DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

June 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)

UPDATE ON NBIS RECOVERY PLAN AND DIGITAL TRANSFORMATION

NBIS: We will get it done right.

DCSA has collaborated with the Office of the Under Secretary for Intelligence and Security; the Office of the Under Secretary for Acquisition and Sustainment; the Department of Defense Office of the Chief Information Officer to include the Chief Digital and Artificial Intelligence Officer, and the Defense Digital Services on coordinated recovery efforts to realign the NBIS program to execute development under the context of Trusted Workforce 2.0 requirements. The recovery planning period is ending, and movements are underway to usher in the NBIS program's digital transformation.

The NBIS program digital transformation roadmap enables a data driven vision for the future. NBIS' digital transformation will modernize code currently residing in multiple existing applications such as the Defense Information System for Security (DISS), which is familiar to and utilized by many of our customers. Once the roadmap is approved, we will leverage existing capital investments to accelerate NBIS technology delivery, reducing risk and increasing deployment of capability to mission owners. And to prepare customers for these changes, we will continue our ongoing outreach and communication efforts to inform and improve the customer experience.

The Electronic Application, known as eApp, will remain the entry point for applicants to submit investigation and continuous vetting requests. Until further notice, customers will continue to initiate cases through NBIS Agency and eApp interfaces.

The NBIS user experience is a priority. DCSA is committed to minimizing the impacts on the NBIS user community when we implement the digital transformation roadmap. The NBIS program will partner user experience professionals with mission owners to enable a better coupling of requirements to operationalize capability.

We encourage continued participation in our public user forums. Your input is crucial to the success of this program.

For additional NBIS resources and information, please visit www.dcsa.mil.

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, you'll find a comprehensive training library which includes job aids, e-learnings, video shorts, learner paths, and registration for live webinars.

NBIS Training Updates:

- A helpful desk reference on NBIS eApp Pre-fill can be found under the Additional Resources section. Select the tile titled "FAQs and Useful Tips" to find it. This document provides troubleshooting tips to assist users who are encountering challenges with pre-fill on their standard forms.
- DISS eLearning modules can now be accessed via the NBIS Training Catalog on STEPP.
- The I-R Guide for Industry has been updated and posted under the Industry Tools section on STEPP. This is a packet of job aids and an illustration with business rules on the I-R process.
- New Webinar Wednesdays—these shorter, 30 minute live webinars began in March. Topics are rotated on Wednesdays and are planned through mid-summer. See STEPP for topics and registration. These webinars will be recorded and posted to STEPP under the Webinar section.

Be on the lookout for the NBIS Training Newsletter, which is sent via email to all NBIS users. Current and previous newsletters can be found on www.dcsa.mil under NBIS Training. For questions about NBIS Training, contact the NBIS Training Program at dcsa.quantico.nbis.mbx.training@mail.mil.

SECURITY RATING PROCESS REFINEMENTS

DCSA is announcing the successful joint development of a Security Rating Scorecard in cooperation with the National Industrial Security Program Policy Advisory Committee (NISPPAC) national working group. This scorecard will not change any aspect of the current security review process and is expected to be implemented on October 1, 2024. These changes reflect DCSA's ongoing commitment to partner with industry to enhance clarity, fairness, and transparency within the security framework governing the NISP.

In May 2023, DCSA and industry partners initiated a project to refine its security rating process, emphasizing the agency's dedication to continuous improvement. These refinements are not a response to systemic errs, rather, they are a direct response to industry feedback on how the rating system delivers outcomes. The scorecard is designed to streamline and simplify the security rating process for all stakeholders. Starting October 1, 2024, the refined process will include the introduction of a numeric Security Rating Score (SRS) and enhanced criteria definitions to ensure consistent understanding and application based on DoD Manual 5220.32 Volume 1, "National Industrial Security Program: Industrial Security Procedures for Government Activities."

The refined system aims to minimize subjectivity, increase quality, and enhance clarity for all parties involved. DCSA will roll out comprehensive communication and training initiatives to ensure all stakeholders are well-informed about these changes. Detailed information and training materials will be available on the DCSA website.

The refined security rating process underscores DCSA's mission and capability to safeguard critical national security information (CNSI) through a streamlined approach which places compliance with 32 CFR Part 117 first. This approach should help enable a smooth transition for industry partners and stakeholders. DCSA aims to eliminate gaps or uncertainties, empowering stakeholders with a clear understanding and confidence in the updated security rating process.

UPDATED POLICY LINKS

On May 28, DCSA IS Policy updated links to the SEAD 3 Industrial Security Letter (ISL) 2021-02 and added the new link to the updated Worldwide Threat Assessment of the U.S. Intelligence Community document located here on the DCSA.mil website under Resources for SEAD 3 Unofficial Foreign Travel Reporting.

2024 COGSWELL AWARD RECIPIENTS

DCSA has recognized 14 facilities as recipients of the 2024 James S. Cogswell Outstanding Industrial Security Achievement Award. Chosen from nearly 12,500 cleared facilities in the United States, each facility has demonstrated industrial security excellence. To qualify, companies must establish and maintain a security program that exceeds basic NISP requirements. Recipients also help other cleared facilities establish security-related best practices while maintaining the highest security standards for their own facility. See the list of winning facilities here.

NISP CONTRACT CLASSIFICATION SYSTEM

What is NCCS?

The NISP Contract Classification System (NCCS) is the one-stop shop for processing, distributing, and collecting DoD Contract Security Classification Specifications (DD Form 254) for contracts that require access to classified information.

Why Use NCCS?

- Mandated by the Federal Acquisition Regulation (FAR) 4.402, NCCS is the federal enterprise information system for the DD Form 254 process for the Department of Defense and other federal agencies under NISP agreement, as well as for the cleared industry organizations that support them.

- NCCS improves efficiency by automating manual practices and removing paper from the DD Form 254 process. FAR 4.402 is the guiding policy for NCCS and will keep your agency or organization compliant.

- As the NCCS program matures, all mandated Government agencies will be onboarded and will exclusively use NCCS to manage all DD 254s in their portfolio. Because of this, Industry partners should proactively register and use NCCS to avoid gaps or delays in the DD Form 254 process.

Current Industry Users – As of the end of June, there are 107 user organizations across Industry.

NCCS Resources:

- NCCS Website
- NCCS Training Materials
- NCCS FAQs

BLACK LABEL GSA CONTAINERS

BLACK LABEL GSA CONTAINER PHASE OUT

The black label container phase out by the General Services Administration (GSA) begins October 1, 2024. Agencies and contractors must phase out the 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 which can be viewed in ISOO Notice 2021-01.

The phase-out plan rescinds approval over a period of four years beginning on October 1, 2024, with GSA Class 2 containers (filing cabinets, FedSpec AA-F-357). It starts with the oldest cabinets and proceeds to the last of the black labels. Before the dates listed in the notice, agencies/contractors must take actions to replace the containers and vault doors as needed.

It should be noted that GSA/IACSE Black Label Letter clarified that ISOO Notice 2021-01 applies to all GSA-approved black label containers regardless of the date of manufacture, and ISOO Notice 2022-03 extended the phase-out to October 1, 2035 for black label vault doors (Class 5 & 6, FedSpec AA-D-600).

If you need to purchase approved replacement containers, go to Ordering Security Containers | GSA for more information. As an option to purchasing through GSA, cleared contractors are authorized to purchase newer red label containers from other cleared contractors in accordance with FEDSTD-809E as long as two provisions are met:

- The transfer of the GSA-approved security containers can be securely accomplished (escorted movement).
- The security containers are inspected upon arrival within the accredited facility by a GSA Certified Inspector prior to the storage of classified information.

Agencies can easily identify the GSA-approved cabinets and vault doors produced prior to 1989 by the silver and black GSA approval label on the outside of the cabinet or vault door and by the certification labels and manufacturing dates located on the control drawer body or on the inside of the vault door. The containers should be destroyed/dispositioned in accordance with the appropriate destruction guidance for each entity.

If you have any additional questions or need assistance, please contact your assigned ISR.

INDUSTRY-OWNED BLACK LABEL GSA CONTAINER DISPOSITION GUIDANCE

For Industry-Owned Black Label security equipment disposal shall be 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 and interior certification and identification labels should be removed.
3. Any "limited-use" electromechanical combination locks should be removed and destroyed or returned to the U.S. Government.
4. The Black Label security equipment should be directly rendered to a steel recycle facility for destruction and reclamation.

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 creating a supply chain security risk.

The future protection of classified information requires that these supply chain security measures be utilized in the end-of-service process of Black Label security equipment.

BLACK LABEL GSA CONTAINER USE AFTER DECOMMISSIONING

Contractors may continue to use the decommissioned containers in multiple ways. Some FAQs include:

- Can a decommissioned Black Label container be used as a secure filing cabinet?
  - Yes, it can be kept and used as secure filing cabinet.
- What actions are to be taken to continue use?
  - Remove GSA certification label (i.e., the silver and black label on the front of the container)
  - Install "Not Authorized For Storage Of Classified" label on front face of container.
  - Remove the lock, destroy it locally, and send the disabled lock to a scrap metal recycling center.
- Can a decommissioned Black Label containers remain in an open storage area?
  - Yes, they can be used as secure filing cabinets to separate information for multiple programs.
- Are GSA-approved containers required in open storage areas?
  - No, an approved open storage area is considered a secure container, which allows for classified information to be openly stored. A contractor may use a decommissioned GSA-approved container as a locking filing cabinet to control access for multiple programs or contracts.

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.

UPDATE ON 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 identified here.

NEW 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.

NEW AVS CALL CENTER NUMBER

The AVS Call Center has a new phone number. The new number is 667-424-3850. The old 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.

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.

COUNTERINTELLIGENCE UNCLASSIFIED WEBINAR

DCSA invites cleared industry and academia personnel to participate in an unclassified webinar entitled, "The Weaponization of Artificial Intelligence (AI)." On Thursday, July 18, 2024, Mr. Steve Cook, Microsoft Risk Mitigation Program Manager, will provide an unclassified presentation on the use of AI by threat actors to target the defense 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 July 18, from 1:00 to 2:30 p.m. (ET). Please register here.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

LOOKING FOR A SECURITY BRIEFING?

Download the one you need. Just go to the NAESOC web page and tab over to the FSO Answers and Resources section. You can download approved, blank versions of the NATO, COMSEC, Critical Nuclear Weapon Design Information (CNWDI), and Controlled Cryptographic Information (CCI) briefings.

FIELD OFFICE ASSIGNMENT AND CONTACT

NAESOC facilities are scheduled to undergo security reviews. Your facility may receive NISS notifications supporting an update in the identification of the local DCSA field office and be temporarily reassigned to that field office. This supports the communication and task workflows within NISS during security review activities. NISS users should review their NISS profile to identify their current DCSA Field Office and ISR and directly contact them as appropriate. If you have any questions about who is providing your industrial security oversight or notifications you received from NISS, please feel free to contact us directly at the NAESOC Help Desk:

- Phone (888) 282-7682, Option 7
  Monday through Thursday - 9:00 a.m. to 3:00 p.m. ET
  Friday - 8:00 a.m. to 2:00 p.m. ET
- Or use NISS Messaging
- Or email dcsa.naesoc.generalmailbox@mail.mil

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

JULY PULSE NOW AVAILABLE

We recently released the CDSE Pulse, a monthly security awareness newsletter that features topics of interest to the security community. In addition, we share upcoming courses, webinars, and conferences. The July newsletter focused on "Personnel Vetting." 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.

NEW INDUSTRIAL SECURITY POSTERS NOW AVAILABLE

CDSE recently released new industrial security posters. Download and display the new and existing posters to enhance your organization's security awareness program. Here are a few of our latest posters:

Espionage is Not a Mirage

Vigilance is our Best Defense

Protecting Trade Secrets

Think Before You Sync

Print and post these and other posters to promote security awareness in the workplace!

GETTING STARTED SEMINAR FOR NEW FACILITY SECURITY OFFICERS (FSOs)

CDSE is hosting the virtual instructor-led Getting Started Seminar from August 20-23. This 4.5-day course allows new FSOs and security personnel the opportunity to learn and apply fundamental NISP requirements in a collaborative environment. It also serves as a refresher on industrial security basics for experienced FSOs. Areas of focus include the DD 254, Insider Threat, reporting requirements, counterintelligence, security and contractor reviews, security training and briefings, and personnel security. Learn more and sign up for this course to learn about the NISP requirements for FSOs.

INSTRUCTOR-LED CYBERSECURITY COURSE AT CDSE IN SEPTEMBER

CDSE is offering an instructor-led course on Assessing Risk and Applying Security Controls to NISP Systems (CS301.01) in September. This course is tuition free and runs September 9-13 in Linthicum, MD. Students should have completed enrollment (prerequisites and registration) by August 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.

UPCOMING WEBINARS

Sign-up is available for the following upcoming live webinars:

Corporal, Conspiracy, and Countertransference: Threat Management Challenges with a Domestic Terrorist
July 11, 2024
12:00 p.m. to 1:30 p.m. ET

The Weaponization of Artificial Intelligence
July 18, 2024
1:00 p.m. to 2:30 p.m. ET

Security Rating Score Criteria Requirements
July 30, 2024
1:00 p.m. to 2:30 p.m. ET

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, but if you were forwarded this newsletter from another source and 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

SAFEGUARD OUR MILITARY EXPERTISE

On June 5, The Office of the Director of National Intelligence's National Counterintelligence and Security Center (NCSC) joined partners from Australia, Canada, New Zealand, and the United Kingdom in warning about continued efforts by the People's Republic of China (PRC) to recruit current and former Western military personnel to train the PRC military.

"To overcome their shortcomings, China's People's Liberation Army (PLA) has been aggressively recruiting Western military talent to train their aviators, using private firms around the globe that conceal their PLA ties and offer recruits exorbitant salaries. Recent actions by Western governments have impacted these operations, but PLA recruitment efforts continue to evolve in response," said NCSC Director Michael C. Casey. "Today's joint bulletin by FVEY partners seeks to highlight this persistent threat and deter any current or former Western service members from actions that put their military colleagues at risk and erode our national security."

The joint bulletin provides information on this threat, as well as indicators, impact, mitigation, and where to report incidents.

FACILITIES MAY ADVERTISE EMPLOYEE POSITION PCLS

In accordance with Title 32 of the Code of Federal Regulations 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 REMINDER

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.

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)