DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

June 2025

Dear Facility Security Officer (FSO) (sent on behalf of your Industrial Security Representative (ISR)),

DCSA Industrial Security (IS) publishes the monthly Voice of Industry (VOI) newsletter to provide recent information, policy guidance, and security education and training updates for facilities in the National Industrial Security Program (NISP). Please let us know if you have questions or comments. VOIs are posted on DCSA's website on the NISP Tools & Resources page, as well as in the National Industrial Security System (NISS) Knowledge Base. For more information on all things DCSA, visit www.dcsa.mil.

TABLE OF CONTENTS

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

NBIS MULTI-FACTOR AUTHENTICATION (MFA) UPDATE

NBIS is committed to continuously improving the user experience for both case processors and applicants. To ease the burdens resulting from the implementation of the new Multi-factor Authentication (MFA) process, NBIS has restored the functionality enabling case processors to reset an applicant's eApp password. This feature operates identically to its pre-D-ICAM rollout state, providing a familiar and efficient method for assisting applicants who require password resets. This restoration is intended to streamline workflow and minimize disruptions caused by MFA.

Furthermore, NBIS is introducing a new eApp Custom Landing page designed to simplify the login process for applicants. This update removes the visibility of the Common Access Card (CAC)/Personal Identity Verification (PIV) login option, which has been non-functional since the D-ICAM rollout. By eliminating this inactive option, the new landing page provides a cleaner, more straightforward login experience for applicants, reducing confusion and ensuring a smoother entry point to the eApp system.

Please continue to utilize the DCSA Multi-Factor Authentication Assistance website.

FEBRUARY 2024 VERSION OF PERSONNEL SECURITY STANDARD FORMS REQUIRED BEGINNING AUGUST 1, 2025

The February 2024 version of Standard Forms 85, 85P, 85P-S, and 86 was enabled by DCSA for use within NBIS Agency and eApp on May 12, 2025. Upon implementation, it was announced DCSA would continue to receive and process requests initiated on prior versions of the applicable Standard Forms 85, 85P, 85P-S, or 86 until August 1, 2025.

What does this mean for customers? Starting August 1, DCSA Background Investigations (BI) will reject requests that are not on the February 2024 version of the Standard Forms. There are two options recommended to ensure compliance. First, customers should make every attempt to release any requests on prior versions of the Standard Forms soonest to ensure they are processed prior to the deadline, recognizing that the forms will need sufficient time (~10 days) to go through the Adjudication and Vetting Services (AVS) workflow before they are received by BI. Next, FSOs can cancel investigation requests initiated on prior versions and initiate a new request on the February 2024 form. Previous data entered by the subject will be pre-filled into the new request on the 2024 version.

For additional details, or more information, customers are encouraged to reach out to the Customer Engagements Team (CET) at:

dcsa.ncr.nbis.mbx.contact-center@mail.mil

878-274-1765

Hours 6:00 a.m. – 5:00 p.m. ET

2025 COGSWELL AWARD RECIPIENTS ANNOUNCED

DCSA has recognized 15 facilities as recipients of the 2025 James S. Cogswell Outstanding Industrial Security Achievement Award. Chosen from nearly 13,000 cleared facilities in the United States, each facility has demonstrated industrial security excellence. To qualify, companies must establish and maintain a security program that exceeds basic NISP requirements. Recipients also help other cleared facilities establish security-related best practices while maintaining the highest security standards for their own facility. See the list of winning facilities here.

SECURITY REVIEW RATING RESULTS

The following security review results are current as of June 18, 2025:

Overall Fiscal Year Goal:	4,000	
Rated Security Reviews Completed:	3,116	(78.0%)
Rated Security Reviews Remaining:	884	(22.0%)
Superior Ratings Issued:	475	(15.2%)
Commendable Ratings Issued:	1,114	(35.8%)
Satisfactory Ratings Issued:	1,500	(48.1%)
Marginal Ratings Issued:	12	(00.4%)
Unsatisfactory Ratings Issued:	15	(00.5%)

Note: These results include both initial security review ratings and compliance review ratings. DCSA conducts a compliance review when a contractor receives marginal or unsatisfactory rating during a security review. Access the informational Compliance Reviews slick sheet to learn more.

DCSA FORM 147, JANUARY 2025 - IMPLEMENTATION

The Office of Personnel Management (OPM) has approved the collection renewal using the revised DCSA Form 147, Open Storage Area and Vault Approval Checklist, dated January 2025. This revision significantly reduces the time required to complete it, removes identified redundancies, and reduces the page count by more than half. The form's purpose remains the same: to provide a sufficient description of the approved area and encourage Industry to transition older closed areas. These improvements are a direct result of feedback received from DCSA field personnel and industry security professionals. The revised form aligns with safeguarding requirements outlined in the Title 32 Code of Federal Regulations (32 CFR) Part 117, National Industrial Security Program Operating Manual (NISPOM) Section 117.15, Safeguarding Classified Information, and 32 CFR Part 2001.53, Open Storage Areas.

DCSA Form 147 is available for download at NISP Tools & Resources (under the Industry Tools FSO Forms dropdown) for use starting July 1, 2025. To facilitate a smooth transition, DCSA will implement a "soft-landing" approach from the current April 2022 version to the revised January 2025 version as follows:

- July 1, 2025 through September 30, 2025 (90-day grace period): Industry may submit either the April 2022 or the January 2025 version of DCSA Form 147.
- September 30, 2025: End of the 90-day transition period.
- Effective October 1, 2025: Only submit the January 2025 version of DCSA Form 147.
- October 1, 2027: Extended suspense date for submitting a new DCSA Form 147 to complete the transition of older closed areas previously approved on the obsolete one-page DCSA Form 147.

Important Notes

- Open storage areas and vaults approved using DCSA Form 147, April 2022 version, will remain valid.
- Closed areas approved using the obsolete one-page DCSA Form 147 must be updated and documented as open storage areas. The deadline for this transition has been extended to October 1, 2027. Industry must submit a new DCSA Form 147 to their assigned ISR to complete this transition.
- Reminders of these transition dates will be disseminated through the VOI on a recurring basis until the transition is complete.

If you have any questions or need assistance, please contact HQ DCSA, NISP Mission Performance (NMP) Division at dcsa.quantico.dcsa.mbx.isd-operations@mail.mil.

INDUSTRY SELF-CERTIFICATION FOR OPEN STORAGE AREAS

DCSA has approved the return of a self-certification process, also referred to as self-approval, for open storage areas within Industry. This process had been disestablished with the introduction of the 32 CFR Part 117, NISPOM and is now being reintroduced. To successfully implement the reintroduction, DCSA will employ a collaborative approach with the National Industrial Security Program Policy Advisory Committee (NISPPAC) Industry Group. DCSA will establish two working groups, one internal with our field personnel and one external with NISPPAC industry security professionals to collect recommendations and suggestions, update guidance, and implement the process for FSOs to approve open storage areas.

This reintroduction was considered after careful review by DCSA senior leadership with feedback from our industry partners. Although not explicitly defined in the NISPOM, the Department of Defense Manual (DoDM) 5220.32, Volume 1, government policy guidance for industrial security allows DCSA to grant self-certification when a contractor meets qualification criteria and training program requirements. We anticipate positive benefits such as reduced approval timelines, minimal impacts to contract deliverables, and more efficient time management. This is very impactful for larger facilities with multiple open storage areas. The working groups will run concurrently through July and August, with a test period in September. The goal is to have written procedures, validate them with Industry, with full implementation beginning October 1, 2025. Additional information will be provided as we approach the October conclusion. Please contact the NMP Division at dcsa.quantico.dcsa.mbx.isd-operations@mail.mil with questions or suggestions.

MILITARY SDDC CUSTOMER AND CARRIER ADVISORY

On April 9, 2025, the Military Surface Deployment and Distribution Command (SDDC) issued a Customer and Carrier Advisory found here regarding use of the Defense Transportation Tracking System (DTTS) services for shipments of Arms, Ammunition and Explosives (AA&E) and other sensitive materials (OSM). The advisory indicated DTTS will only execute Satellite Motor Surveillance (SNS) and Trailer Tracking (DCS) transportation protective services when the motor carrier has been selected through the Domestic Tender Program via a designated Department of Defense (DoD) shipper system by a DoD transportation Office. This advisory essentially means DTTS will no longer accept out-of-system Transportation Protective Services requests.

On May 13, 2025, SDDC issued an update to the original advisory temporarily reinstating the acceptance of such requests to execute SNS and DCS using an updated DTTS Shipment Form which now requires additional information to include a DoD POC to identify which DoD agency owns the requirement. SDDC advises that the form has specific instructions that must be closely followed and failure to follow the instructions will result in the shipment not being monitored by the DTTS Program Management Office. Continued noncompliance with the form's instructions will result in DTTS not monitoring future shipments from that organization. Additional information may be requested from the SDDC, G3, Defense Transportation Tracking System PMO at usarmy.scott.sddc.mbx.dtts@mail.mil.

UPDATED SF 328 OVERVIEW AND IMPLEMENTATION

As a continued reminder, the updated Standard Form (SF) 328, "Certificate Pertaining to Foreign Interests," was approved on May 1, 2025, and includes several improvements to increase users' clarity and understanding of the questions and subsequent requirements. After extensive coordination and collaboration with Industry and other government stakeholders, the SF 328 was updated to include better-scoped questions, comprehensive instructions, definitions, and a Statement of Full Disclosure of Foreign Affiliations used to report foreign employment throughout the form. The updated SF 328 was deployed in NISS on May 12, 2025. Any packages initiated or submitted on or after May 12 are required to use the updated SF 328. DCSA published a two-page information paper highlighting key updates and the implementation plan provided to DCSA field elements; it can be viewed here on the DCSA website under Updates. For questions or assistance, please contact the Entity Vetting Knowledge Center at 878-274-2000, (Option 2, then Option 1) or dcsa.fcb@mail.mil.

RECORDING NATO BRIEFING DATES IN DISS

The DCSA NMP Division is addressing questions about North Atlantic Treaty Organization (NATO) briefing requirements. We are developing updated guidance in coordination with NISPPAC, which will be released in a future VOI.

In the meantime, we want to clarify a common point of confusion pertaining to the recording of NATO briefings in the CSA-designated database. For contractors under DCSA cognizance, this means you must enter the ***NATO initial briefing date*** and the ***NATO debriefing date*** in the Defense Information System for Security (DISS). DCSA does not require contractors to enter the annual NATO refresher briefing dates in DISS or to upload a copy of the actual briefing certificates.

COVERED JVs IN THE NISP: AN OVERVIEW FOR INDUSTRY

As a continued reminder, DCSA has issued updated procedures for processing covered joint ventures (JVs) under the NISP in accordance with DoD Directive-Type Memorandum (DTM) 24-004. A critical update for industry partners: covered JVs will not be issued a facility clearance (FCL) by DCSA on behalf of DoD.

A JV qualifies as a covered JV when awarded a DoD classified contract and all participating venturers hold active FCLs at the same level or higher as that required for the JV. The covered JV must still be sponsored in NISS to support classified contract performance and will still have an active NISS profile. If any venturer does not hold the requisite FCL, the JV must be processed for an FCL.

The sponsor should clearly indicate if it is requesting the JV be processed as a covered JV or if it will follow the normal FCL process when submitting the NISS sponsorship. The JV is responsible for providing the following documents to DCSA through an FCL package once the sponsorship is submitted and approved:

- Security Plan approved by the Government Contracting Activity (GCA), identifying key management personnel (KMP) and the venturer managing the JV's security program
- SF 328 from the JV and each venturer
- Corporate governance documents for the JV's legal structure (e.g., JV agreement, bylaws, or operating agreement)
- Organizational chart showing the JV's legal structure and full ownership and control information for each venturer with five percent or greater interest, fully diluted, direct or indirect
- Exclusion resolutions excluding the JV and its subcontractors from accessing classified information held by the venturers.

DCSA will review and validate submissions, ensure records are accurate, and confirm which venturer manages the JV's security program. The Field Office associated with the venturer managing the JV's security program will provide oversight of the JV as part of its oversight of the managing venturer. Covered JVs must continue to update their NISS profile when changed conditions occur, such as new contracts, KMP updates, material SF 328 updates, or restructuring. Failure to maintain current records may impact classified work authorization for the JV and venturers.

These updates reflect DoD's ongoing effort to streamline oversight of classified contracts while maintaining robust security standards. Covered JV eligibility is not automatic - DCSA will validate each venturer's FCL status and confirm classified contract requirements before accepting the JV sponsorship.

For questions or assistance, please contact the Entity Vetting Knowledge Center at 878-274-2000 (Option 2, then Option 1) or dcsa.fcb@mail.mil.

OFFICE OF COUNTERINTELLIGENCE SVTC AND WEBINAR

Defense Industrial Base Counterintelligence Threat Trends Secure Video Teleconference (SVTC)

DCSA invites cleared industry and academia personnel to participate in an SVTC for the Defense Industrial Base entitled, "Defense Industrial Base Counterintelligence Threat Trends." DCSA counterintelligence analysts and agents will provide a classified presentation on the latest quarterly update of the DCSA annual report "Targeting U.S. Technologies: A Report of Threats to Cleared Industry."

The SVTC is an in-person event at most DCSA field offices on July 10, 2025, from 1:00 to 2:30 p.m. ET. Please register by July 3, 2025 by filling out the form here.

Artificial Intelligence Webinar

DCSA invites cleared industry and academia personnel to participate in an unclassified webinar on July 17, 2025 from 1:00 to 2:30 p.m. ET, exploring "Artificial Intelligence (AI) Risks and Threats to National Security." Department of Justice expert Mr. David DeCola will discuss how to balance the advantages of AI with its potential security vulnerabilities in technology and operations. This session is designed for cleared industry and academic personnel, including leaders, security professionals, engineers, and cybersecurity experts. Please register here by July 14, 2025.

NISP CONTRACT CLASSIFICATION SYSTEM (NCCS)

NCCS TEAM ENGAGES WITH INDUSTRY AT NCMS

The NCCS Team recently participated in the annual NCMS Industrial Security Conference, providing direct support to cleared industry partners through an on-site help desk. Over the 4-day event, our team addressed 78 NCCS inquiries and distributed 350 informational brochures to conference attendees.

Meeting our industry partners face-to-face was invaluable. The level of interest in NCCS demonstrated the system's growing importance within the industrial security community. The NCCS help desk received lots of attention on Tuesday and Wednesday, with many questions focusing on system capabilities, user access, and the application process. Industry representatives expressed particular interest in how NCCS streamlines the classification management process and enhances security compliance.

In addition to NCCS support, our team assisted with 72 NISS-related inquiries, leveraging virtual collaboration tools to connect users with remote subject matter experts when needed.

The conference provided a unique opportunity to gather direct feedback from our user community. These insights will help shape future NCCS enhancements as we continue to refine the system to meet industry needs.

Cleared contractors interested in learning more are encouraged to visit the NCCS website to review available resources and begin the onboarding process. Training materials, quick start guides, and system documentation are readily accessible to support your implementation.

NCCS PRESENTATIONS AVAILABLE

The recordings from the NCCS presentation, "The Power of Partnership: Trust in People, Facilities, Systems, and Data," delivered at the CDSE Industry Conference in April, are now available on the CDSE website. These recordings highlight the industry perspective and can be accessed via the following links:

- Day 1 - NCCS Presentation to Industry
- Day 2 - NCCS Q&A with Industry

For questions or additional information regarding NCCS, please contact our support team at dcsa.quantico.is.mbx.nccs-support@mail.mil.

NAESOC UPDATES

UPCOMING WEBINARS

The National Access Elsewhere Security Oversight Center's (NAESOC) latest Webinar for 2025 entitled "This is the NAESOC" is now available on the CDSE website. This Webinar provides an updated view of the multiple services the NAESOC provides and how its activities support the DCSA mission. Assigned facilities, GCAs, other stakeholders, and interested parties may see how our mission and activities can support their requirements. We welcome all to take a listen and learn more about us.

ITEMS OF NOTE

Also please visit the NAESOC web page to find updates on the Resources tab. There you will find a current list of FAQs inspired by FSO requests.

Do you have an idea for a future training topic or need a speaker at your event? Please click here to request a speaker or suggest a training topic.

REQUESTS SENT TO THE NAESOC

The NAESOC assigns priority to Industry requests and actions based on identified risk. If you identify that an already-submitted issue or request requires a higher priority than it has been assigned, or if you have issues that require the immediate attention of NAESOC leadership, please access the NAESOC web page and activate the "Blue Button" (Escalate an Existing Inquiry) which will generate an email you can send directly to NAESOC leadership.

For routine requests:

- (878) 274-1800 for your Live Queries
  Monday through Thursday - 9:00 a.m. to 3:00 p.m. ET
  Friday - 8:00 a.m. to 2:00 p.m. ET
- E-mail dcsa.naesoc.generalmailbox@mail.mil
- NISS message

QUARTERLY INDUSTRY STAKEHOLDER ENGAGEMENT

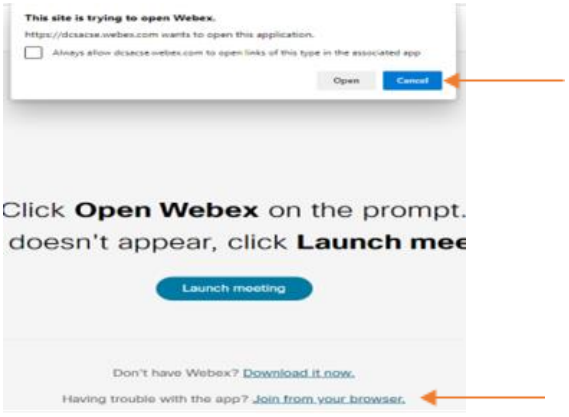
The DCSA Customer & Stakeholder Engagement (CSE) team will host the next quarterly Industry Stakeholder Engagement (ISE) on July 10, 2025 from 10:30 a.m. to 12:00 p.m. ET for all Industry FSOs and Security Professionals. The last engagement, held on March 18, 2025, resulted in an outstanding attendance of almost 400 FSOs and industry security professionals. Last quarter's engagement focused on FCL Metrics and Processes, NBIS, AVS and BI updates.

The July ISE will be held virtually via Webex and a dial in number. The tentative agenda for the meeting will consist of:

- Introduction/Welcome
- DCSA Background Investigations (BI) – Industry Metrics, Best Practices and DISS SII Search Overview
- Adjudication and Vetting Services (AVS) – AVS Updates
- DCSA Field Support and Review – Catch'em-in-CONUS processes
- NBIS Program Executive Office – NBIS Updates
- Conclusion.

Note: When logging into Webex, please use your government/company email (vs. personal email) and First/Last name. **This is beneficial to us to help address individuals and their questions.**

Logging into Webex Meetings: After clicking on the meeting link or copy/pasting the link into your browser, click Cancel and then Join from your browser.



If you are still experiencing issues, please use the dial in information using your phone.

Phone: 1-415-527-5035

Access Code: 2825 212 0010

Join meeting

INSIDER THREAT TRAINING FOR CLEARED INDUSTRY

DCSA has announced updated training guidance for insider threat program personnel in cleared industry, effective July 1, 2025. This update continues to provide industry partners with flexibility in meeting mandatory training requirements while ensuring classified information and critical assets are protected.

Under the updated guidance, newly appointed insider threat program personnel can satisfy minimum training requirements by either completing the Center for Development of Security Excellence (CDSE) Insider Threat Program for Industry Curriculum, INT333.CU or by completing a contractor-developed training program that incorporates the required topics outlined in 32 CFR Part 117.12(g)(1).

The term "program personnel" refers to individuals who ***manage*** the insider threat program, including the Insider Threat Program Senior Official (ITPSO). The ITPSO is responsible for identifying the specific individuals within their organization who are considered program personnel and therefore subject to these training requirements. Importantly, insider threat program personnel appointed prior to July 1, 2025, who have already completed training ***are not*** required to complete the new curriculum.

Industry partners are encouraged to review the updated guidance posted to the DCSA Tools and Resources page and implement the necessary changes to their insider threat training programs. Questions concerning the updated insider threat program personnel training requirements can be directed to your ISR or the NMP Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

ADJUDICATION AND VETTING SERVICES (AVS)

AVS CALL CENTER NUMBER

The AVS Call Center can now be reached at 667-424-3850. The legacy CAS Call center number is still active but will be deactivated in the near future.

As a reminder, the AVS Call Center will continue to provide direct support and timely adjudicative updates to Senior Management Officials (SMOs) and FSOs worldwide. The AVS Call Center is available to answer phone and email inquiries from SMOs/FSOs and to provide instant resolution on issues identified by Security Offices whenever possible, and serves as the POC for HSPD12/Suitability Inquiries.

The AVS Call Center is available from Monday through Friday between 6:30 a.m. and 5:00 p.m. ET to answer phone and email inquiries from FSOs only. Contact the AVS Call Center by phone at 667-424-3850 (SMOs and FSOs ONLY; no subject callers), or via email at dcsa.meade.cas.mbx.call-center@mail.mil.

For Industry PIN Resets, contact the Applicant Knowledge Center at 878-274-5091 or via email at DCSAAKC@mail.mil.

SF 312 JOB AID

NISP contractor personnel may now sign SF 312s using a DoD Sponsored/Approved External Certificate Authority (ECA) Public Key Infrastructure (PKI):

- The use of digital signatures on the SF 312 is optional. Manual or wet signatures will still be accepted by AVS.
- If the Subject digitally signs the SF 312, the witness block does not require a signature.
- Digital signatures must be from the list of DoD Sponsored/Approved ECA PKI located here.
- The public list of DoD approved external PKIs that are authorized to digitally sign the SF 312 can be located here.

The Job Aid and OUSD I&S Memorandum are available on the DCSA Website.

REMINDER ON TIMING OF ELECTRONIC FINGERPRINT TRANSMISSION

As we move closer to full implementation of Trusted Workforce 2.0, AVS continues to work diligently to partner with Industry to get cleared people to work faster and more efficiently all while effectively managing risk. To maintain our interim determination timeliness goals, we ask that electronic fingerprints be submitted at the same time or just before an investigation request is released to DCSA in DISS.

Fingerprint results are valid for 120 days, the same amount of time for which eApp signature pages are valid. Therefore, submitting electronic fingerprints at the same time or just before you complete your review for adequacy and completeness, should prevent an investigation request from being rejected for missing fingerprints.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

URL CHANGES FOR SECURITY TRAINING WEBSITES

Security Training, Education, and Professionalization Portal (STEPP) and the Security Awareness Hub (SAH) will have new URLs effective Monday, June 30, 2025. The update will transition the security training URLs to DCSA-owned domains. Training will be available throughout the transition with minimal impact anticipated. The new URL for the STEPP platforms is https://securitytraining.dcsa.mil/ replacing https://cdse.usalearning.gov/. The new SAH URL is https://securityawareness.dcsa.mil/ replacing https://securityawareness.usalearning.gov/. Users will need to update bookmarks to these new URLs.

JUNE PULSE NOW AVAILABLE

DCSA recently released the CDSE Pulse, a monthly security awareness newsletter that features topics of interest to the security community as well as upcoming courses, webinars, and conferences. The June Pulse focused on training and resources related to CUI. Check out all the newsletters in CDSE's Electronic Library or subscribe to have the newsletter sent directly to your inbox by signing up here.

INSIDER THREAT

The Insider Threat team has launched a new curriculum for Industry titled "Insider Threat for Industry Curriculum (INT333.CU)." This curriculum provides training for insider threat program personnel working in cleared defense industries. It was developed to support students in meeting the requirements outlined in 32 CFR Part 117, NISPOM.

The INT333.CU curriculum description, learning objectives and courses can be found here.

PERSONNEL VETTING

Customer Service Request (CSR) and Incident Report (IR) Management Resource

Check out the CSR and IR Management Resource, which provides clarification and guidance on submitting Customer Service Requests and Incident Reports to DCSA AVS. The materials are provided as part of a larger effort across the DoD to improve the personnel vetting mission. DCSA AVS has provided individual CSR and IR guidance on an as needed basis to customers. However, until now, the guidance has never been publicly available. The new materials will answer customer requests for specific information on CSR and IR submissions and incorporate customer feedback. As a result, this will enable customers to submit timely, quality-improved CSR and IR information for adjudication.

Personnel Vetting Seminar

CDSE will present the virtual instructor-led Personnel Vetting Seminar on August 5 and 6 to address requirements associated with personnel vetting reform, known as Trusted Workforce (TW) 2.0. The course aims to provide personnel vetting practitioners across Government and Industry with an understanding of TW 2.0 requirements, gaps, and 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-day sessions targeting U.S. Government security practitioners, military personnel, and other Federal personnel performing personnel vetting security-related duties and for FSOs and other personnel executing security programs for cleared industry. Visit the course page to register.

SPECIAL ACCESS PROGRAMS (SAP)

Fixed Facility Checklist Short

SAP released a new Fixed Facility Checklist short. The short focuses on the Fixed Facility Checklist and explains how to fill out the necessary information concerning the establishment and maintenance of a SAP facility.

Introduction to Special Access Programs (SAPs) Course (SA101.01)

The Introduction to SAPs course focuses on the DoD SAP fundamentals to prepare students to become SAP security professionals. The lessons address security enhancements across all security disciplines, compliance inspection requirements, annual reviews, and audits. The course is administered through eLearning prerequisites and synchronous elements using the collaborative learning environment (CLE)

STEPP. Class activities include group and individual practical exercises, quizzes, a team capstone, and a final course exam. The prerequisite eLearning courses/exams that provide a comprehensive introduction to SAP must be successfully completed prior to requesting enrollment into the instructor-led course. The course is offered on the following dates:

- August 5 to 8, 2025 (Lexington, MA) (MIT)
- September 9 to 12, 2025 (Rolling Meadows, IL) (NGC).

FISCAL YEAR 2025 UPCOMING COURSES

CDSE instructor-led training (ILT) or virtual instructor-led training (VILT) courses are a great way to earn professional development units (PDUs) and maintain Security Professional Education Development (SPēD) Program certifications and credentials. Secure your spot now as classes fill quickly! Available ILT/VILT courses are listed below.

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)

- July 28 - August 24, 2025 (Virtual)

INSIDER THREAT

Insider Threat Detection Analysis VILT (INT200.10)

- July 21 - 25, 2025 (Virtual)
- August 18 - 22, 2025 (Virtual)
- September 22 - 26, 2025 (Virtual)

PERSONNEL SECURITY

Personnel Vetting Seminar VILT (PS200.10)

- August 5 - 6, 2025 (Virtual)

PHYSICAL SECURITY

Physical Security and Asset Protection (PY201.01)

- August 18 - 22, 2025 (Linthicum, MD)

SPECIAL ACCESS PROGRAMS

Introduction to Special Access Programs (SA101.01)

- August 5 - 8, 2025 (Lexington, MA) (MIT)
- September 9 - 12, 2025 (Rolling Meadows, IL) (NGC)

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)

SPēD Certification Program Review

The DCSA Security Training Directorate is initiating a comprehensive review of the SPēD Certification Program effective immediately.

A topic of concern for the SPēD program is the Candidate Management System (CMS), which recently migrated to a new platform to meet DoD cybersecurity requirements.

As part of this review, DCSA is pausing the requirement to track and report PDUs indefinitely. SPēD, APC, and CCITP certified professionals should no longer use the CMS to track PDUs or submit for certification renewal, until an alternative solution is identified.

Current SPēD, APC, and CCITP certifications remain valid, and we will ensure this pause does not negatively impact current credentials. Certification testing for these programs will continue as usual and personnel needing to obtain any of these certifications will still be able to do so.

All certificants will receive a new expiration date when the pause concludes. No certifications will expire or be lost during this pause. This pause will allow the SPēD Program Management Office to evaluate and improve the certification maintenance process.

For questions, please contact the SPēD PMO at dcsa.spedcert@mail.mil.

CDSE NEWS

2024 Security Training Annual Report Now Available

The ST Annual Report highlights FY24 significant achievements and progress made in enhancing security education, expanding accessibility, as well as accreditation. Did you know that in FY24 over 5 million CDSE courses were completed? Check out the annual report to view other statistics, accomplishments, and efforts to strengthen the Defense Security Enterprise (DSE) by ensuring the workforce is properly trained and educated to safeguard national security.

CDSE News by Subscription

Get the latest CDSE news, updates, and information. You may be receiving the Pulse through a subscription already, but if not and you would like to subscribe to the Pulse or one of our other products, visit CDSE News and sign up or update your account.

SOCIAL MEDIA

Connect with us on social media!

DCSA X: @DCSAgov

CDSE X: @TheCDSE

DCSA Facebook: @DCSAgov

CDSE Facebook: @TheCDSE

DCSA LinkedIn: https://www.linkedin.com/company/dcsagov/

CDSE LinkedIn: https://www.linkedin.com/showcase/cdse/

REMINDERS

DO NOT SEARCH FOR CLASSIFIED IN THE PUBLIC DOMAIN

Per the principles the 2017 DCSA (then DSS) Notice to Contractors Cleared Under the NISP on Inadvertent Exposure to Classified in the Public Domain, NISP contractors are reminded to not search for classified in the public domain.

FACILITIES MAY ADVERTISE EMPLOYEE POSITION PCLS

In accordance with 32 CFR Part 117.9(a)(9), a contractor is permitted to advertise employee positions that require a PCL in connection with the position. Separately, 32 CFR Part 117.9(a)(9) states "A contractor will not use its favorable entity eligibility determination [aka its Facility Clearance] for advertising or promotional purposes."

NISP CHECKUP

The granting of an FCL is an important accomplishment and its anniversary marks a good time to do a NISP checkup for reporting requirements.

During your FCL anniversary month, DCSA will send out the Annual Industry Check-Up Tool as a reminder to check completion of reporting requirements outlined in 32 CFR Part 117, NISPOM. The tool will help you recognize reporting that you need to do.

DCSA recommends you keep the message as a reminder throughout the year in case things change and reminds cleared contractors that changes should be reported as soon as they occur. You will find information concerning the Tool in a link in NISS. If you have any questions on reporting, contact your assigned ISR. This tool does not replace for or count as your self-inspection, as it is only a tool to determine report status.

An additional note regarding self-inspections, they will help identify and reduce the number of vulnerabilities found during your DCSA annual security review. Please ensure your SMO certifies the self-inspection and that it is annotated as complete in NISS.