DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

May 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) SUPPORT

DCSA implemented a new MFA for NBIS (eApp and NBIS Agency) on May 14 to strengthen cybersecurity posture and align with DoD Zero Trust and Risk Management Framework. This has caused difficulties for users and applicants, which DCSA is addressing.

Recent Actions:

- The DCSA Technical Services Team is working to resolve system access issues through root cause analysis and IT fixes
- Increased Help Desk support with additional resources and overtime
- A step-by-step job aid has been attached to all eApp notification emails to walk applicants through the login process
- Created a dedicated DCSA webpage (https://www.dcsa.mil/Systems-Applications/National-Background-Investigation-Services-NBIS/Multi-Factor-Authentication-Assistance/) to provide status and instructions for login issues including:
  - Status Updates
  - The DCSA Director's Video Message
  - Fact Sheets
  - Job Aids
  - An eApp Walkthrough Webex conducted M-F from 9:00 to 11:00 a.m. and 1:00 to 3:00 p.m. ET.

Support Contacts:

- System Access/MFA Issues (New):
  - Phone: 878-274-1344
  - Email: dcsa.ITSupport@mail.mil
  - Hours: M-F from 5:00 a.m. to 8:00 p.m. ET; Sat from 8:00 a.m. to 2:00 p.m. ET
- Applicant Support (Non-MFA):
  - Phone: 878-274-5091
  - Email: dcsa.boyers.dcsa.mbx.applicant-knowledge-center@mail.mil
  - Hours: M-F from 6:00 a.m. to 5:00 p.m. ET
- NBIS Industry/FSO Support:
  - Phone: 878-274-1765
  - Email: dcsa.ncr.nbis.mbx.contact-center@mail.mil
  - Hours: M-F from 6:00 a.m. to 5:00 p.m. ET.

NBIS UPDATES

Updated Personnel Security System Access Request (PSSAR)

A new version of the DD2962v2 PSSAR form is now available for the Defense Information System for Security, NBIS, and Secure Web Fingerprint Transmission (SWFT) users. Please be aware that while the content of the form remains unchanged, the Office of Management and Budget (OMB) approval has been extended to May 31, 2028. The prior version will no longer be accepted after June 1. Please begin using the updated form immediately.

Therefore, please cease using any DD2962v2 PSSAR forms displaying an OMB approval date other than May 31, 2028. The updated DD2962v2 form is readily accessible and can be downloaded from the following link: https://www.esd.whs.mil/Directives/forms/dd2500_2999/DD2962v2/.

New NBIS Service Level Management Email

For users seeking training/instructional information on the NBIS system, NBIS Service Level Management (SLM) now has a dedicated email address to handle your requests. Please direct all inquiries to dcsa.nbis.mbx.servicelevelmanagement@mail.mil. This will ensure your requests are routed to the appropriate team and addressed promptly.

Low Side Repository (LSR) Consolidation

On March 30, DCSA successfully updated Department of Defense (DoD) civilian, military, and contractor records in the first wave of data from the Clearance Verification System (CVS) to the Defense Information System for Security - Joint Verification System (DISS-JVS). The data in this first wave included full name, place of birth, alias, and investigation or adjudication history. Data was added to DISS to improve efficiency and build the foundation for future phases of the Trusted Workforce 2.0.

Please note we did not overwrite existing data in DISS-JVS with data from CVS. Data was added from CVS that was not previously recorded in DISS-JVS. For example, if a Subject's middle name is missing in JVS, but CVS has one, we only added the middle name. The same is true for blank Birth Country, Birth State, Birth City, Subject Alias, and missing Investigations and Adjudications in the histories.

By introducing CVS data into DISS-JVS, users may notice the following enhancements:

- More cases in the Investigation Summary: Prior to the March update, only investigations adjudicated by the DoD Central Adjudication Facility (CAF) were presented in the Investigation Summary panel. Investigations performed by Federal Agencies were recorded in CVS and presented to DISS-JVS users through the Security/Suitability Investigations Index (SII) Search. These investigations are now presented on the Investigation Summary panel on the Subject screens.

- CE RAPBACK cases: "CE RAPBACK" is a case type that users may see in the Investigation History of the Subject screens. It indicates a Special Agreement Check (SAC) was submitted to DCSA by a Federal Agency (non-DoD) and recorded in CVS. This is a separate effort from the future DCSA Adjudication and Vetting Services effort to enroll members of the DoD and Cleared Industry into the DoD Rap Back Program.

Data Delivery Service (DDS) Updates

Recently, DISS-JVS implemented an interface with the Defense Manpower Data Center (DMDC) Data Delivery Services (DDS) system to control the unmanaged subject issue with the military services. As a result, DISS-JVS is updating industry subject PII based on the data received from the DDS interface. While DDS is an authoritative data source for civilians and military it is not one for industry and FSOs have reported receiving erroneous Personnel Data Repository (PDR) Notifications. Effective immediately, the DISS-JVS Team implemented a daily Data Quality Initiative (DQI) to stop these updates being applied to industry subjects. This update is retroactive and previous notifications have been corrected.

SECURITY REVIEW RATING RESULTS

The following security review results are current as of May 21, 2025:

Overall Fiscal Year Goal:	4,000	
Rated Security Reviews Completed:	2,686	(67.2%)
Rated Security Reviews Remaining:	1,314	(32.8%)
Superior Ratings Issued:	401	(14.9%)
Commendable Ratings Issued:	968	(36.0%)
Satisfactory Ratings Issued:	1,293	(48.1%)
Marginal Ratings Issued:	12	(0.5%)
Unsatisfactory Ratings Issued:	12	(0.5%)

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.

UPDATED SF 328 OVERVIEW AND IMPLEMENTATION

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. Any packages initiated or submitted on or after May 12 will be 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.

INSIDER THREAT PROGRAM PERSONNEL TRAINING

DCSA announces updated training requirements 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 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 at DCSA Industry Tools, NISP Resources, FSO Guides and implement 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 NISP Mission Performance (NMP) Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

REPORT INFORMATION IN DISS PRIOR TO OUT-PROCESSING

Contractors are required to submit Security Executive Agent Directive 3 (SEAD 3) and adverse information reports for subjects who are maintained within their DISS Security Management Office (SMO). If a subject has current eligibility but the contractor has not taken an affiliation with the individual due to having no reasonable expectation of granting the employee access in the future, the individual is not subject to SEAD 3 or adverse information reporting to that contractor. Refer to the DISS Management Job Aid for additional information.

Contractors must submit any known reportable information prior to out-processing a subject from the DISS SMO due to termination or deciding they no longer have a reasonable expectation to access classified information again during their employment.

If a contractor fails to submit known reportable information prior to out-processing a subject from the DISS SMO, the contractor must either re-establish an affiliation with the subject, submit the report, and then out-process the subject once again ***or*** contact DCSA's Adjudication and Vetting Services (AVS) for guidance (contact information is available at the Adjudication & Vetting Services (AVS) webpage).

If a contractor discovers new reportable information after out-processing a subject from the DISS SMO, the contractor should contact DCSA AVS for additional guidance at the AVS webpage.

RECORDING NATO BRIEFING DATES

The DCSA NMP Division is addressing questions about North Atlantic Treaty Organization (NATO) briefing requirements. We are developing updated guidance in coordination with the National Industrial Security Program Policy Advisory Committee (NISPPAC), which will be released during the June Voice of Industry.

In the meantime, we want to clarify a common point of confusion: the recording NATO briefings in the CSA-designated database. For contractors under DCSA cognizance, this means you must enter the ***NATO initial briefing date*** and ***NATO debriefing date*** in 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

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.

THE LATEST IN THE CUI MISSION SPACE

Recent updates that impact the Controlled Unclassified Information (CUI) mission space include the release of a new Controlled Unclassified Information Marking Aid, updates to DCSA's CUI Frequently Asked Questions, and an update regarding the current state of Cybersecurity Maturity Model Certification (CMMC) deployment.

UPDATED CUI MARKING AID

DoD released an updated CUI Marking Aid in December 2024. The updated information clarified the marking requirements when multiple categories of CUI exist within the same document. See the updated CUI Marking Aid as well as other DoD CUI Training Resources here.

CUI FREQUENTLY ASKED QUESTIONS (FAQ)

To provide Industry with the most up to date developments within the CUI mission space, the FAQ page maintained by the CUI Branch, Enterprise Security Operations (ESO) Division, Industrial Security was updated. The CUI FAQs have been updated to reflect the current CUI mission space and will be uploaded to DCSA's CUI Resources page under the Resources for Industry tab.

THE CMMC PROGRAM

The Cybersecurity Maturity Model Certification (CMMC) Program aims to enhance the cybersecurity posture of the Defense Industrial Base by establishing a standardized set of requirements for protecting Federal Contract Information (FCI) and CUI. The CMMC Program provides assessments at three levels, each incorporating security requirements from existing regulations and guidelines.

Level 1: Basic Safeguarding of FCI Requirements

- Annual self-assessment and annual affirmation of compliance with the 15 security requirements in FAR Clause 52.204-21.

Level 2: Broad Protection of CUI Requirements

- Either a self-assessment or C3PAO assessment every 3 years, as specified in the solicitation.
    - Determined by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems.
- Annual affirmation verifying compliance with the 110 security requirements in NIST SP 800-171 Revision 2.

Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats Requirements

- Achievement of CMMC Status of Final Level 2.
- An assessment every 3 years by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).
- Annual affirmation verifying compliance with the 24 identified requirements from NIST SP 800-172.

On December 16, 2024, DoD published 32 CFR Part 170, "CMMC Rule" on the U.S. National Archives and Records Administration (NARA) Federal Register establishing the CMMC Program. In addition to 32 CFR Part 170, DoD has proposed an acquisition rule (48 CFR CMMC Acquisition Rule) to amend the DFARS to address procurement related considerations and requirements related to this program rule. When finalized, the Rule will allow DoD to require a specific CMMC level in a solicitation or contract. The CMMC Acquisition Rule is expected to be released by the end of FY 2025. Additional information is available from DoD OCIO and the CMMC Program.

CUI ASSISTANCE

Remember the ESO CUI Branch remains ready to hear from cleared Industry so that appropriate steps can be taken to assist as needed with the understanding and implementation of contractually obligated CUI safeguarding requirements. For assistance with your CUI related questions, you can reach the CUI Branch for Industrial Security Support by sending an e-mail the CUI Branch or calling the CUI Branch hotline at (571) 305-4878.

OFFICE OF COUNTERINTELLIGENCE SVTC BRIEFINGS

DCSA's Office of Counterintelligence invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) for the Defense Industrial Base for two briefings from the Air Force Office of Special Investigations (AFOSI) entitled, "Counterintelligence Analytical Support to Rapid Acquisition-FY23 Trends and Insights" and "Small Percentage Investment Product" The first briefing distills complex data from AFOSI analytical reports, offering a clearer picture of emerging trends identified during an AFOSI review of companies supporting the Air Force Research Laboratory (AFRL) AFWERX rapid acquisition mission. The briefing will enable participants to understand the evolving counterintelligence landscape and technology protection mission as it merges with rapid acquisition. The second briefing is comprised of exploratory case studies that highlight vulnerabilities from low-percentage or minority investments that malign entities can use to influence and control small businesses. It uncovers the plausibility and implications that particular tactics and techniques can have on innovative entities and emerging technology.

The SVTC is an in-person event at most DCSA field offices on June 12, 2025, from 1:00 to 2:30 p.m. ET.

Please note: The eInvitation system is scheduled to be deactivated in August 2025 and we are transitioning to MS Forms to register for SVTCs. Either option may be used this month to register for the SVTC, however, there is no need to register on both systems.

Please register by June 3, 2025 by either filling out the form here, or by using the eInvitation here.

NAESOC UPDATES

UPCOMING WEBINARS

The National Access Elsewhere Security Oversight Center's (NAESOC) latest Webinar for 2025 entitled "We are the NAESOC" which will be unveiled this month on the CDSE website. This Webinar provides a fresh perspective on the various types of support we provide and how our activities support the DCSA mission. It can be used to assist assigned facilities, GCAs, and other stakeholders, as well as interested parties, to obtain maximum benefit from our services.

ITEMS OF NOTE

Also please visit the NAESOC web page to find updates under 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

NCCS TEAM PRESENTS TO INDUSTRY

The NISP Contracts Classification System (NCCS) Team presented at the DCSA Conference, The Power of Partnership: Trust in People, Facilities, Systems, and Data. The recording is posted here on the CDSE website. A Q&A session was conducted at the close of the conference and the Q & A document from the conference will be available for review on the CDSE website at a later date.

Please direct all questions and correspondence to our support inbox: dcsa.quantico.is.mbx.nccs-support@mail.mil.

ADJUDICATION AND VETTING SERVICES (AVS)

MENTAL HEALTH FIRESIDE CHAT

On January 30, AVS personnel delivered a briefing at the recent Mental Health Fireside Chat hosted by the Institute for Defense Analyses (IDA) in Alexandria, VA. The event provided the audience of NISP contractors and DCSA personnel with valuable insights into mental health, security clearances, and the importance of seeking mental health support. Additionally, AVS offered assistance to the attendees through the PCL help desk. AVS plans to conduct this briefing at future outreach events. More information on Mental Health is available here on the DCSA Website.

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.

CONTINUOUS VETTING ENROLLMENT BEGINS FOR NSPT

DCSA announced the beginning of phased implementation of Continuous Vetting (CV) services for the Non-sensitive Public Trust (NSPT) population in August 2024. This milestone achievement marks the start of a process that will eventually see more than one million additional personnel enrolled in CV services - ensuring a trusted workforce in near real time through automated records, time and event based investigative activity, and agency-specific information sharing. To prepare for this new capability, agencies are encouraged to start working on the process now. DCSA will coordinate with customers during the phased implementation period to ensure agencies are ready to begin enrollment.

Please refer to DCSA News: CV Enrollment Begins for NSPT Federal Workforce for more information.

CONDITIONAL ELIGIBILITY DETERMINATIONS

In February 2024, DCSA AVS began granting Conditional National Security Eligibility Determinations for NISP contractors. "Conditionals" provide increased mission resiliency to our customers by diverting national security cases from due process to monitoring provided by the DCSA Continuous Vetting Program. An update on the process and fact sheet can be seen here.

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 fingerprint 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.

CONTINUOUS VETTING UNENROLLMENT

On February 13, 2025, DISS Release 13.28.0 implemented a change request to update Continuous Evaluation (CE) Enrollment Status interface when a subject "separates" or "reinstates." As a result, when a subject lost affiliation, they were being automatically unenrolled in DISS and subsequently re-enrolled upon re-establishment of affiliation with a new DISS SMO. This re-enrollment process was effectively resetting the "CE Enrollment Date."

To correct this problem, DCSA coordinated with OUSD I&S and deployed DISS Release 13.28.2 overnight on March 13, 2025 to remove the CE status updates to the DISS user interface introduced in Release 13.28.

For questions, please contact the Customer Engagements Team (CET) for assistance with the use of DISS via phone at 878-274-1765 or email at dcsa.ncr.nbis.mbx.contact-center@mail.mil.

Please contact AVS - Vetting for questions on DoD Continuous Vetting Statuses via email at dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

MAY PULSE NOW AVAILABLE

We recently released the CDSE Pulse, a monthly security awareness newsletter that features topics of interest to the security community. In addition, we share upcoming courses, webinars, and conferences. The May newsletter focused on "Mental Health Awareness" month. Check out all the newsletters in CDSE's Electronic Library or subscribe/update your current subscription to get the newsletter sent directly to your inbox by submitting your email address from CDSE News.

2025 VIRTUAL DCSA SECURITY CONFERENCE FOR INDUSTRY RECORDINGS

The 2025 Virtual DCSA Security Conference for Industry was held on April 23-24. The conference was a great success and more than 2,500 participants had the distinct pleasure to hear from panelists discussing policy and operational updates, personnel security updates, and industrial security integration updates from the U.S. military. This year's theme – "The Power of Partnership: Trust in People, Facilities, Systems, and Data," emphasized the important role of trust and building strong partnership across the Defense Industrial Base. Conference recordings are now available.

PERSONNEL VETTING

Customer Service Request and Incident Report Management Resource

On April 1, CDSE, in coordination with DCSA AVS, posted an information resource on cdse.edu. The Customer Service Request (CSR) and Incident Report (IR) Management Resource provides clarification and guidance on submissions of CSRs and IRs to DCSA AVS.

The materials are part of a larger effort across the DoD to improve the Personnel Vetting (PV) mission, or "Pathfinder Initiative." AVS has provided individual CSR and IR guidance on an ad hoc 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 submission and incorporate customer feedback. This will enable customers to submit timely, quality-improved CSR and IR information for adjudication. To receive more information, view the product.

Personnel Vetting Seminar

CDSE is presenting the "Virtual Instructor-led Personnel Vetting Seminar" on Aug 5-6. This seminar addresses the requirements associated with the reform of the Federal Government's PV system, known as Trusted Workforce (TW) 2.0. This course is intended to aid PV 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 PV 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 FSOs, and other Federal personnel performing PV security-related duties, as well as personnel executing security programs for cleared industry. Visit the course page to learn more and register.

New Personnel Vetting Job Aids

The PV Team released three new job aids – PV Scenarios: Continuous Vetting; National Security Adjudication; and PV Scenarios: Upgrades, Transfer of Trust, and Re-Establishment of Trust.

- PV Scenarios: Continuous Vetting. CV is one of the five PV 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.

- 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 the whole person concept, identifying the 13 adjudicative guidelines, and identifying the adjudicative factors used to evaluate the relevance of an individual's conduct.

- PV Scenarios: Upgrades, Transfer of Trust, and Re-Establishment of Trust. This trifold provides a description of three of the 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).

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

INFORMATION SECURITY

Marking Syntax Short (IFS0048)

The DoD Security Training Branch's Information Security team published a new version of the Marking Syntax Short on May 5. This new version of the security short addresses needed updates to ensure the classification security marking guidance is aligned with both DoD and Intelligence Community Directive regulatory guidance. The security short also implemented strategic quality improvements to enhance learner engagement and learning transfer of the content. This security short can be accessed on CDSE's website.

FISCAL YEAR 2025 UPCOMING 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 opportunity 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 plan now for your Fiscal Year 2025 security training. Below is a list of available 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)

- July 28 - August 24, 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) f
- 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)

CDSE NEWS

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.