as a foundation for those evaluating DOD Sensitive Compartmented Information Facilities (SCIFs). Course updates include an updated user interface and a more interactive virtual practical exercise as a final assessment.



Physical Security and Asset Protection PY201.10

The Physical Security and Asset Protection (PY201.10) Virtual Instructor-led training (VILT) course will be held March 10-28. This **21-day course** will provide students the ability to identify and utilize regulatory guidance, methodologies, and concepts for protecting DOD assets. Students will be able to apply the risk management process, conduct problem solving, and incorporate best practices to develop courses of action utilizing physical security measures, based on a cost-benefit analysis, to protect an installation's assets. This course is intended for DOD civilian and military personnel, as well as contractors involved in the planning and management of physical security programs.

The course teaches students how to understand physical security concepts, measures, countermeasures, and aids as well as how to analyze threats, vulnerabilities, and risks to DOD assets to manage risk. Additionally, students will examine physical security plans and requirements for installation and facility access control, while also conducting cost benefit analysis to justify physical security measures.

The prerequisite eLearning courses and exams provide a comprehensive introduction to the Physical Security Program. Students are required to successfully complete all the prerequisites prior to requesting enrollment in the Instructor-led course.

INDUSTRIAL SECURITY

Upcoming Getting Started Seminar for New Facility Security

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



Acronym Adventure Game

The Industrial Security team is pleased to announce the release of a new security awareness game, **Acronym Adventure**. The game will help improve or refresh your knowledge of acronyms commonly used in the Industrial Security field. This game provides our stakeholders with a fun and unique challenge of selectively aligning with allies to securely transport a classified package by accurately deciphering acronyms.



NISP Acronyms Job Aid

The Industrial Security team released a new job aid, **NISP Acronyms**. This job aid provides commonly used acronyms and their terms within the National Industrial Security Program.

New Industrial Security Job Aid

Industrial Security is pleased to announce the release of a new job aid, the Industrial Security Flyers! This job aid is a collection of security flyers that provide security reminders to individuals operating within the NISP. The security flyers highlight the following areas of Industrial Security: Classified Visits and Meetings, Counterintelligence, Foreign Travel, Insider Threat Indicators and Reporting, Investigation and Clearance Process, Make Sure It's Secure, OPSEC, Reporting Requirements, Safeguarding Classified Material, Security Awareness, Security Violations, and Upcoming Security Review. These security flyers can be used in two ways: they can be inserted directly into an email message or network pop-up or they can be saved locally, and the security officer's information can be added to the lower left form field. **View the security flyers** and learn more.

CDSE & DCSA NEWS

CDSE Webinars

Behind the Threat: Unraveling Violence Theories, Legal Shifts, Defensible Tactics, and Real-World Lessons

March 13, 2025
12:00 pm to 2:00 pm ET
[Click here to register](#)

Strengthening the DIB through the DC3 Vulnerability Disclosure Program (VDP): an Information and Enrollment Session

March 20, 2025
1:00 pm to 2:30 pm ET
[Click here to register](#)

Listen to the Voices of DCSA

To defend national security, trust must be the bedrock of every government agency. It is at the forefront of everything DCSA and CDSE do to combat insider and foreign threats. It builds confidence with our industry partners and throughout our facilities. In their own words, Gatekeepers, including DCSA Director David Cattler, share their feelings about this critical mission. Watch the DCSA's America's Gatekeeper "**Safeguarding tomorrow, today,**" 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.



STAFF SPOTLIGHT

Meet Tom Gentle: Counterintelligence Curriculum Manager



Tom Gentle

Tom Gentle is the Counterintelligence (CI) 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), and is responsible for the management of the CI training and awareness curriculum.

Gentle's professional career includes 20 years in the U.S. Army as a CI Special Agent in both strategic and tactical environments; 12 years as a Senior Manager and Program Manager in the private sector, and five years supporting the CDSE Insider Threat Team.

The CI Team's success is the result of many individuals' expertise on the CI Team, internally to CDSE and DCSA, and externally. While the CDSE CI Team is small, consisting of three contractors – two instructors and one instructional system designer, it is highly productive and efficient. The FY24 CI curriculum

consisted of 107 products hosted within the CI toolkit on the CDSE website, and the FY25 CI curriculum will see the addition of 23 new products. Those products include case studies, eLearning, instructional presentations, job aids, posters, shorts, videos, and webinars, which support the Defense Security Enterprise. During FY24, the CI Team developed 10 new products and conducted a comprehensive review of the entire CI catalog, ensuring all products were current.

For FY25, the CI Team is incorporating three new content areas into the CI curriculum – fraud; artificial intelligence; and behavioral science. These new content areas will be included in eLearning, case studies, job aids, posters, and webinars. The CI Team also provides CI training and awareness instruction in four CDSE courses that include the Fundamentals of National Security Adjudications, DOD Security Specialist Course, Getting Started Seminar for New Facility Security Officers, and the Mid-Level Special Access Program Manager's Course. The CI Team hosts two CI webinar annually and collaborates with the CI Partnership Branch, DCSA on four quarterly CI webinars. You can learn more about the CI curriculum [here](#).



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/SPeD 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

