



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY

DCSA MONTHLY
NEWSLETTER

December 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

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)	2
IMPORTANT MILESTONE FOR EAPP	2
NBIS TRAINING RESOURCES	2
SECURITY RATING SCORECARD IMPLEMENTATION	3
NAESOC UPDATES	3
TEMPORARY REASSIGNMENT IN NISS	3
REQUESTS SENT TO THE NAESOC	4
OFFICE OF COUNTERINTELLIGENCE	4
JANUARY SVTC: CONCERNS WITH UNMANNED SYSTEMS (UXS)	4
JANUARY WEBINAR: RESEARCH RELATIONSHIPS WITH CHINA	4
ADJUDICATION AND VETTING SERVICES	5
RENAMING OF CAS AND VRO	5
AVS CALL CENTER NUMBER	5
CONTINUOUS VETTING ENROLLMENT BEGINS FOR NSPT	5
CONDITIONAL ELIGIBILITY DETERMINATIONS	6
SF 312 JOB AID	6
REMINDER ON TIMING OF ELECTRONIC FINGERPRINT TRANSMISSION	6
CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)	6
DECEMBER PULSE NOW AVAILABLE	6
ACTIVITY SECURITY MANAGER COURSE	7
INSIDER THREAT DETECTION AND ANALYSIS COURSE	7
CDSE SPRING 2025 EDUCATION COURSES	8
CDSE EARNING CONTENT CONTROLLER TEAM RECEIVES INNOVATION AWARD	8
NEW INDUSTRIAL SECURITY SHORT	8
UPDATED INDUSTRIAL SECURITY EARNING COURSE	8
NEW INDUSTRIAL SECURITY POSTERS	8
NEW INDUSTRIAL SECURITY GAMES	9
NEW SPECIAL ACCESS PROGRAM (SAP) POLICY RELEASED	9
CDSE NEWS	9
SOCIAL MEDIA	9
REMINDERS	9
DO NOT SEARCH FOR CLASSIFIED IN THE PUBLIC DOMAIN	9
FACILITIES MAY ADVERTISE EMPLOYEE POSITION PCLS	10
NISP CHECKUP	10



NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

IMPORTANT MILESTONE FOR EAPP

On the [DCSA News](#) page, you will find a link to a December 3 press release titled "DCSA announces full transition to NBIS eApp for background investigation initiation." The press release informs DCSA stakeholders that all required customer agencies have transitioned to NBIS eApp (electronic application) for background investigation case initiation. This marks a significant milestone for the NBIS program and Trusted Workforce 2.0.

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

NBIS TRAINING RESOURCES

All NBIS training resources are available on the Security Training, Education, and Professional Portal ([STEPP](#)). Access to STEPP requires an account, and the site is accessible via a secure Smart Card Login. For any issues accessing STEPP, contact the STEPP Help Desk at 202-753-0845 (M-F 8:30 a.m. to 6:00 p.m. ET).

Once on the [STEPP NBIS Training Homepage](#), users will find a comprehensive training library which includes job aids, e-learning, video shorts, learner paths, and webinar recordings.

The Defense Information System for Security (DISS) JVS Training Modules are now located on STEPP. The DISS JVS Training Modules on the Security Awareness Hub will be decommissioned on December 31, 2024.

NBIS Training Updates:

- DISS job aids can be accessed on STEPP via the NBIS Training landing page.
- An updated version of Initiate, Review and Authorize (IRA) e-Learning has been posted to STEPP.
- Live "IRA webinars" are open for registration; log into STEPP for enrollment. You **MUST** select your date of attendance to complete your registration for the webinar.
- Check out the latest webinar recordings posted to STEPP, located in the webinar section of the NBIS Training Catalog:
 - Organization Management: Notifications
 - Affiliations and Access
 - A Day in The Life: NBIS for Security Managers.

Be on the lookout for the NBIS Training Newsletter, which is sent quarterly via email to all NBIS users. The newsletters can also be found on <https://www.dcsa.mil> under NBIS Training. For questions on NBIS Training, contact the NBIS Training Program at dcsa.quantico.nbis.mbx.training@mail.mil.



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](#)

NAESOC UPDATES

TEMPORARY REASSIGNMENT IN NISS

In 2024, many National Access Elsewhere Security Oversight Center (NAESOC) facilities participated in 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 will be 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 Counterintelligence Special Agent (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 assigned POC in NISS.

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



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

OFFICE OF COUNTERINTELLIGENCE

JANUARY SVTC: CONCERNS WITH UNMANNED SYSTEMS (UXS)

The previously scheduled January 2025 Secure Video Teleconferences (SVTC) on “The Weaponization of Artificial Intelligence (AI)” has been postponed. A new date will be advertised once determined.

DCSA invites cleared industry and academia personnel to participate in an SVTC titled “Concerns with Unmanned Systems (UXS).” A representative from the National Counterintelligence Task Force (NCITF) will brief concerns of UXS to national security interests, in particular Department of Defense (DoD) facilities and Defense Critical Infrastructure sites. There will also be a threat briefing for those attending the International Defence Exhibition and Conference 2025 (IDEX 2025) being held in Abu Dhabi, United Arab Emirates. 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.

Note: the SVTC topic and recent media reports about drones observed in upper New England are coincidental. The SVTC brief is NOT designed to address NE activity.

Please register [here](#) for the SVTC.

JANUARY 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.” Special Agents from the Department of Army Criminal Investigations Division, Special Investigations Field Office, will present a study regarding fundamental research relationships with China's defense research and industrial base. 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. The webinar will be held Thursday, January 16, from 1:00 p.m. to 2:30 p.m. ET.

Please register [here](#) for the webinar.

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 DCSAKAC@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.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

DECEMBER 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 December newsletter focused on “Safety Tips for Safe Travel.” 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](#).



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. It equips students to effectively mitigate and manage risks associated with developing, managing, and evaluating a DoD Information Security Program (ISP). Students are anticipated to invest 40 to 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](#).

INSIDER THREAT DETECTION AND ANALYSIS COURSE

The virtual instructor-led "Insider Threat Detection Analysis Course" (ITDAC) training for January has been cancelled. Secure your spot now for the next session starting February 10, 2025.

This 5-day course enables attendees to apply critical thinking skills and applicable structured analytic techniques to potential insider threat indicators. Participants will work with CDSE experts and obtain and use holistic data in conjunction with the application of critical pathway theory. Additionally, learners will be taught how to apply Executive Orders, OD, and Intelligence Community (IC) authorities in data gathering, receive instruction on constitutional and privacy rights, and will learn the processes for conducting and reporting response actions from intake of an initial potential threat to mitigation of the threat.

Prerequisites for the ITDAC have been updated to make the course more accessible. Effective immediately, candidates are no longer required to complete the Insider Threat Program Operations Personnel Curriculum INT311.CU or the Insider Threat Program Management Personnel Curriculum INT312.CU.

The 2025 course schedule is as follows:

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

Register for the ITDAC course and view the full list of prerequisites [here](#).



CDSE SPRING 2025 EDUCATION COURSES

CDSE's Education Division's (ED) Spring 2025 Semester courses are open for registration until January 20, 2025. CDSE ED offers advanced and graduate courses and post-baccalaureate certificate programs designed specifically to broaden DoD security specialists' knowledge and understanding of the security profession and prepare them for leadership positions and responsibilities. All courses are tuition-free and offered in a virtual instructor-led environment on STEPP. To participate in the CDSE Education Program, you must be a U.S. Government civilian employee or U.S. military service member with an updated STEPP account with a .gov or .mil email address listed in your profile. The Spring 2025 Semester begins on January 20, 2025.

Register now! To learn more, check out the [CDSE ED website](#) and [register on STEPP](#).

CDSE eLEARNING CONTENT CONTROLLER TEAM RECEIVES INNOVATION AWARD

CDSE's eLearning Content Controller (eCC) team was recently honored with The Federal Government Distance Learning Association's 2024 Innovation Award. The award recognizes the eCC team's hard work developing a distance-learning platform that works in concert with the organization's Learning Management System. Read more about the team and the prestigious award in the [full article](#).

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 incidents, including the key roles within the NISP that have the responsibility 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 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.

NEW INDUSTRIAL SECURITY POSTERS

The Industrial Security team released five new [security posters](#). Our posters are available for you to download and promote security awareness in the workplace.



NEW INDUSTRIAL SECURITY GAMES

The Industrial Security team released two new security awareness games to provide a quick and easy way to test your knowledge and encourage security awareness at your organization. Check out [Concentrated Jeopardy](#) and [Spot the Vulnerabilities](#).

NEW SPECIAL ACCESS PROGRAM (SAP) POLICY RELEASED

On September 12, 2024, the DoD released new SAP policies 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 on 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.

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 (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 SMO certifies the self-inspection and that it is annotated as complete in NISS.