DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

February 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

The NBIS Quarterly meeting was held on Tuesday, February 4, 2025, to serve as a primary source for comprehensive, verified NBIS updates. The meeting offered an opportunity for customer agencies and industry partners to receive information and updates on the program, pose questions, and provide feedback directly to NBIS and Personnel Security mission representatives.

Mr. Rob Schadey, Executive Program Manager for NBIS, opened the meeting by sharing the primary functions the NBIS team had been focused on over the past quarter, which included the Personnel Vetting Questionnaire (PVQ), the program's return to the execution phase, migration and modernization, and sustainment releases. Mr. Schadey introduced the first Minimum Viable Product (MVP) of the PVQ and reiterated the importance of the voice of the customer throughout development, stating that the priority is functionality for users. Mr. Schadey defined an MVP as an early version of a product that's used to test a concept and gather user feedback to learn and validate assumptions as early as possible.

The newly formed NBIS Service Level Management (SLM) team was introduced to the audience. Their mission is to ensure that the process of defining, monitoring, and maintaining service levels between DCSA and our customers is met. The SLM team will incorporate a change request intake process to ensure system requirements are collected, managed, and implemented.

DCSA's development team provided a demonstration of the updated PVQ to include new questioning, branching, and processing. The product presented was the first MVP of PVQ for non-DCSA Investigation Service Providers. This will not affect Cleared Industry. The form is still in development and was presented to obtain feedback and input from the meeting attendees, which was well-received.

The NBIS Quarterly meeting invitation is sent to an approved, appropriate distribution list, which includes federal and industry stakeholders. These meetings kicked off in October 2024 to provide key updates, show progress through the product roadmap, and present demonstrations when possible and appropriate. The next NBIS Quarterly meeting is expected to take place in early spring 2025.

NEW: SENIOR MANAGEMENT OFFICIAL SLICK SHEET

We are pleased to announce the availability of a new slick sheet for cleared contractors under DCSA cognizance that provides guidance related to Senior Management Official (SMO) duties, responsibilities, and appointments for single and multiple facility organizations.

While we encourage you to review the slick sheet in its entirety, a few highlights include:

- The SMO for the home office facility (HOF) is determined by a review of the legal entity's governance documents. This individual is a cleared employee who occupies a position within the legal entity with ultimate authority and accountability for the management and operations of the security program throughout the legal entity.

- The SMO for individual branch/division facilities is determined by contractor appointment. The contractor can choose to either appoint the HOF SMO as the branch/division SMO or may choose to appoint another cleared employee who has oversight of the classified work being performed at the branch/division facility. The appointed individual does not have to be physically located at the branch/division facility, nor do they have to be the senior most person assigned to the branch/division site.

- The SMO, whether at the HOF or branch/division, is designated in writing by being included on the Key Management Personnel (KMP) List. No appointment letter is required. The HOF SMO will only be listed on the branch/division KMP List if that individual is also identified as the branch/division SMO.

- The branch/division SMO will perform security related duties such as certifying the branch/division facility's annual self-inspection to DCSA.

A copy of the SMO Slick Sheet is located within the NISP Tools & Resources section of the DCSA website.

NEW: DISS MANAGEMENT JOB AID

We are pleased to announce the availability of a new job aid for cleared contractors under DCSA cognizance that provides guidance on how to annotate and maintain records for "break in access" and "break in employment" in the Defense Information System for Security (DISS).

While we encourage you to review the job aid in its entirety, a few highlights include:

- If a contractor employe no longer has a requirement to access classified information but remains employed by the contractor and the contractor determines there is a reasonable expectation that the employee will require access to classified information again in the future while employed by the contractor, the contractor is not required to remove the employee from DISS. However, the contractor must complete additional actions outlined in the job aid.

- If a contractor hires an employee with current eligibility, but the contractor has no reasonable expectation of granting access to the employee in the future, the contractor will not establish an affiliation with the employee's eligibility record in DISS.

- Contractors are authorized to establish/maintain an affiliation with employees' records in DISS for purposes other than access to classified information (e.g., base access, suitability for logical access to unclassified IT systems, positions of trust). However, the GCA is responsible for funding, submitting, and managing these types of investigations.

- Contractors must debrief cleared employees when there is no longer a reasonable expectation for the employee to access classified information. There is no policy requirement to obtain a signed debriefing nor are there specific elements that must be covered during the debriefing. As a best practice, DCSA encourages contractors to share the information from the SF 312 "debriefing" section.

A copy of the DISS Management Job Aid is located within the NISP Tools & Resources section of the DCSA website.

NAESOC UPDATES

PUBLISHED WEBINARS

The NAESOC recently published two webinars to the CDSE website. The first focuses on Facility Profile Updates and Changed Conditions packages. The second describes reporting obligations. Facilities assigned to the NAESOC are the target audience, but the information is valuable for all cleared facilities. If you would like to learn more about communicating changes and events at your facility, please click these links:

NAESOC - Changed Conditions and Facility Updates

NAESOC - Reporting Requirements

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 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

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.

NISP CONTRACTS CLASSIFICATION SYSTEM (NCCS)

NEW FEATURES FROM THE 2.9 RELEASE

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. It can be executed on existing DD Form 254s and is generated in the same manner as a revision or final DD Form 254. This highly requested feature 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 the industry reviewer to the appropriate government reviewer and certifier for action before routing back to the industry partner for certification and release. This core function and requirement for some government clients is now live for all industry partners to utilize.

IMPORTANT NOTICE: DUPLICATE EMAIL ISSUE

We are currently experiencing a duplicate email issue when users attempt to re-register. If you try to re-register and encounter this issue, please email the NCCS Support Inbox at dcsa.quantico.is.mbx.nccs-support@mail.mil. We will submit a ticket and work to resolve the issue as quickly as possible.

Thank you for your patience and continued support.

OFFICE OF COUNTERINTELLIGENCE

UNCLASSIFIED MARCH WEBINAR

The Department of Defense Cyber Crime Center (DC3) and DCSA have established a fully operational vulnerability disclosure program supporting the Defense Industrial Base (DIB). Following a successful pilot in 2022, which focused on delivering a DoD/DC3 vulnerability disclosure capability to the DIB, this strategic alignment has further enhanced DC3 and DCSA support to the DIB in the vulnerability, analytical, cybersecurity, and cyber forensics domains. Since late 2016, the DoD Vulnerability Disclosure Program (VDP) has crowdsourced more than 28,000 vulnerabilities on DoD external-facing information systems. The DIB-VDP was born out of the desire to bring lessons learned by the DoD VDP to DIB companies.

To learn more, DCSA invites cleared industry and academia personnel to participate in an unclassified webinar entitled, “DC3 Presents: Strengthening the DIB through the DC3 Vulnerability Disclosure Program (VDP): Information and Enrollment Session Update” on March 20, 2025 from 1:00 to 2:30 p.m. ET. This event is intended for all personnel including, but not limited to FSOs, executive officers, key management personnel, engineers, business development personnel, industrial security personnel, and cyber security professionals.

Please use this link to register for the webinar.

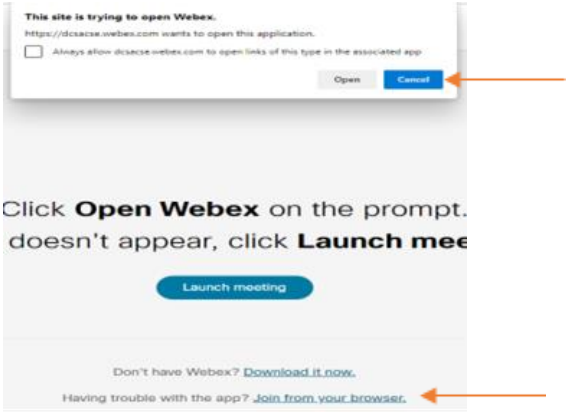
QUARTERLY INDUSTRY STAKEHOLDER ENGAGEMENT

The DCSA Customer & Stakeholder Engagement (CSE) team will host the next quarterly Industry Stakeholder Engagement (ISE) on March 18 from 10:30 a.m. to 12:00 p.m. ET for all Industry FSOs and Security Professionals. The last engagement, held on December 10, 2024, resulted in an outstanding attendance of over 300 FSOs and Industry Security Professionals. Last quarter's engagement focused on dangers of online gaming, foreign intelligence gathering, foreign contact reporting and the "How To's" for Cybersecurity Maturity Model Certification (CMMC) 2.0. The slide decks and Q&A for past engagements can be requested by e-mailing the DCSA Industry Liaisons at: dcsa.boyers.dcsa.mbx.industry-agency-liaison@mail.mil.

The March 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 Investigation (BI) – Industry Metrics and Updates
- Adjudication and Vetting Services (AVS) – AVS Updates
- NBIS Program Executive Office – NBIS Updates
- FCL Metrics and Processes
- Conclusion.

Note: When logging into Webex, please use your government/company email (vs. personal email) and First/Last name.



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

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.

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 SMOs 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)

FEBRUARY 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 February newsletter focuses on "CDSE's Continued Evolution and Changing Your Password." 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.

INDUSTRIAL SECURITY

Acronym Adventure Game

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

NISP Acronyms Job Aid

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

INSIDER THREAT

Insider Threat to Supply Chains Job Aid

Supply chain security is a crucial component of any organization that focuses on risk management of external suppliers, vendors, logistics, and transportation. It involves ensuring products are not tampered with or stolen during the production, storage, transportation, or delivery processes. What some organizations overlook are vulnerabilities of risks during these processes. Insider threat risks can be unintentional and may not always be malicious. For example, an insider threat risk may be caused by an employee unintentionally exposing information by disregarding protocols.

Organizations can be proactive in identifying and mitigating supply chain insider risks. The Insider Threat to Supply Chains Job Aid provides common supply chain insider threat examples, mitigation steps to identify potential risks, and best practices in preventing insider threat incidents. The job aid is also located in the Insider Threat Toolkit, under the Cyber Insider Threat/User Activity Monitoring category.

PERSONNEL SECURITY

Sensitive Compartmented Information (SCI) Security Refresher SC100.16

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

PHYSICAL SECURITY

ICD 705 Physical Security Construction Requirements for SAPs SA501.16

The CDSE SAP team has released a new version of the Intelligence Community Directive (ICD) 705 Physical Security Construction Requirements for SAPs. This updated course presents the basic skills required to

evaluate the ICD and SAP policies with regards to SAP facility construction. Due to the similarity in construction standards, this course can also be utilized as a foundation for those evaluating DoD sensitive compartmented information facilities. Course updates include an updated user interface and a more interactive virtual practical exercise as a final assessment. Visit the course page to learn more and take the course.

Introduction to Special Access Programs (SAPs) SA101.01

CDSE will be offering the Introduction 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, SAP facility 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.

FY 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 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)

- April 21 - May 18, 2025 (Virtual)
- July 28 - August 24, 2025 (Virtual)

INSIDER THREAT

Insider Threat Detection Analysis VILT (INT200.10)

- 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)

- 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)

- 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, 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.