DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

August 2025

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)

DCSA INVESTIGATIVE SYSTEMS TRAINING

The DCSA System Liaison Team is pleased to announce the expansion of its training offerings with the addition of three newly developed Investigative Systems Training classes, designed to enhance the knowledge and proficiency of individuals involved in personnel vetting processes. These virtual offerings include classes on the Defense Information System for Security (DISS) and NBIS for Industry.

For more detailed information about the Investigative Systems Training program, including course schedules, learning objectives, and registration instructions, please visit the Investigative Systems Training website.

Should you have any questions or require further clarification regarding the Investigative Systems Training program or any of the related system changes, please do not hesitate to contact us directly at DCSAAgencyTraining@mail.mil.

NEW PROCESS FOR OBTAINING ARCHIVAL COPIES

The Investigation Request functionality will be turned off in DISS to prepare the system for connecting to eApp and full IRA functional migration. While we work to re-establish a direct process for obtaining historical SF-86 Archival Copies, Industry users should contact the CET at 878-274-1765 or dcsa.ncr.nbis.mbx.contact-center@mail.mil.

New requests for background investigations or Continuous Vetting updates/enrollments will continue to be completed via NBIS.

NISS V2.7.3 - UPDATE ON SYSTEM LATENCY

The NISS Team deployed NISS v2.7.3 on July 27, 2025. Unfortunately, since the deployment, the system has been experiencing significant latency.

We understand that this system latency is impacting your work and productivity, and we sincerely apologize for any inconvenience this is causing.

We want to assure you that the NISS Team is actively investigating the root cause of this issue and working diligently to implement a solution as quickly as possible.

We appreciate your patience and cooperation as we work to resolve this issue and restore NISS to optimal performance. Updates will be forthcoming as applicable on our NISS Webpage.

Please call the Knowledge Center at 667-424-3903 to report any issues. If you are calling to report latency issues, please clearly state that you are reporting a NISS latency issue. This will help us prioritize your report and direct it to the appropriate support team.

Thank you for your understanding.

SECURITY REVIEW RATING RESULTS

The following security review results are current as of August 20, 2025:

Overall Fiscal Year Goal:	4,000	
Rated Security Reviews Completed:	3,978	(99.4%)
Rated Security Reviews Remaining:	22	(00.6%)
Superior Ratings Issued:	587	(14.7%)
Commendable Ratings Issued:	1,415	(35.6%)
Satisfactory Ratings Issued:	1,941	(48.8%)
Marginal Ratings Issued:	16	(00.4%)
Unsatisfactory Ratings Issued:	19	(00.5%)

Note: These results include both initial security review ratings and compliance review ratings. DCSA conducts a compliance review when a contractor receives marginal or unsatisfactory rating during a security review. Access the informational Compliance Reviews slick sheet to learn more.

DCSA FORM 147, JANUARY 2025 - IMPLEMENTATION

DCSA announced the 90-day transition period in July for the recently released DCSA Form 147, Open Storage Area and Vault Approval Checklist, dated January 2025. This revision significantly reduces the time required to complete the form, removes identified redundancies, and reduces the page count by more than half. The form's purpose remains the same: to provide a sufficient description of an approved open storage area and to encourage industry partners to transition older closed areas to current policy standards. The improvements are a direct result of feedback received from DCSA field personnel and industry security professionals. The revised form aligns with safeguarding requirements outlined in the Title 32 Code of Federal Regulations (32 CFR) Part 117, National Industrial Security Program Operating Manual (NISPOM) Section 117.15, Safeguarding Classified Information, and 32 CFR Part 2001.53, Open Storage Areas, construction requirements.

DCSA Form 147 is available for download at NISP Tools & Resources (under the Industry Tools FSO Forms dropdown). To facilitate a smooth transition, DCSA will implement a "soft-landing" approach from the April 2022 version to the current January 2025 version as follows:

- July 1, 2025 through September 30, 2025 (90-day grace period): Industry may submit either the April 2022 or the January 2025 version of DCSA Form 147.
- September 30, 2025: End of the 90-day transition period.
- Effective October 1, 2025: Only submit the January 2025 version of DCSA Form 147.
- October 1, 2027: Extended suspense date for submitting a new DCSA Form 147 to complete the transition of older closed areas previously approved on the obsolete one-page DCSA Form 147.

Important Notes

- Open storage areas and vaults approved using DCSA Form 147, April 2022 version, will remain valid.
- A closed area approved using the obsolete one-page DCSA Form 147 must be updated and documented as an "open storage area."
    - The deadline for this transition has been extended to October 1, 2027.
    - Industry must submit a new DCSA Form 147 to their assigned ISR to complete this transition for each approved space.

If you have any questions or need assistance, please contact HQ DCSA, NISP Mission Performance (NMP) Division at dcsa.quantico.dcsa.mbx.isd-operations@mail.mil.

OFFICE OF COUNTERINTELLIGENCE SVTC AND WEBINAR

SAFEGUARDING ACADEMIA

On August 25, the Office of the Director of National Intelligence's (ODNI) National Counterintelligence and Security Center (NCSC) issued a "Joint Seal Product" with DCSA Counterintelligence and seven other stakeholder community partners.

The Safeguarding Academia bulletin provides guidance to the U.S. academic community to promote a research ecosystem that balances openness, collaboration, integrity, fairness, responsibility, and security.

The companion Quick Reference Guide for Academic Institutions provides research administrators with information to guide informed decisions about potential risks and proactive measures to safeguard research, while preserving the values that foster academic advancement.

CLASSIFIED SEPTEMBER SVTC

DCSA invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) for the Defense Industrial Base entitled, "Defense Industrial Base Counterintelligence Threat Trends." DCSA counterintelligence analysts and agents will provide a classified presentation on the latest quarterly update of the DCSA annual report "Targeting U.S. Technologies: A Report of Threats to Cleared Industry."

The SVTC is an in-person event at most DCSA field offices on Thursday, September 11, 2025, from 1:00 to 2:30 p.m. ET. Please register for the SVTC here by September 4, 2025:

UNCLASSIFIED SEPTEMBER WEBINAR

DCSA invites cleared industry and academic professionals to an unclassified webinar on September 22, 2025, from 12:00 to 1:30 p.m. ET, entitled "Shadow Banking and Financial Fraud: Exploring North Korea's Fraud and Sanctions Evasion Schemes."

This webinar will feature a Certified Fraud Examiner who will discuss North Korea's sophisticated and large-scale fraud operations. The regime's illicit activities, fueled by a convergence of need, opportunity, and rationalization (the "fraud triangle"), rely on a network of domestic and international operatives to generate financing, evade sanctions, and move funds through the global financial system. Participants will gain insights into North Korea's covert methods, real-world examples of fraud, money laundering, and conspiracies, and identify relevant red flags and risk indicators across various business sectors.

Please register for the webinar here.

BLACK LABEL GSA CONTAINER PHASE-OUT

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

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

Black label containers to be phased out by October 1, 2025, are identified below. Please ensure any black label container is removed from service (i.e., cannot store classified material) by the indicated date.

GSA Class	FED Spec	Rev.	Years Produced	Years of Service	End of Service
2	AA-F-357	A- F	1954-1970	50-70	1 Oct 2024
3	AA-F-358	A- F	1956-1968	52-69	1 Oct 2025
4	AA-F-358	A- F	1956-1968	52-69	1 Oct 2025

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.

BLACK LABEL CONTAINER USE AFTER DECOMMISSIONING

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

1. Thoroughly search to ensure all classified materials have been removed.
2. Remove all exterior GSA-approval black labels and interior certification and identification labels.
3. Place this notice on front of container, "No Longer GSA Approved (Standard File Cabinet Use Only)." (Order a magnetic sticker using Phase Out Sticker Request on the DoD Lock Program website.)
4. Visit the website in the future for disposition guidance when the container is no longer needed.

BLACK LABEL CONTAINER DISPOSAL

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

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

For specific questions or assistance, please contact the DoD Lock Program, Technical Support Hotline:

Toll-free: (800) 290-7607

DSN: 551-1212

Commercial: (805) 982-1212

Or Use the Technical Support Request Form

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

NCCS MIGRATION TO NI2!

The NISP Contract Classification System (NCCS) has been selected as the next feature to be integrated into the National Industrial Security System Increment 2 (NI2) application. This migration supports DCSA's ongoing effort to streamline and enhance its industrial security offerings for government and industry partners.

Impact on Existing NCCS Users:

- Minimal impact is anticipated for current users.
- All existing users and data will be migrated automatically.
- No data re-creation will be necessary.
- System functionality is intended to remain like the current NCCS.
- The primary change for users will be navigating to a different web address.

Next Steps:

- Stay tuned for additional communications and details as they become available.
- Questions? Contact us at dcsa.quantico.is.mbx.nccs-support@mail.mil.

NAESOC UPDATES

WELCOME TO THE NAESOC!

For the numerous facilities that received an email or NISS notice in recent weeks informing you of your transfer to the National Access Elsewhere Security Oversight Center (NAESOC), we would like to extend an invitation to utilize the resources available at the NAESOC to enhance your security programs.

Here are additional tips that will help you make the most out of your time assigned to the NAESOC:

- Always Have Your CAGE Code Ready: Be sure to include it in the Subject Line of your email or introduce yourself with it when you call on the phone. That helps to ensure quick retrieval of your facility's history and helps us help you quicker.

- Prepare to Talk to an Expert: Although you may not talk to, or get an email from, the most recent person you last talked to at NAESOC, our trained and experienced Help Desk is your central point of contact for concerns, requirements, and issues. It will efficiently connect you with the most appropriate subject matter expert for your requirements.

- Check Out the Web Page First: We maintain a current library of Self-Help resources, including FAQs, Webexes developed especially for non-possessing facilities, and forms you may need for your security program. These all can be found on the NAESOC web page, and especially on the NAESOC Resources link. Please feel free to take some time and tour the entire site.

CONTACT US

Your best way to contact us:

- (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

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 for prioritized attention.

ADJUDICATION AND VETTING SERVICES (AVS)

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 soon.

As a reminder, the AVS Call Center will continue to provide direct support and timely adjudicative updates to Senior Management Officials (SMOs) 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 serve 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.

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 the investigation request is sent to the subject for completion. **Note:** this is an update to previous guidance that instructed FSOs to submit FPs at the same time the eApp is released to DCSA.

Fingerprint results are valid for 120 days, the same amount of time for which eApp signature pages are valid. Therefore, submitting electronic fingerprints 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

AUGUST PULSE NOW AVAILABLE

DCSA recently released the CDSE Pulse, a monthly security awareness newsletter that features topics of interest to the security community as well as upcoming courses, webinars, and conferences. The August newsletter focused on Antiterrorism Awareness Month. Check out all the newsletters in CDSE's Electronic Library or subscribe to have the newsletter sent directly to your inbox by signing up here.

INSIDER THREAT

National Insider Threat Awareness Month. This September marks the seventh annual NITAM, as well as an opportunity to elevate the overall security posture, strengthen insider threat programs, and ensure a trusted workforce.

For ideas on how to participate in the month-long campaign, check out the newly launched NITAM site, updated for 2025 with FAQs, events, and helpful resources including games, case studies, and items such as the Adventures of Earl Lee Indicator game and the DITMAC DOD Insider Threat Reporting Portal.

This year's theme, "Partnering for Progress," highlights the power of collaboration. By actively promoting teamwork and information sharing, organizations can significantly enhance their ability to detect, prevent, and respond to insider threats, ultimately creating a more secure and resilient environment

Insider Threat for Industry Curriculum. The "Insider Threat for Industry Curriculum" (INT333.CU) provides specialized training for insider threat program personnel working in cleared defense industries, including contractor-designated Insider Threat Program Senior Official (ITPSO). It is designed to equip students with the knowledge, skills, and abilities required to conduct their duties.

Executive Order 13587, National Minimum Standards for Insider Threat, and 32 CFR § 117 NISPOM mandate that "the designated ITPSO will ensure that contractor program personnel assigned insider Threat program responsibilities complete training consistent with applicable CSA provided guidance." Such training must include:

1. Counterintelligence and security fundamentals
2. Procedures for conducting insider threat response actions
3. Applicable laws and regulations regarding gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information
4. Legal, civil liberties, and privacy policies and requirements applicable to insider threat programs

This curriculum satisfies the 32 CFR § 117.12 (g)(1) requirements. Register for the course here.

E Learning Course Major Update: Establishing an Insider Threat Program for Your Organization INT122.16. The "Establishing an Insider Threat Program for Your Organization" (INT122) eLearning course is under revision with a planned release in November. The course provides insider threat program managers with practical guidance on developing compliant insider threat programs. The course presents scenarios and case studies of insider threat behaviors. Learners will explore the critical path model, regulatory standards, and key implementation steps to meet the minimum requirements of Executive Order 13587.

This course equips managers with knowledge and tools to establish insider threat programs that meet national standards. The goal is to help managers implement these programs effectively, ensuring compliance and reducing insider threat risks. This course is for individuals designated as organizational insider threat program managers, including both government and industry.

Coming Soon: Supervisor and Command Leader Awareness of Insider Risk. The "Supervisor and Command Leader Awareness of Insider Threat Risk" web-based training course provides supervisors, managers, and command leaders with an overview of concerning behaviors that lead to insider threats and the subsequent actions they can take to mitigate risk. The course, planned to release in September, presents scenarios and examples of insider threat behavior and informs leaders about how organizational culture, proactive engagement, and leadership actions play a role in risk mitigation. The purpose of this course is to provide supervisors and leaders with knowledge to support insider risk mitigation. The course incorporates recent updates to insider risk policies, procedures, and best practices. The goal of the course is to empower supervisors and leaders by providing information on the impact they have and the strategies they need to mitigate insider risk.

New Security Short: Human Resources and Insider Threat. This all-new short, which replaces the previous version of the same name, provides learners with an overview of the role human resources (HR) personnel play on an insider threat hub team and the importance of HR in mitigating insider threats. This training will give learners a better understanding of the HR 'pillar' during an insider threat investigation and provide learners with foundational knowledge applicable to insider threat hub activities.

The audience for this short includes HR personnel assigned with insider threat responsibilities, as well as industry or government personnel tasked with establishing a hub.

The short is structured as an interview with an experienced HR expert who serves as a member of an active insider threat hub team. Learners can choose questions from a list of frequently asked questions and hear real-world explanations and answers from an expert.

At the conclusion of this security short, learners should better understand the role HR personnel play in deterring, detecting, analyzing, and mitigating potential insider threats.

PHYSICAL SECURITY

Enhance Your Security Expertise: New Physical Security Training. Coming this fall, enhance your security expertise with the "Introduction to Physical Security (PY011.16)" course. The course will provide the tools and knowledge you need to learn how to apply security-in-depth principles and contribute to a stronger security posture. This eLearning course, geared toward DoD civilians, military personnel, and defense contractors, covers physical security planning, implementation, and countermeasures to deter, delay, detect, deny, and defend against attacks.

INDUSTRIAL SECURITY

Industrial Security New Summer Security Posters. Check out the four new security posters, including some with a summer theme, from the Industrial Security team.

SPECIAL ACCESS PROGRAMS (SAP)

SAP Accountability Officer Short. The SAP Accountability Officer Short covers the newly created SAP Accountability Officer role identified in the January 2025 DoDM 5205.07. The short outlines the responsibilities associated with being an SAP Accountability Officer and what the role entails.

View the short to learn more about the role at here.

FISCAL YEAR 2025 UPCOMING COURSES

CDSE instructor-led training (ILT) or virtual instructor-led training (VILT) courses are a great way to earn professional development units (PDUs).

Secure your spot now as classes fill quickly! Available ILT and VILT courses are listed below.

CYBERSECURITY

Assessing Risk and Applying Security Controls to NISP Systems (CS301.01)

- September 22 - 26, 2025 (Linthicum, MD)

SPECIAL ACCESS PROGRAMS

Introduction to Special Access Programs (SA101.01)

- September 9 - 12, 2025 (Rolling Meadows, IL) (NGC)

CDSE NEWS

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: @DCSAgov

CDSE X: @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 32 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 an 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, NISPOM. 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.