DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

January 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 QUARTERLY MEETING

NBIS Quarterly meetings were kicked off in October 2024 to provide key updates, show progress through the product roadmap, and present demonstrations when possible and appropriate. This venue will serve as a primary source for comprehensive, verified NBIS updates for customer agencies and industry partners. The next **NBIS Quarterly meeting will be held on Tuesday, February 4, 2025**. A calendar invite has been sent to an approved, appropriate distribution list. Next month's Voice of Industry will include a summary and/or outcomes from this meeting.

SECURITY RATING SCORECARD IMPLEMENTATION UPDATE

DCSA fully implemented the Security Rating Scorecard on October 1, 2024, which was jointly developed in collaboration with the National Industrial Security Program Policy Advisory Committee (NISPPAC) Industry Working Group.

DCSA has monitored implementation closely since October 1. Initial analysis indicates:

- There have been no major implementation challenges thus far.
- The Security Rating Scorecard successfully addresses industry requests for greater clarity, consistency, and transparency.
- There is an overall increase in superior and commendable ratings compared to Fiscal Year (FY) 2024 averages. This increase was expected and is due to the Security Rating Scorecard decoupling the final rating from the lowest category rating used under the previous model, resulting in fairer and more balanced whole-of-company ratings.

Feedback from our government stakeholders and industry partners has been overwhelmingly positive thus far. We attribute this to the unprecedented partnership between DCSA and industry when developing, piloting, and communicating this process. In the words of an industry partner, the Security Rating Scorecard "introduced a more objective, transparent, and risk-focused approach compared to the previous model, which often felt subjective and less tailored to specific needs. [It] allows for a clearer, more structured evaluation of a facility's security measures and emphasizes collaboration and solutions."

DCSA will continue to monitor implementation throughout FY 25. Successes, challenges, and unattributed feedback will be shared with the NISPPAC Industry Working Group during monthly meetings to help guide informed decisions on potential improvements.

DCSA is seeking your feedback related to Scorecard implementation. If you have feedback to share, send an email to the DCSA NISP Mission Performance Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

Visit the DCSA Security Review & Rating Process webpage to learn more about the Scorecard, download copies of important job aids, and access recorded webinars.

JOINT VENTURE FCL REQUIREMENTS PER DTM 24-004

In accordance with the authority in DoD Directive (DoDD) 5143.01 and Section 1629 of Public Law 116-92 (also known as "the National Defense Authorization Act for Fiscal Year 2020" and referred to in the DTM as "Section 1629"), Directive-Type Memorandum (DTM) 24-004, "Facility Security Clearance Requirements for Covered Joint Ventures," establishes policy, assigns responsibilities, and prescribes procedures for covered joint venture (JV) facility security clearances (FCLs) that meet the criteria in Section 1629 and supersedes guidance on the implementation of Section 1629 currently found in Paragraphs 4.3.a. and 4.8.c.(6) of Volume 1 of DoD Manual (DoDM) 5220.32.

DTM 24-004 requires compliance with all other FCL requirements in Volume 1 of DoDM 5220.32 not covered in the DTM and became effective July 19, 2024. The DTM will be incorporated into Volume 1 of DoDM 5220.32.

DTM 24-004 documents DCSA's role in processing JVs for FCLs. An FCL is not required for a "covered JV," which is defined as those in which all venturers maintain active FCLs granted by DCSA. If the JV is uncleared and one or more venturers do not hold FCLs, the JV is required to be sponsored for an FCL. JVs required to be sponsored for an FCL will submit the sponsorship package via NISS as usual. Entity Vetting will review the sponsorship and determine whether a JV is "covered" or not. The JV will need to submit their FCL package with the materials identified in the DTM. Due to NISS restrictions, JV FCLs cannot be currently verified via NISS and the JV will be assigned to the HQ field office.

NAESOC UPDATES

PREPARING FOR A REMOTE SECURITY REVIEW

Contractors under DCSA security cognizance must have a standard practice procedure (SPP) in place for implementation of SEAD 3 reporting requirements. This SPP must be available for review during all scheduled security reviews. Be sure to review yours and have it prepared for your remote security review. Minimum requirements that must be incorporated into the contractor's SPP may be found here.

REQUESTS SENT TO THE NAESOC

The NAESOC assigns priority to your request 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 2.9 RELEASE NEW FEATURES

New features from the 2.9 Release of the NISP Contracts Classification System (NCCS) include:

Acquisition Assist DD Form 254: This feature allows users to generate acquisition assist DD Form 254s for GCA routing, task orders, purchasing agreements and ordering agreements. This feature will be executable on existing DD Form 254s and will be generated in the same manner as a revision or final DD Form 254 would be. This feature has been highly requested by the user base, and it is now live for all Government Originators to utilize.

Sub DD Form 254 Routing: This feature enables the Sub DD Form 254 generated by an industry partner to be routed back to the respective government client for review and approval. The approval chain flows from industry reviewer to the appropriate government reviewer and certifier for action before routing back to the industry partner for certification and release. As a core function and requirement for some government clients, this feature is now live for all industry partners to utilize.

NISP PSI DATA COLLECTION TO OPEN IN NISS

DCSA is responsible for projecting Personnel Security Investigations (PSI) requirements each year. The data collection for PSI projection requirements will be open from March 3 to March 28 through the NISS Submission Site. More information will be provided on February 14.

OFFICE OF COUNTERINTELLIGENCE

FEBRUARY SVTC: USA SPENDING: A TARGETING TREASURE TROVE

DCSA invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) entitled, "USA Spending: A Targeting Treasure Trove." Analysts and agents from the Department of Commerce will brief concerns and potential risks caused by information posted on USA Spending. The SVTC is an in-person event to be held at most DCSA field offices on Thursday, February 13, 2025, from 1:00 p.m. to 2:30 p.m. ET.

Please register here for the SVTC.

ADJUDICATION AND VETTING SERVICES

RENAMING OF CAS AND VRO

DCSA Consolidated Adjudications Services (CAS) and Vetting Risk Operations (VRO) have united to form Adjudication and Vetting Services (AVS). AVS promises to deliver enhanced service offerings, improved response times, and optimized case management for our customers. Leadership is carefully managing the transition to ensure service continues without interruption.

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 Official (SMO) and FSOs worldwide. The AVS Call Center is available to answer phone and email inquiries from SMOs/FSOs, 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 (TW) 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 the Defense Information System for Security (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.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

JANUARY PULSE NOW AVAILABLE

CDSE recently released the Pulse, a monthly security awareness newsletter that features topics of interest to the security community. In addition, it shares upcoming courses, webinars, and conferences. The January newsletter focuses on "CDSE's 2024: A Year in Review." You can access all past newsletters in CDSE's Electronic Library. Subscribe or update your current subscription to get the newsletter sent directly to your inbox by submitting your email address through CDSE News.

INTRODUCTION TO SPECIAL ACCESS PROGRAMS (SAPs)

CDSE will be offering the Intro to SAPs course (SA101.01) in China Lake, CA from March 4-7 and Sunnyvale, CA from April 1-4. This course will provide entry-level SAP security professionals with the tools needed to implement DoD policies in their programs. Participants will learn about security enhancements such as the SAP nomination process, SAPF construction requirements, the Risk Management Framework, and other security aspects as outlined in DoD policy.

The course lasts three and a half days and is geared towards new U.S. Government SAP security professionals, whether they are civilian, contractors, or military personnel, as well as those in other federal agencies that work with DoD SAPs. Visit the course page to learn more and register.

ACTIVITY SECURITY MANAGER

Don't miss CDSE's upcoming "Activity Security Manager" course. This mid-level, virtual instructor-led course offers students with a comprehensive understanding of how to apply and implement specific DoD Information Security policies and procedures. It equips students to effectively mitigate and manage risks associated with developing, managing, and evaluating a DoD Information Security Program (ISP). Students can expect to invest 40 to 60 hours over a 4-week period in a primarily asynchronous environment. The course is designed for DoD civilian, military, and contractor personnel with primary duties as an activity security manager, an information security program specialist, or a manager within a DoD Component ISP. A functional working knowledge of the DoD ISP is recommended for participants.

Upon completion of the course, students will be able to implement the fundamental policies and requirements of the ISP, implement risk management to protect DoD assets, understand core cybersecurity and information technology principles, and more. The first iteration takes place February 2 to March 3. For more dates and information, visit the CDSE website.

PERSONNEL VETTING SEMINAR

CDSE is presenting the "Virtual Instructor-led Personnel Vetting Seminar" on February 4-5. 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 is intended for U.S. Government security professionals, military personnel, cleared industry FSOs, 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.

SECURITY PROFESSIONAL TW 2.0 GAP TRAINING RECORDING

In case you missed it, the TW 2.0 training is on demand! CDSE Personnel Vetting is pleased to announce the Security Professional TW 2.0 Gap Training Recording. This training is designed to help security practitioners understand the TW 2.0 framework and policy, the TW 2.0 implementation process, and how TW 2.0 affects your professional responsibilities. This 90-minute training targets DoD security practitioners, FSOs, and security staff members. A downloadable CDSE Certificate of Training is included. Visit here to learn more and register today!

ADVERSE INFORMATION REPORTING SECURITY SHORT

CDSE Personnel Vetting released a new security short, "Adverse Information Reporting." This short allows security practitioners to evaluate information and behaviors to determine if an incident report is appropriate and identify when and how adverse information should be reported. Click here to learn more and view the short today!

INDUSTRIAL SECURITY TRAINING ASSETS

NEW INDUSTRIAL SECURITY SHORT

The Industrial Security team released a new short, Security Incidents in the NISP. This short provides an overview of security incidents and the processes involved in reporting and investigating these incidents, including the key roles within the NISP that are responsible for processing security violation reports and conducting investigations.

UPDATED INDUSTRIAL SECURITY eLEARNING COURSE

The Industrial Security team released the new updated eLearning course, Personnel Clearances in the NISP IS142.16. This course includes a review of the regulatory basis for the Personnel Security Program (PSP) and the process to obtain a favorable national security eligibility determination, also referred to as a Personnel Security Clearance (PCL). The course also describes entity and individual responsibilities in the eligibility determination process, as well as the basic and common functions of the DoD Personnel Security System of Record.

UPDATED INDUSTRIAL SECURITY JOB AID

The Industrial Security team has released an updated Industrial Security Program Annual Planner for 2025. This job aid serves as a supplemental tool to help support and grow industrial security training and awareness within your organization. The job aid combines performance support tools from various security content areas that comprise the industrial security discipline that can be used to promote security awareness on a monthly basis throughout the year.

INDUSTRIAL SECURITY OVERSIGHT CREDENTIAL (ISOC)

The ISOC is ideal for DoD, industry, and federal members under the NISP.

The ISOC is ideal if a candidate:

- Occupies a full-time Industrial Security position for which obtaining this credential has been deemed a requirement or professional development milestone (i.e., ISR)
- Is performing Industrial Security functions as an additional or embedded duty.

OBTAIN ISOC

To obtain the ISOC, a candidate must submit an assessment request form through their Defense Acquisition University (DAU) account which will be verified by their customer service representative (CSR) before being approved to take the assessment. To be conferred for the ISOC, the candidate must successfully meet the credential assessment's qualifying score. There are no exceptions or waivers to these requirements.

MAINTAIN ISOC

To maintain ISOC, certificants must successfully complete and record 100 professional development units (PDUs), 50 of which must be security related, and submit their Certification Renewal Package (CRP) within their 2-year certification maintenance cycle.

THE CERTIFICATION RENEWAL PROGRAM

Obtaining a certification or credential is a significant achievement in a candidate's career. A certification or credential indicates the certificant possesses the knowledge and skills associated with the competencies necessary to successfully carry out DoD-defined security functional tasks.

The DoD has a professionalization goal of establishing a systematic approach for fostering learning and professional growth of the security workforce. Certification renewal is the long-term strategy for meeting this goal.

This approach allows the DoD, the DoD Security Training Council (DSTC), the Adjudicator Certification Governance Board (ACGB), and DCSA to meet both National Intelligence Strategy (NIS) Enterprise Objective (EO) 6 and USD(I&S) Human Capital Goals and Objectives for the security workforce. NIS EO 6 focuses on developing the workforce and strives to "attract, develop, and retain a diverse, results-focused, and high-performing workforce capable of providing the technical expertise and exceptional leadership necessary to address our Nation's security challenges."

The Certification Renewal Program supports certificants' ongoing educational and professional development. The PDUs requirement provides opportunity for certificants to enhance job-related skills and knowledge, as well as become familiar with new regulations and technological advances in related security areas to meet security objectives.

All submitted CRPs are subject to audit and review by Security Professional Education Development (SPēD) Program Management Office (PMO) personnel at any time within the 2-year renewal period. These audits assist in compliance verification and the integrity of certification maintenance standards as described below.

The purpose of the Certification Renewal Program is to:

- Enhance continuing subject matter competence
- Recognize and encourage learning opportunities
- Maintain and grow mastery-level knowledge of critical security skills
- Offer a standardized and objective mechanism for obtaining and recording professional development activities
- Sustain the global recognition and value of SPēD certifications and credentials.

FY 2025 UPCOMING COURSES

Interested in earning PDUs toward maintenance of 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 and eliminate travel expenses. Select courses have the American Council on Education (ACE) credit recommendations that can earn transfer credits at participating universities.

Classes fill quickly, so start planning now for your FY25 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)

- April 8 - 11, 2025 (Virtual)
- August 5 - 8, 2025 (Virtual)

INFORMATION SECURITY

Activity Security Manager VILT (IF203.10)

- February 2 - March 3, 2025 (Virtual)
- April 21 - May 18, 2025 (Virtual)
- July 28 - August 24, 2025 (Virtual)

INSIDER THREAT

Insider Threat Detection Analysis VILT (INT200.10)

- February 10 - 14, 2025 (Virtual)
- March 17 - 21, 2025 (Virtual)
- April 7 - 11, 2025 (Virtual)
- May 12 - 16, 2025 (Virtual)
- June 23 - 27, 2025 (Virtual)
- July 21 - 25, 2025 (Virtual)
- August 18 - 22, 2025 (Virtual)
- September 22 - 26, 2025 (Virtual)

PERSONNEL SECURITY

Personnel Vetting Seminar VILT (PS200.10)

- February 4 - 5, 2025 (Virtual)
- May 6 - 7, 2025 (Virtual)
- August 5 - 6, 2025 (Virtual)

PHYSICAL SECURITY

Physical Security and Asset Protection (PY201.01)

- April 21 - 25, 2025 (Linthicum, MD)
- August 18 - 22, 2025 (Linthicum, MD)

Physical Security and Asset Protection VILT (PY201.10)

- March 10 - 28, 2025 (Virtual)

SPECIAL ACCESS PROGRAMS

Introduction to Special Access Programs (SA101.01)

- March 4 - 7, 2025 (China Lake, CA)
- March 11 - 14, 2025 (Sunnyvale, CA)
- April 22 - 25, 2025 (Linthicum, MD)
- May 13 - 16, 2025 (Linthicum, MD)
- August 5 - 8, 2025 (Lexington, MA) (MIT)
- 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)

- February 19 - 20, 2025 (Linthicum, MD)
- August 11 - 12, 2025 (Lexington, MA)

SAP Mid-Level Security Management (SA201.01)

- July 14 - 18, 2025 (Linthicum, MD)

CDSE NEWS

CDSE offers an email subscriber news service to get the latest CDSE news, updates, and information. You may be receiving the Pulse through 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, National Industrial Security Program Operating Manual. 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.