DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

September 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)

NBIS INBOX CLOSING

Due to limited use, DCSA will be closing the Industry/Federal Onboarding mailbox (dcsa.meade.dcsa.mbx.nbis-pmo@mail.mil). An automatic reply has been implemented to redirect inquiries to one of our existing help desks.

For NBIS Industry/FSOs support, contact the Customer Engagements Team (CET) at 878-274-1765 or dcsa.ncr.nbis.mbx.contact-center@mail.mil.

For applicant support with eApp, contact the Applicant Knowledge Center (AKC) at 878-274-5091 or dcsa.boyers.dcsa.mbx.applicant-knowledge-center@mail.mil.

CET HOURS OF OPERATION

Effective September 30, the Customer Engagement Team will establish hours of operation from Monday through Friday between 6:00 a.m. to 5:00 p.m. ET. The Applicant Knowledge Center will operate during the same hours, effectively extending their availability by 30 minutes.

DCSA will update the NBIS website, applicant email messaging, and phone line greetings to notify our customers about this change.

NBIS UPDATES 4.7.2 AND 4.8

DCSA released NBIS release 4.7.2 on September 11. The release included several Initiate, Review, and Authorize (IRA) updates. Specific release notes are available on the NBIS News Page and the Security Training, Education, and Professionalization Portal (STEPP).

One important enhancement of the release is the Obligating Document Number (ODN), which is a billing code in the Financial Details section of the order form and a required field deployed in 4.7.2. Addition of the code requires NO ACTION for Cleared Industry as it relates to the ODN. The NBIS team worked with AVS (formally VRO) to add the correct ODN into the Order Form Templates, which are available to all Industry users in the NISP Contractor hierarchy in NBIS.

DCSA plans to release NBIS version 4.8 in late September/early October. Specific release notes will be available on the NBIS News Page and STEPP.

UPDATE ON THE NEW SF-328

On September 12, 2024, the updated Certificate Pertaining to Foreign Interests (SF-328) entered the Federal Register for its final 30-day public notice. This is the final step before the new SF-328 is officially approved for use. Once the 30-day period ends and the form receives final approval, the updated SF-328 will replace the previous version as the approved form used for recording foreign ownership, control or influence responses.

DCSA is updating NISS to align with the changes in the new SF-328. This update will ensure that NISS is ready to handle/contain the revised form and reflect all appropriate changes. DCSA expects the NISS update to happen soon following the forms final approval and will provide the exact date as soon as it is confirmed to provide industry with sufficient notice.

Until DCSA updates NISS with the new form, companies may continue using the previous version of the SF-328 (REV. 11/2018, expiration April 30, 2024) for any submissions. However, once NISS is updated to incorporate the new SF-328, all new submissions will be required to use the updated form. This applies to both initial or upgrade Facility Clearance (FCL) packages and changed condition packages. DCSA will not require any contractor that has an existing package under review to change their SF-328 to the new version once it launches.

For submissions made before the NISS update, it is strongly recommended you refer to the new SF-328 and its instructions as a guide when completing the older version of the form. This will help ensure you provide all required information, and the form is completed accurately, even if the old version is still being used.

After the 30-day public review period, the new SF-328 will be published and made available for download on both the DCSA website and the Washington Headquarters Services (WHS) document repository. DCSA will provide further updates as available.

SECURITY RATING SCORECARD IMPLEMENTATION

On June 10, DCSA announced the successful joint development of a Security Rating Scorecard in cooperation with the National Industrial Security Program Policy Advisory Committee (NISPPAC) national working group. The Scorecard, which will be implemented on October 1, incorporates a numeric security rating score and enhanced criteria definitions, as requested by industry. It does not change the way DCSA conducts security reviews, rather, aims to minimize subjectivity, increase quality, and enhance clarity in the security rating process for all stakeholders.

To date, DCSA has conducted 21 internal training sessions ensuring industrial security field personnel are fully prepared to implement the Scorecard on October 1. Additionally, DCSA has conducted 18 external sessions attended by approximately 5,800 industry participants.

To learn more about the Security Rating Scorecard:

- Visit the DCSA Security Review and Rating Process webpage, future rating process tab, to access the Security Rating Process Slick Sheet, Security Rating Criteria Reference Card, Security Rating Score Tool, and other important resources.
- Review the following CDSE webinar recordings:
  - Introduction to the Security Rating Score
  - Security Rating Criteria Requirements
  - Security Rating Score Tool and Resources.

BLACK LABEL GSA CONTAINER PHASE-OUT

The planned phase-out by the General Services Administration (GSA) of black label GSA containers begins October 1, 2024. GSA has determined that agencies must phase out use of all GSA-approved security containers and vault doors manufactured from 1954 through 1989 ("black labels") to store classified information and materials. To begin this process, GSA has issued a detailed phase-out plan which 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 process is removing the authorization to use these containers for the protection and storage of classified material. It does not require them to be disposed of if the owner has other uses for them. There may be multiple uses for an unclassified reason such as to separate contract material, for access control purposes, or as a lockable filing cabinet. Additionally, decommissioned containers located in an approved Open Storage Area may continue to be used for the same reasons for both unclassified and classified material. The protection of classified material is provided by the security measures incorporated into the Open Storage Area.

BLACK LABEL CONTAINER USE AFTER DECOMMISSIONING

If the container owner decides to continue the use of a decommissioned container, the following actions must be taken:

1. The old black label security containers and cabinets should be thoroughly searched to ensure all classified materials have been removed before disposal.

2. The exterior GSA-approval label with black lettering, and the interior certification and identification labels, must all be removed.

3. And, a notice must be placed on front of container stating, "Not Authorized For Storage Of Classified Material." The DoD Lock Program will have magnetic labels available soon, so check their website site for updated information on availability.

Follow current disposition guidance if in the future the container is no longer needed, and disposition/disposal is then required.

BLACK LABEL CONTAINER DISPOSAL

Follow the latest disposal guidance from the General Services Administration, Interagency Advisory Committee on Security Equipment (GSA/IACSE) and DoD Lock Program.

Black label security equipment disposal is as follows:

1. The old black label security containers and cabinets should be thoroughly searched to ensure all classified materials have been removed before disposal.

2. The exterior GSA-approval label with black lettering, and the interior certification and identification labels, must all be removed.

3. Any "limited use" electromechanical combination locks should be removed and destroyed or returned to the U.S. Government. Follow the guidance for the disposition of the electromechanical mounted combination locks that are required to be returned or destroyed. Refer to the DoD Lock Program website at: Security Equipment Disposal.

4. The black label security equipment should be directly rendered to a steel recycling facility for destruction and reclamation.

5. Black label security equipment and limited-use electromechanical combination locks must not be auctioned off or resold intact as they may end up being refurbished and inappropriately resold to the U.S. Government or its contractors which creates a security risk in the supply chain. The future protection of classified information requires that these supply chain security measures be utilized in the end of service process for black label security equipment.

If you have specific questions or need assistance, please contact:
The DoD Lock Program, Technical Support Hotline:
Toll-free: (800) 290-7607
DSN: 551-1212
Commercial: (805) 982-1212
Email: Technical Support Hotline.

If you need to purchase an approved replacement container, go to Ordering Security Containers | GSA for more information.

NAESOC ENHANCEMENTS 2025

As its mission and support capability grows into Fiscal Year 2025, the National Access Elsewhere Security Oversight Center (NAESOC) is leveraging and updating technology to support oversight for its assigned population:

- NAESOC now has a direct-call phone line at **(878) 274-1800**. Queries can be made directly to the NAESOC rather than using the legacy call tree. Additionally, you can immediately select, "Send Voicemail" when you call to maximize efficiency. The legacy call tree also remains available for your convenience at (888) 282-7682, Option 7.

- The NAESOC website has been updated. Content has been added based on your queries and requests. Shortcuts to the website, as well as NAESOC Resources, have been added to left of the page to access content quickly.

Our Help Desk hours for Live Questions are:
Monday through Thursday - 9:00 a.m. to 3:00 p.m. ET
Friday - 8:00 a.m. to 2:00 p.m. ET

You can also reach us via e-mail at dcsa.naesoc.generalmailbox@mail.mil or NISS message.

SAM.GOV PROCESSING TIMELINES

DCSA is aware of delays in processing timelines and documentation issues associated with the System for Award Management website (SAM.gov). Field personnel have encountered past-due registrations and outdated information associated with cleared facilities. Facility actions should not be delayed if the facility has provided documentation to DCSA proving they have submitted requests for changes or other required information through SAM.gov or other instructions per the Federal Service Desk guide. These delays have received Congressional interest. Please coordinate through your region if you have additional questions or concerns.

NCCS TRAINING MATERIALS

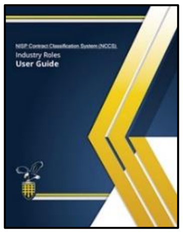
NCCS training materials are available at this link to help you and your team get the most out of the system: www.dcsa.mil/is/nccs/training.

Whether you're just getting started or need a quick refresher, we've got you covered with a range of resources tailored to different user needs.

Gaining Access Video
An overview on how to gain access to the hosting platform and register to start using the application quickly and easily.

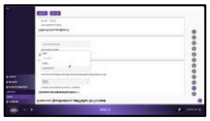
Quick Start Guide
Perfect for beginners, this guide provides an overview to get you up and running in no time.

Gov/Industry Role Slick Sheets
Learn the specific responsibilities and functionalities for each role within the system to maximize efficiency.



NISP Contract Classification System (NCCS)
Industry Roles
User Guide

Gov/Industry User Guides
This step-by-step manual guides users through the process of creating, reviewing, and certifying an accurate subcontract DD Form 254.



Webinars
Watch the interface in action and follow along to navigate through the system and perform specific functions.

We are here to support you every step of the way. If you have any questions, don't hesitate to reach out at dcsa.quantico.is.mbx.nccs@mail.mil. Our team is always here to help our partners.

COUNTERINTELLIGENCE SVTC

DCSA invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) entitled, "Conferences, Conventions, and Tradeshows (CCTs)." On Thursday, October 10, 2024, agents from DCSA and Army Counterintelligence will discuss counterintelligence threats at CCTs, to include the 2024 Association of U.S. Army (AUSA) Exposition, which is scheduled for October 14-16, 2024, in Washington, DC. 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 and will be held October 10, from 1:00 to 2:30 p.m. ET at most DCSA field office locations. Please register here.

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.

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.

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.

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)

SEPTEMBER 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 September newsletter focused on “Insider Threat Awareness.” 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, register, and view the required prerequisites.

PERSONNEL VETTING SEMINAR

CDSE is presenting the Virtual-led Personnel Vetting Seminar on November 19-21. This seminar will address the requirements associated with the reform of the Federal Government's personnel vetting system, which is known as Trusted Workforce 2.0 (TW 2.0). Its purpose is 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 provide support through the implementation process. The seminar covers topics such as end-to-end personnel vetting operations to include the federal background investigations program, National Security Adjudications, Continuous Vetting, and Insider Threat analysis in a collaborative environment.

This 3.5-day course is intended for U.S. Government security professionals, military personnel, cleared industry FSOs, and other federal personnel performing personnel vetting security-related duties, as well as personnel executing security programs for cleared industry. Visit the course page to learn more and register.

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 four 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 so much more. The first iteration takes place October 21 through November 17. For more dates and information, check out the CDSE website.

PHYSICAL SECURITY AND ASSET PROTECTION COURSE

There are still seats available for CDSE's "Physical Security and Asset Protection" instructor-led course October 21-25. This course provides students the ability to identify and utilize regulatory guidance, methodologies, and concepts for protecting DoD assets. This course is tailored for DoD civilian and military personnel, as well as contractors involved in the planning and management of physical security programs. For more information, click here.

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:

October 21-25, 2024 (Virtual)

November 18-22, 2024 (Virtual)

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.

TW 2.0 OVERVIEW FOR NATIONAL SECURITY ADJUDICATORS

CDSE is presenting the Trusted Workforce (TW) 2.0 Overview for National Security Adjudicators on October 22, 2024, from 10:00 a.m. to 12:00 p.m. ET. This Virtual Instructor-Led Training (VILT) will cover the changes and reforms driven by TW 2.0 that impact National Security trust determinations. These Federal Personnel Vetting (FPV) reforms aim to better support agencies' missions by reducing the time required to bring new hires on-board, enabling mobility of the federal workforce, and improving insight into workforce behaviors. This webinar contains exercises in identifying and defining the FPV Framework, the Adjudicative Process Framework, FPV Investigative Standards, Trust Determinations, FPV Scenarios, and Unconscious Bias.

This 2-hour virtual training is intended for DoD, DoD Intelligence Community (IC), and Non-DoD federal civilians who adjudicate national security eligibility for assignment to sensitive positions and/or access to collateral and Sensitive Compartmented Information (SCI) program information. Visit the course page to learn more and register.

THE SECURITY TRIANGLE COURSE

CDSE's Education Program released its newest virtual instructor-led course, ED402, The Security Triangle: Security, Law Enforcement (LE), and Intelligence. It focuses on the three components of the security triangle. Through the review of case studies, this course explores how the DoD security professional collaborates with and supports Law Enforcement (LE) and intelligence communities to prevent future security failures. This new 8-week course runs between October 14 and December 15 and is open to all federal civilians and military personnel (active and reserve) with or without an undergraduate degree. The course is unavailable to contractors. Students will receive 80 professional development units (PDUs) upon successful completion. Visit the course webpage to learn more and the Security Training, Education, and Professionalization Portal to register.

NEW SPECIAL ACCESS PROGRAM (SAP) POLICY RELEASED

On September 12, 2024, the DoD released a new SAP policy with the DoDD 5205.07 and the DoDI 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 DoDM 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 to receive:

- The Pulse
- Insider Threat Bulletins
- The Flash.

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

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."

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.

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.

DCSA ORGANIZATION NAME CHANGES

Organization (Old)	Organization (New)
Entity Vetting	Entity Vetting
Facility Clearance Branch (FCB)	Verification and Triage Unit (VTU)
Business Analysis Unit (BAU)	Due Diligence Unit (DDU)
Mitigation Strategy Unit (MSU)	Risk Management Unit (RMU)
NISP Authorization Office (NAO)	NISP Cybersecurity Office (NCSO)
Command Cyber Readiness Inspection (CCRI)	Cyber Operational Readiness Assessment (CORA)
Programs, Plans and Strategy (PPS)	Industrial Security Technologies and Strategy (ISTS)
Operations Division (Ops)	NISP Mission Performance (NMP)
Operations Branch	Mission Branch
Consolidated Adjudications Services (CAS) and Vetting Risk Operations (VRO)	Adjudication and Vetting Services (AVS)