DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

July 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)

NBIS BRANDING

NBIS is a suite of information technology systems that support the end-to-end process for personnel vetting.

The front side of this process starts with the initiation of a background investigation and encompasses activities including the background investigation, adjudication, and continuous vetting processes.

DCSA is establishing a common lexicon and promoting awareness and understanding of the NBIS Suite of Applications to align with the PAC Shared Services catalog which can be located here on max.gov.

The NBIS Suite of Applications are as follows, with definitions:

Low Side Repository (LSR): The single repository for vetting information; currently referred to as "DISS-JVS" or "JVS"

Adjudication Management: Case management for adjudication and personnel vetting management; currently referred to as "DISS-CATS" or "CATS"

Personnel Vetting Management (PVM): Subject management activities; currently referred to as "DISS-JVS" or "JVS"

Continuous Vetting (CV): CV alerts/services; currently referred to as "Mirador"

Individual Engagement: This will be for individuals/subjects to self-report and provide information, respond to requests, and check their status for vetting related information; often referred to as "Subject Portal."

NEW SUPPORT MATERIALS

DCSA's communication team and the Personnel Vetting mission has been preparing expanded information on the DCSA website and on STEPP in August. To support NBIS Branding and the new terminology of systems, groups, and processes, the following materials will be made available to users:

- NBIS Branding Lexicon: The updated NBIS Branding lexicon will be presented to customers in a "Rosetta Stone" format which will translate previous systems/terms to the new products and platforms. We believe this will greatly aid customers as they perform the crosswalk from legacy technology to our modernized NBIS suite of products.

- Campaign Plans: One-pagers that outline specific activities and efforts (such as the Central Verification System (CVS) to the Low Side Repository (LSR) migration). These documents will outline the intent of the effort, along with key messages and customer requirements. They will also feature a breakdown of future communication activities, timeframes and the audience/ stakeholders involved.

- Marketing Documents: One to two-page documents that outline the key milestones and deliverables from the NBIS Roadmap and the PAC's Trusted Workforce 2.0's Implementation Strategy. Documents have been created for PVQ, CVS to LSR, PVM, IRA, and Adjudication Management. These documents outline our deliverables, definitions, and key capabilities and their importance and benefits (i.e. - what's in it for me?).

All these materials are under review now and are expected to be pushed out in August.

SECURITY REVIEW RATING RESULTS

The following security review results are current as of July 23, 2025:

Overall Fiscal Year Goal:	4,000	
Rated Security Reviews Completed:	3,597	(89.9%)
Rated Security Reviews Remaining:	403	(10.1%)
Superior Ratings Issued:	531	(14.8%)
Commendable Ratings Issued:	1,281	(35.6%)
Satisfactory Ratings Issued:	1,754	(48.7%)
Marginal Ratings Issued:	13	(00.4%)
Unsatisfactory Ratings Issued:	18	(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.

UPDATED SF 328 OVERVIEW AND IMPLEMENTATION

As a continued reminder, the updated Standard Form (SF) 328, "Certificate Pertaining to Foreign Interests," was approved on May 1, 2025, and includes several improvements to increase users' clarity and understanding of the questions and subsequent requirements. After extensive coordination and collaboration with Industry and other government stakeholders, the SF 328 was updated to include better-scoped questions, comprehensive instructions, definitions, and a Statement of Full Disclosure of Foreign Affiliations used to report foreign employment throughout the form. The updated SF 328 was deployed in NISS on May 12, 2025. Any packages initiated or submitted on or after May 12 are required to use the updated SF 328. DCSA published a two-page information paper highlighting key updates and the implementation plan provided to DCSA field elements; it can be viewed here on the DCSA website under Updates. For questions or assistance, please contact the Entity Vetting Knowledge Center at 878-274-2000, (Option 2, then Option 1) or dcsa.fcb@mail.mil.

DCSA FORM 147, JANUARY 2025 - IMPLEMENTATION CONTINUANCE

DCSA announced the implementation period last month for the revised 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 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, 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 current April 2022 version to the revised 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.
- Closed areas approved using the obsolete one-page DCSA Form 147 must be updated and documented as open storage areas. 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.
- Reminders of these transition dates will be disseminated through the VOI on a recurring basis until the transition is complete.

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.

CMMC IMPLEMENTATION, TODAY

In a recent review of defense contract data, DoD found that DFARS Clause 252.204-7021, Cybersecurity Maturity Model Certification (CMMC) Requirements, had appeared in over 14,000 FY25 DoD contracts issued by 14 different DoD components. This prompted immediate action because the Clause is not currently authorized for use in DoD contracts, nor should CMMC requirements be levied on contractors through any other contractual terms. USD(A&S) reminded the DoD contracting workforce to comply with regulations and DoD policy consistent with DFARS 204.7503 and the CMMC Program implementation timeline spelled out at in 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program.

DCSA is aware of companies that have been affected by DoD components implementing CMMC Level 2 requirements before the Department's planned implementation of the CMMC Program. We are working with these companies and components to minimize the impact and educate the entities on the status of the CMMC Program. As of today, the CMMC Program implementation date will be 60 days after publication of the final Title 48 CFR Part 204, CMMC Acquisition Rule, which is the implementation guidance for 32 CFR Part 170 issued in December 2024.

The anticipated release date for the 48 CFR Part 204, CMMC Acquisition Rule, was June 2025, but as of today, it has not been published to the Federal Register. CMMC assessment requirements will be implemented in four phases over a 3-year period. The phases add CMMC Level requirements incrementally, starting with self-assessments in Phase 1 and ending with full implementation of program requirements in Phase 4. This approach allows time to train assessors and companies to understand and implement CMMC assessment requirements.

CMMC 2.0 Implementation (48 CFR Part 204, CMMC Acquisition Rule) Pending Publication in the Federal Register.

- To be implemented through the acquisition and contracting process.
- Require compliance with CMMC as a condition of contract award.
- CMMC level will be specified in the solicitation & RFIs, if utilized.
- Key features identified in the CMMC Model Structure.
- CMMC Level 2 is implemented **VOLUNTARILY** as of February 28, 2025.

In advance of CMMC Phase 1, now is the time for contractors and DoD components to become more familiar with CMMC and other cybersecurity related subjects.

The Federal Register Notice on the Suspension of the CMMC Program states: *"Until the CMMC 2.0 changes become effective through both the title 32 CFR and title 48 CFR rulemaking processes, the Department will suspend the CMMC Piloting efforts and will not approve inclusion of a CMMC requirement in DoD solicitations."*

The 32 CFR Part 170, CMMC Program Rule can be found here.

The Proposed 48 CFR Part 204, CMMC Acquisition Rule can be found here.

The Cybersecurity Maturity Model Certification (CMMC) Program Phases can be found here.

INFORMATION SAFEGUARDING FOR FCL LETTERS

NISS is the system of record for maintaining Facility Clearances (FCLs) for each facility in the NISP. Government Contracting Activities (GCAs) often request this information during the Request for Proposal (RFP) process to verify and validate a facility's proposal package.

Documents are not dynamically marked within NISS because data within the system is designated Controlled Unclassified Information (CUI). Therefore, it is the responsibility of the authorized NISS user to ensure any receiving system meets or exceeds the minimum safeguarding requirements of CUI prior to transferring any data from NISS.

To assist Industry with meeting the task of providing FCL letters as part of their RFP process, the following Designator Indicator (DI) block should be added to each FCL letter prior to providing it to the GCA (see the below DI Block).

Controlled by: Defense Counterintelligence and Security Agency
Controlled by: Contractor Facility Name (CAGE Code)
CUI Category: OPSEC
LDC: FEDCON
POC: Verification & Triage Unit (VTU) / dcsa.quantico.hq.mbx.occ-facilities@mail.mil

OFFICE OF COUNTERINTELLIGENCE SVTC

DCSA invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) for the Defense Industrial Base entitled, "The Weaponization of Artificial Intelligence (AI)." A representative from the DCSA Counterintelligence Partnership with Cleared Industry (CIPCI) will provide a classified presentation on the weaponization of AI by our adversaries for CI and security purposes.

The SVTC is an in-person event at most DCSA field offices on August 21, 2025, from 1:00 to 2:30 p.m. ET. Please register by August 14, 2025 by filling out the form here.

DESIGNATED GOVERNMENT REPRESENTATIVE REMINDER

Here is a friendly reminder to all those who are to be a Designated Government Representative (DGR). A DGR must have successfully completed the FSO Program Management for Possessing Facilities Curriculum offered by the Center for Development of Security Excellence (CDSE), legacy FSO Role in the NISP, or **must** have other suitable qualifications as determined by the field office on a case-by-case basis.

DCSA offers several resources to aid DGRs to stay on top of training. These resources include:

- The DGR Brief found on DCSA's external webpage
- The DGR Roles and Responsibilities Short located on DCSA CDSE's website
- The DGR Roles and Responsibilities Job Aid located on DCSA CDSE's website.

INTERNATIONAL OUTGOING VISITS OUTREACH

The DCSA International and Special Programs Division is pleased to invite you to a comprehensive webinar on Wednesday, August 27, 2025, at 1:00 p.m. ET.

This newly enhanced session will provide step-by-step guidance on:

- Completing visit requests accurately
- Understanding when and how to submit requests
- Identifying common errors and how to avoid them
- Navigating different types of visits and required lead times
- Best practices for streamlined processing.

You'll have the opportunity to ask questions directly, and we welcome your input on how DCSA can better support your needs.

To secure your spot, please contact DCSA.RFV@MAIL.MIL by Friday, August 22, 2025.

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 many facilities who received an email or NISS notice in the past few weeks letting you know of your transfer to the National Access Elsewhere Security Oversight Center (NAESOC), we want to take the opportunity to invite you to take advantage of the resources the NAESOC has to offer to support your security programs.

Here is a list of some of the capabilities and resources provided by the NAESOC:

- Prioritized Effort: The NAESOC prioritizes all requests and actions based on identified risk.
- Expert Help Desk: 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.
- Team-Based Assistance: While you don't have an individually assigned ISR, you gain access to a dedicated team of ISRs and security specialists, all prepared to assist.

CONTACT US

Please take advantage of reaching us at:

- (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

We also maintain a 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.

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

CDSE WEBINARS & TRAINING

Registration Open: DCSA Security Conference for DOD

The DCSA Security Conference for DOD will be held virtually Aug. 26-28, 2025. This year's theme is "Mission and Security Integration: Safeguarding the Future."

The three-day virtual conference aims to bring together thousands of DOD security professionals across personnel security, acquisitions, insider threat, policy, counterintelligence and compliance. The conference is only open to federal employees with .mil or .gov email addresses.

Register to secure your spot today!

JULY 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 July newsletter focused on training and resources related to SPeD Certifications. Check out all the newsletters in CDSE Electronic Library or subscribe to have the newsletter sent directly to your inbox by signing up here.

INSIDER THREAT

New Curriculum: Insider Threat for Industry

The Insider Threat team just launched a new curriculum for Industry titled "Insider Threat for Industry." This curriculum was developed to support Industry in meeting the requirements found in the National Industrial Security Program Operating Manual (NISPOM).

The Insider Threat for Industry curriculum description, objectives, and courses can be found here.

DCSA's National Insider Threat Awareness Month (NITAM) Forum

Join DCSA for the National Insider Threat Awareness Month (NITAM) Forum on Aug. 18 and 19 at the U.S. Patent & Trademark Office in Alexandria, Va. This year's theme is, "Partnering for Progress & Innovation," and the event will be hosted by the DOD Insider Threat Management & Analysis Center (DITMAC).

The conference is open to federal employees and insider threat professionals working in academia. If you are unable to attend in person, join virtually!

Register here and secure your spot today!

PERSONNEL VETTING

New Resource Available: Customer Service Request (CSR) and Incident Report (IR) Management

Check out the CSR and IR Management Resource, which provides clarification and guidance on submitting Customer Service Requests and Incident Reports to DCSA AVS.

The resource is part of a larger effort across DoD to improve the Personnel Vetting mission. DCSA AVS has provided individual CSR and IR guidance on an ad hoc basis to customers.

However, until now, the guidance has never been publicly available. The new resource assists customers with submitting timely, accurate CSR and IR information for adjudication.

View the resource to learn more!

SPECIAL ACCESS PROGRAMS (SAP)

Introduction to Special Access Programs (SAPs) Course (SA101.01)

The Introduction to SAPs course focuses on the DoD SAP fundamentals to prepare students to become SAP security professionals. The lessons address security enhancements across all security disciplines, compliance inspection requirements, annual reviews, and audits. The course is administered through eLearning prerequisites and synchronous elements using the collaborative learning environment (CLE) STEPP. Class activities include group and individual practical exercises, quizzes, a team capstone, and a final course exam. The prerequisite eLearning courses/exams that provide a comprehensive introduction to SAP must be successfully completed prior to requesting enrollment into the instructor-led course. The course is offered on the following dates:

- August 5 to 8, 2025 (Lexington, MA) (MIT)
- September 9 to 12, 2025 (Rolling Meadows, IL) (NGC).

FISCAL YEAR 2025 UPCOMING COURSES

CDSE courses are a great way to gain security knowledge and awareness and expand skill sets.

Secure your spot now as classes fill quickly! Available Instructor-Led Training (ILT) and Virtual Instructor-Led Training (VILT) courses are listed below.

CYBERSECURITY

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

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

INDUSTRIAL SECURITY

Getting Started Seminar for New Facility Security Officers (FSOs) VILT (IS121.10)

- August 5 - 8, 2025 (Virtual)

INFORMATION SECURITY

Activity Security Manager VILT (IF203.10)

- July 28 - August 24, 2025 (Virtual)

PERSONNEL SECURITY

Personnel Vetting Seminar VILT (PS200.10)

- August 5 - 6, 2025 (Virtual)

PHYSICAL SECURITY

Physical Security and Asset Protection (PY201.01)

- August 18 - 22, 2025 (Linthicum, MD)

SPECIAL ACCESS PROGRAMS

Introduction to Special Access Programs (SA101.01)

- August 5 - 8, 2025 (Lexington, MA) (MIT)
- September 9 - 12, 2025 (Rolling Meadows, IL) (NGC)

Orientation to SAP Security Compliance Inspections (SA210.0)

- August 11 - 12, 2025 (Lexington, MA)

DCSA NEWS: NEW SECURITY TRAINING WEBSITES

Security Training, Education, and Professionalization Portal (STEPP) and the Security Awareness Hub (SAH) URLs changed to DCSA owned domains at the end of June.

- New STEPP link: https://securitytraining.dcsa.mil/
- New SAH link: https://securityawareness.dcsa.mil/

CDSE NEWS

Get the latest CDSE news, updates, and information. To subscribe to the Pulse or other CDSE publications, visit CDSE News to sign up or manage subscriptions.

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.