DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

November 2024

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

DCSA'S NEW ROLE IN SUPPORTING DOD REFORM OF DUE PROCESS AND APPEALS

Effective December 8, DCSA will implement DOD reforms for security review proceedings in support of due process and appeals for military servicemembers, DOD civilians, and contractor personnel whose eligibility for access to Sensitive Compartmented Information (SCI) is adjudicated by DCSA.

The changes were directed by the Under Secretary of Defense for Intelligence and Security and are the result of an analysis of the DOD due process and appeals procedures.

Once the reforms are effective, individuals who receive Letters of Intent (LOI) to deny or revoke their eligibility for access to classified information or SCI will continue to have the opportunity to respond with written materials and will also be able to have a personal appearance with an adjudicator prior to a decision by DCSA on the denial or revocation action. Cleared contractor personnel who are adjudicated for collateral access eligibility (Confidential, Secret, Top Secret), are not affected by this change.

The reforms are the result of an ongoing effort to transform the Department's personnel security review processes for determining eligibility for access to classified information or to occupy a national security position. The goal is to make the process transparent, person-focused, and courteous.

For more information, visit www.dcsa.mil.

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

NBIS MODERNIZATION REACHES ACQUISITION MILESTONE

On the NBIS News page, you will find a link to a November 8 press release titled "NBIS modernization reaches acquisition milestone." The press release informs DCSA stakeholders of the October 18th signing of the Acquisition Decision Memorandum by Dr. William LaPlante, Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) and Decision Authority for the National Background Investigation Services (NBIS) program. This important milestone documents the way forward for the NBIS program and approves DCSA's plan for the NBIS digital transformation.

Please continue to check NBIS News for more updates and notices.

NBIS UPDATE 4.8

DCSA released NBIS version 4.8 on November 7. Specific release notes have been posted on NBIS News and STEPP.

SECURITY RATING SCORECARD IMPLEMENTATION

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. This initiative marks a significant milestone in the agency's Industrial Security oversight mission.

DCSA is committed to the successful implementation of the new Security Rating Scorecard. Throughout fiscal year 2025, the agency will monitor implementation and measure success through consistent application. 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.

Your voice matters! DCSA is seeking feedback related to Scorecard implementation from all stakeholders and partners. 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.

As a reminder, Industry can visit the DCSA Security Review & Rating Process webpage to learn more about the Scorecard, download copies of important job aids, and access the following CDSE recorded webinars:

- Session 1: Introduction to the Security Rating Score
- Session 2: Security Rating Criteria Requirements
- Session 3: Security Rating Score Tool and Resources

BLACK LABEL GSA CONTAINER PHASE-OUT

The phase-out of black label General Services Administration (GSA) containers began October 1, 2024. GSA determined that agencies must phase out all GSA-approved security containers and vault doors manufactured from 1954 through 1989 ("black labels") to store classified information and materials. GSA's detailed phase-out plan can be viewed in ISOO Notice 2021-01.

Disposal of GSA-approved security containers is left to the discretion of the agency, command, company security officer, or equivalent authority. The phase-out removes the authorization to use these containers to protect and store classified material but does not require disposal if the containers are used for an unclassified purpose. All containers must be decommissioned but may still be used for classified within an approved Open Storage Area because of the required security measures are already in-place.

BLACK LABEL CONTAINER USE AFTER DECOMMISSIONING

The container owner must do the following to continue use of a decommissioned black label container:

1. Thoroughly search to ensure all classified materials have been removed.
2. Remove all exterior GSA-approval black labels and interior certification and identification labels.

3. Place this notice on front of container, “No Longer GSA Approved (Standard File Cabinet Use Only).” (Order a magnetic sticker using Phase Out Sticker Request on the DoD Lock Program.)
4. Visit the website in the future for disposition guidance when the container is no longer needed.

BLACK LABEL CONTAINER DISPOSAL

The latest disposal guidance for black label containers from the General Services Administration, Interagency Advisory Committee on Security Equipment (GSA/IACSE) and DoD Lock Program is as follows:

1. Thoroughly search to ensure all classified materials have been removed.
2. Remove all exterior GSA-approval black labels and interior certification and identification labels.
3. Remove any “limited use” electromechanical combination locks. Destroy or return them to the U.S. Government in accordance with DoD Lock Program Security Equipment Disposal guidance.
4. Directly render the container to a steel recycling facility for destruction and steel reclamation.
5. Do not auction off or resell any intact decommissioned black label security equipment as it could be inappropriately resold, creating a security risk. This black label equipment end-of-service process must be followed to ensure supply chain integrity and protect classified information.

For specific questions or assistance, please contact the DoD Lock Program, Technical Support Hotline:
Toll-free: (800) 290-7607
DSN: 551-1212
Commercial: (805) 982-1212
Or Use the Technical Support Request Form

To purchase an approved replacement container, go to Ordering Security Containers | GSA.

NAESOC UPDATES

“Why did I get a NISS ‘Oversight Team Reassignment’ email?”

In 2024, many NAESOC facilities participated the Remote Security Review Pilot. Because of its success, and because the NAESOC mission continues to grow, more facilities will participate in Remote Security Reviews in 2025. Facilities selected for these security reviews are temporarily reassigned in NISS from the NAESOC to the ISR who will conduct that review. This reassignment triggers an automatic ‘Oversight Team Reassignment’ email from NISS. When the review is complete, an identical email is sent from NISS to signal the return of your facility to NAESOC oversight. If you receive this alert but your oversight team has not been re-assigned, it is possible that your CISA may have been re-assigned in NISS.

Important: For the entire time the facility is assigned, to either the ISR or the NAESOC, all Advise and Assist (A&A) actions and queries must be addressed by the currently assigned POC.

Best Practice: Check NISS and ensure you are aware of who your current oversight POC is prior to submitting an A&A query.

"Where did my ISR's name go in NISS?"

It has been identified that the "IS Rep" field in NISS occasionally reflects no name when your facility is assigned to the NAESOC. This system issue does not affect your oversight support, as NAESOC oversight is provided by a team of ISRs and security specialists. No action or query is needed under this condition.

Best Practice: If you have queries about who to contact for an ISR, please directly contact the NAESOC Help Desk:

(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

"When is the next NAESOC presentation on NCMSLive?"

Our next presentation, "Preparing for a Remote Security Review," will be on December 10.

NCCS: LOOK WHO'S ONBOARD! NEW USER NUMBERS

Adoption of the NISP Contract Classification System (NCCS), the enterprise-wide system for managing security classification specifications, continues to rise. With its user-friendly automated workflows, NCCS is an essential tool for both government agencies and industry partners. The platform simplifies the complex tasks of processing, distributing, and collecting NCCS specifications to ensure efficient and accurate handling of classified information.

The growing number of agencies and contractors onboarding to NCCS are experiencing the benefits of streamlined processes, reduced manual errors, and faster cycle times. The system's automated workflows have enhanced accuracy and efficiency, helping users stay on top of compliance requirements with ease.

As a reminder, all federal agencies bound by Federal Acquisition Regulation (FAR) 4.402 and all cleared contractors under the NISP are required to use NCCS for managing classified contract requirements.

The latest NCCS statistics as of November 15 highlight the continued growth of the NCCS community:

- 790 NCCS Government Users
- 178 NCCS Industry Users
- 1,264 Total DD Form 254s in the System

NISP CYBERSECURITY OFFICE

NISP EMASS QA EFFORT FOR NOT YET AUTHORIZED CLASSIFIED IS

The NISP Cybersecurity Office (NCSO) has initiated a quality assurance (QA) effort related to currently registered, classified information systems (IS), that remain Not Yet Authorized (NYA).

This QA effort specifically aims to address classified information systems IS that fit the below criteria:

1. Systems registered >365 days ago
2. Systems remain in a NYA-state
3. Systems have yet to be formally submitted for an authorization.

The QA effort addresses residual risk in industry by way of:

1. Reducing the overall number of classified IS in the NISP
2. Reducing system-specific artifacts within NISP eMASS
3. Ensuring that DCSA is only tracking valid system records.

NCSO is engaging industry and field personnel regarding systems that meet the above criteria and are removing systems from NISP eMASS that no longer intend to be submitted for an authorization.

If 3 months of targeted engagement with industry fails to return a response, NISP eMASS admins will administratively decommission the systems, which preserves the system records in the event the system needs to be recovered in the future.

Any questions related to the above QA effort can be sent to the NISP eMASS Help Desk by emailing: dcsa.quantico.dcsa.mbx.emass@mail.mil.

OFFICE OF COUNTERINTELLIGENCE

NCSC’S “SECURE INNOVATION” FOR EMERGING TECH COMPANIES

The National Counterintelligence & Security Center (NCSC) is excited to announce the release of *Secure Innovation* – shared security guidance to help protect emerging technology companies from a range of threats, particularly those from nation-state actors. This campaign, backed by the Five Eyes intelligence partnership, provides the tech sector with a set of cost-effective measures that companies can take from Day One to better protect their ideas, reputation, and future success.

Additional information is available in the press release at Five Eyes Launch Shared Security Advice Campaign for Tech Startups, and the U.S.-version of the guidance available on NCSC's Secure Innovation website.

NEXT SVTC: THE WEAPONIZATION OF ARTIFICIAL INTELLIGENCE

In consideration of the federal holidays scheduled in December, DCSA monthly Secure Video Teleconferences (SVTC) with cleared industry will resume on January 9, 2025.

DCSA invites cleared industry and academia personnel to participate in an SVTC titled "The Weaponization of Artificial Intelligence (AI)." A representative from the DCSA Counterintelligence Partnership with Cleared Industry (CIPCI) will discuss counterintelligence threats with AI in a classified forum. The SVTC is intended for cleared personnel including, but not limited to FSOs, executive officers, key management personnel, engineers, business development personnel, industrial security personnel, and cyber security professionals. The SVTC is an in-person event to be held at most DCSA field office locations on Thursday, January 9, 2025, from 1:00 p.m. to 2:30 p.m. ET.

Please register for the SVTC here.

NEXT WEBINAR: RESEARCH RELATIONSHIPS WITH CHINA

DCSA counterintelligence webinars will resume on January 16, 2025, with an unclassified presentation titled "DoD Bibliometric Study: Fundamental Research and Research Relationships with China."

QUARTERLY INDUSTRY STAKEHOLDER ENGAGEMENT

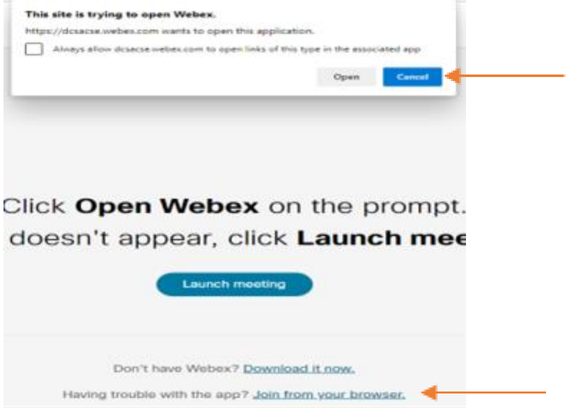
The DCSA Customer & Stakeholder Engagement (CSE) team will host the next quarterly Industry Stakeholder Engagement (ISE) on December 10 from 10:30 a.m. to 12:00 p.m. ET for all Industry FSOs and Security Professionals. The last engagement, held on September 26, resulted in an outstanding attendance of over 400 FSOs and Industry Security Professionals. Last quarter's engagement focused on a "Back to Basics" overview, highlighting the investigative process and some tips to assist the submission of investigations. The slide decks and Q&A for past ISEs can be requested by e-mailing the DCSA Industry Liaisons at: dcsa.boyers.dcsa.mbx.industry-agency-liaison@mail.mil.

The December 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
- Counterintelligence (CI) – Overview of information on the dangers of online gaming, foreign intelligence gathering, foreign contact reporting, etc.
- Masser Technologies – The How To's for CMMC 2.0
- 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.



This site is trying to open Webex.

https://dcsacse.webex.com wants to open this application.

□ Always allow dcsacse.webex.com to open links of this type in the associated app

Click **Open Webex** on the prompt.

doesn't appear, click **Launch mee**

Don't have Webex? Download it now.

Having trouble with the app? 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: 2818 882 2594

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.

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 (CV) 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.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NOVEMBER PULSE NOW AVAILABLE

CDSE recently released the CDSE 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 November newsletter focused on "Infrastructure Security and Resilience 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.

INSTRUCTOR-LED CYBERSECURITY COURSE AT CDSE IN DECEMBER

CDSE is offering an instructor-led course on Assessing Risk and Applying Security Controls to NISP Systems (CS301.01) in December. This course is tuition free and runs December 2-5 in Linthicum, MD. Students should have completed enrollment (prerequisites and registration) by November 15.

The target audience for this training includes Information System Security Managers (ISSMs), Information System Security Officers, and FSOs involved in the planning, management, and execution of security programs for cleared industry. This 5-day course provides students with guidance on applying policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the risk management framework process.

Go here to learn more and view the required prerequisites.

ACTIVITY SECURITY MANAGER COURSE

Don't miss CDSE's upcoming Activity Security Manager course. This mid-level, virtual, instructor-led course provides students with a comprehensive understanding of how to apply and implement specific DoD Information Security policies and procedures to mitigate and manage risks associated with developing, managing, and evaluating a DoD Information Security Program (ISP). Students are anticipated to invest 40-60 hours over 4 weeks in a mostly asynchronous environment. The course is tailored for DoD civilian, military, and contractor personnel with primary duties as an activity security manager, information security program specialist, or manager within a DoD Component ISP. Students should have a functional working knowledge of the DoD ISP.

After taking this course, students can expect to implement the fundamental policies and requirements of the ISP, implement risk management to protect DoD assets, determine fundamental cybersecurity and information technology principles, and more. The next iteration takes place February 2 through March 3, 2025. For more dates and information, check out the CDSE website.

NEW SPECIAL ACCESS PROGRAM (SAP) POLICY RELEASED

On September 12, 2024, the DoD released a new SAP policy with the DoD Directive 5205.07 and the DoD Instruction 5205.11 being signed. These two new policy documents incorporate the SAP Enterprise Reform memorandum that was signed July 11, 2023. The signing of these policies now paves the way for a new DoD Manual 5205.07 to incorporate these changes and provide a roadmap for SAP security specialists. The CDSE SAP team will begin reviewing their catalog of products to incorporate changes.

INSIDER THREAT DETECTION AND ANALYSIS COURSE

Insider threats are one of the biggest risks to national security. Learn the latest analytic techniques with CDSE's virtual instructor-led "Insider Threat Detection Analysis Course" (ITDAC) training. During this 5-day course, attendees will apply critical thinking skills and applicable structured analytic techniques to potential insider threat indicators.

This course also allows learners to obtain and use holistic data in conjunction with the application of critical pathway theory. Some prerequisites apply. The 2024 and 2025 course schedules are as follows:

December. 2-6, 2024 (Virtual)

January 13-17, 2025 (Virtual)

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)

Register here for the ITDAC course.

CDSE SPRING 2025 EDUCATION COURSES

Expand your knowledge with CDSE! Registration is now open for CDSE education courses for the Spring 2025 Spring Semester. The 16-week semester runs from January 20 to May 18, 2025. The courses are asynchronous, online, and tuition-free, and allow students the flexibility to collaborate with each other and instructors. Students can earn 160 professional development units by completing these courses. The CDSE Education Division also offers two 8-week courses: ED401.10, The Defense Security Enterprise: A National Security Enabler and ED203.10, Writing Incident Reports and Research Papers for DOD Security.

Enrollment fills quickly, so register early to secure a spot. Learn more and register via STEPP.

For any questions or additional information, contact the CDSE Education Division at: dss.ncr.dss-cdse.mbx.cdse-education@mail.mil.

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 to receive:

- The Pulse
- Insider Threat Bulletins

SOCIAL MEDIA

Connect with us on social media!

DCSA X (formerly known as Twitter): @DCSAgov	CDSE X (formerly known as Twitter): @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 Title 32 of the Code of Federal Regulations (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 a Facility Clearance (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 Senior Management Official certifies the self-inspection and that it is annotated as complete in NISS.