DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

October 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
QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS UPDATE PENDING 2
NBIS UPDATE 4.8 2
eAPP REPLACES eQIP PER RELEASE OF ISL 2024-02 2
COUNTERINTELLIGENCE WEBINAR 2
SECURITY RATING SCORECARD IMPLEMENTATION 3
BLACK LABEL GSA CONTAINER PHASE-OUT 3
BLACK LABEL CONTAINER USE AFTER DECOMMISSIONING 4
BLACK LABEL CONTAINER DISPOSAL 4
NISP CONTRACT CLASSIFICATION SYSTEM (NCCS) FAQS 5
NCCS FREQUENTLY ASKED QUESTIONS 5
NAESOC PRESENTATIONS AND CONTACT 6
ADJUDICATION AND VETTING SERVICES 7
RENAMING OF CAS AND VRO 7
AVS CALL CENTER NUMBER 7
CONTINUOUS VETTING ENROLLMENT BEGINS FOR NSPT 7
CONDITIONAL ELIGIBILITY DETERMINATIONS 7
SF-312 JOB AID 8
REMINDER ON TIMING OF ELECTRONIC FINGERPRINT TRANSMISSION 8
CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) 8
OCTOBER PULSE NOW AVAILABLE 8
INSTRUCTOR-LED CYBERSECURITY COURSE AT CDSE IN DECEMBER 8
PERSONNEL VETTING SEMINAR 9
ACTIVITY SECURITY MANAGER COURSE 9
NEW SPECIAL ACCESS PROGRAM (SAP) POLICY RELEASED 9
INSIDER THREAT DETECTION AND ANALYSIS COURSE 10
CDSE NEWS 10
SOCIAL MEDIA 10
REMINDERS 11
FACILITIES MAY ADVERTISE EMPLOYEE POSITION PCLS 11
DO NOT SEARCH FOR CLASSIFIED IN THE PUBLIC DOMAIN 11
NISP CHECKUP 11
DCSA ORGANIZATION NAME CHANGES 11

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS UPDATE PENDING

DCSA has been tasked with updating the electronic version of the 2020 Standard Form 86 (SF 86), Questionnaire for National Security Positions, to remove the instructions indicating that a security freeze on an individual's consumer or credit report files should be lifted. The requirement to remove this verbiage from the standard form was issued by the Office of Management and Budget (OMB), OMB No. 3206-0005.

A PDF copy of the February 2024 SF 86 can be located on OMB's website which illustrates the draft change to remove the opening instructions on the Fair Credit Reporting Disclosure and Authorization signature page.

DCSA is currently developing system planning for implementation of the updated SF 86 and will notify customers with deployment dates and materials as they are available.

NBIS UPDATE 4.8

DCSA plans to release NBIS version 4.8 in November. Specific release notes will be available on the NBIS News Page and STEPP.

eAPP REPLACES eQIP PER RELEASE OF ISL 2024-02

DCSA has released Industrial Security Letter (ISL 2024-02), "National Background Investigation Services (NBIS) Electronic Application (eApp)," which notifies cleared industry under DoD cognizance that eAPP has become the successor system to eQIP for the submission of the SF 86 as provided for in NISPOM Section 32 CFR 117.10(d) which directs the SF 86 to be completed in eQIP or its successor system. Information on eAPP can may be found at National Background Investigation Services(NBIS). The ISL can be viewed here.

COUNTERINTELLIGENCE WEBINAR

DCSA invites cleared industry and academia personnel to participate in an unclassified webinar entitled, "Targeting U.S. technologies: A report of Threats to Cleared Industry." On Thursday, November 21, 2024, DCSA counterintelligence analysts will provide an unclassified presentation on the latest unclassified report, usually referred to as the "Trends." 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 November 21, from 1:00 to 2:30 p.m. ET. Please register here.

SECURITY RATING SCORECARD IMPLEMENTATION

Earlier this month, DCSA announced the full implementation of the Security Rating Scorecard, effective October 1, 2024. This initiative marks a significant milestone in the agency's Industrial Security oversight mission.

DCSA successfully developed the Security Rating Scorecard in collaboration with the National Industrial Security Program Policy Advisory Committee (NISPPAC) Industry Working Group. This Scorecard introduces a numeric security rating score and enhanced criteria definitions, addressing industry requests for greater clarity and consistency. Importantly, it does not alter the existing security review process but aims to reduce subjectivity, improve quality, and enhance transparency for all stakeholders.

To ensure a smooth transition, DCSA launched a comprehensive communication and training plan, preparing all stakeholders for the Scorecard's implementation on October 1. This initiative included numerous training sessions, website updates, monthly articles in the Voice of Industry newsletter, and social media postings. To date, the DCSA NISP Mission Performance Division has provided Scorecard training to approximately 6,500 industry participants with numerous training events scheduled for November.

Industry can visit the DCSA Security Review and Rating Process webpage to learn more about the Scorecard and are encouraged to contact their assigned Industrial Security Representative for any questions. Additionally, the following CDSE webinar recordings are available for review:

- Introduction to the Security Rating Score
- Security Rating Criteria Requirements
- Security Rating Score Tool and Resources.

DCSA is committed to the successful implementation of the new Security Rating Scorecard and consistent security site reviews for industry. Throughout fiscal year 2025, the agency will focus on project monitoring and analysis, measuring success through consistent application. Feedback from all stakeholders will be collected and shared in an unattributed manner with the NISPPAC Industry Working Group. This feedback will provide valuable insights for informed decisions on potential improvements. Stakeholders can submit feedback directly to the DCSA NISP Mission Performance Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

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, "No Longer GSA Approved (Standard File Cabinet Use Only)." Please see the Phase Out Sticker Request on the DoD Lock Program website to order a magnetic sticker.

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. Magnetic stickers to replace the black letter labels are available from the DoD Lock Program. It clarifies the use of the container by saying "No Longer GSA Approved (Standard File Cabinet Use Only)." Please see the Phase Out Sticker Request on the DoD Lock Program website for ordering details.

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.

NISP CONTRACT CLASSIFICATION SYSTEM (NCCS) FAQs

NCCS Notice: Due to contract turnover, we are currently experiencing delays in onboarding. Please allow up to 20 business days after submitting the DD Form 2875 (SAAR) before contacting the support box for assistance. We apologize for any inconvenience.

NCCS FREQUENTLY ASKED QUESTIONS

Why was my DD Form 2875 (SAAR) rejected?

Your SAAR may have been rejected for one of the following reasons:

- Scanned PDFs were submitted
- Wet signatures were included instead of valid digital signatures
- Invalid digital signatures were used
- Encrypted emails could not be opened
- Information was missing or incorrect
- Signatures were missing (the User (Part 1), Supervisor (Part 2), and Security Manager (Part 3) are required to sign for processing).

How can I check the status of my SAAR?

NCCS does not send notifications when a SAAR is processed successfully. Try accessing the system 3 to 5 days after submitting your SAAR. To check the status, simply go to the landing page and attempt to log in. If you are able to access the system, you may proceed with the registration steps.

Why am I receiving a "User not found" error after submitting my SAAR?

A "User not found" error often occurs if you are not using the same certificate that was used for the user signature on your SAAR. Please confirm that you are using the correct certificate. If the certificate is correct and it has been 5 business days since submission of the SAAR, please email us at dcsa.quantico.is.mbx.nccs@mail.mil for assistance.

What happens if I upload a Solicitation DD Form 254?

Uploading a Solicitation DD Form 254 will result in its direct release. If the solicitation requires additional checks or verification, the Solicitation DD Form 254 must be created in the application to be properly routed. Please avoid uploading Solicitation DD Form 254s that require additional approval or review.

Can I delete a DD Form 254 once it has been released?

A DD Form 254 cannot be deleted by the originator once it has been released. Deleting a released DD Form 254 can only be done by a specialized developer and may take some time depending on system maintenance schedules. Please ensure that all information on the DD Form 254 is accurate before releasing it to avoid delays.

NAESOC PRESENTATIONS AND CONTACT

For those who may have been unable to attend or missed the National Access Elsewhere Security Oversight Center (NAESOC) presentation on Changed Conditions Processing for NAESOC (Access Elsewhere) Facilities on NCMSLive on October 24, please know, as they become available, these same presentations are archived and available on the NAESOC web page.

The next NAESOC presentation on NCMSLive is scheduled for December 10. It will cover actions the FSO can take to prepare for a remote security review. Please be sure to attend if you can.

The NAESOC's Help Desk direct-call phone line is (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.

You can provide your questions via e-mail dcsa.naesoc.generalmailbox@mail.mil or NISS message.

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)

OCTOBER 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 October 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 instructor-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 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 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:

November 18-22, 2024 (Virtual)	May 12-16, 2025 (Virtual)
December. 2-6, 2024 (Virtual)	June 23-27, 2025 (Virtual)
January 13-17, 2025 (Virtual)	July 21-25, 2025 (Virtual)
February 10-14, 2025 (Virtual)	August 18-22, 2025 (Virtual)
March 17-21, 2025 (Virtual)	September 22-26, 2025 (Virtual)
April 7-11, 2025 (Virtual)	

Register here for the ITDAC course.

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

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)