



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. For more information on all things DCSA, visit www.dcsa.mil.

TABLE OF CONTENTS

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)	2
CHANGES TO eAPP MULTI-FACTOR AUTHENTICATION LOGIN	2
PERSONNEL VETTING QUESTIONNAIRE DEPLOYMENT UPDATE	2
SECURITY REVIEW RATING RESULTS FISCAL YEAR 2025	3
UPDATED: SENIOR MANAGEMENT OFFICIAL SLICK SHEET	3
NEW: NATO BRIEFING JOB AID	4
SELF-APPROVAL FOR OPEN STORAGE AREAS	4
OFFICE OF COUNTERINTELLIGENCE SVTC	5
NAESOC UPDATES	5
STEADY-STATE OVERSIGHT	5
CONTACT US	5
NCCS UPDATE	6
INTERNATIONAL OUTGOING VISITS OUTREACH	6
NISS PHONE NUMBER ISSUE RESOLVED	7
ENSURE YOUR NISS FACILITY PROFILE IS UP-TO-DATE	7
CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)	7
CDSE PULSE UPDATE	7
FISCAL YEAR 26 SECURITY TRAINING COURSES	7
SOCIAL MEDIA	8
REMINDERS	8



NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

CHANGES TO eAPP MULTI-FACTOR AUTHENTICATION LOGIN

This month, NBIS is introducing a more streamlined method for personnel accessing the electronic application (eApp) with Multi-Factor Authentication (MFA). This new process is designed to be user-friendly and will significantly reduce the workload for personnel at DCSA.

Previously, applicants using MFA received two separate verification emails before they could use the DCSA Information Systems Agency Identity, Credential, and Access Management (D-ICAM) verification system. The instruction from two different emails often confused applicants, which overwhelmed the Help Desk with calls.

In October, the NBIS Service Level Management (SLM) Team partnered with cleared industry, military, federal, and contractor personnel and successfully tested the new access protocol that requires only one email response instead of two. Stakeholder feedback was invaluable in refining the new authentication process.

These changes are expected to reduce the Help Desk's workload and enhance the overall user experience, making it easier for applicants to access eApp and complete vetting requests.

For more information about the new process, visit the DCSA [Multi-Factor Authentication Assistance](#) page. Deployment of this MFA capability is expected in early December and will be announced in a news article posted [here](#).

PERSONNEL VETTING QUESTIONNAIRE DEPLOYMENT UPDATE

The Personnel Vetting Questionnaire (PVQ) supports Trusted Workforce 2.0 by providing a standardized and continually updated framework for gathering comprehensive information necessary to assess an individual's trustworthiness and suitability for access. The PVQ is the baseline document for collecting subject information required to initiate and conduct vetting requests under the Trusted Workforce 2.0 framework. The PVQ will streamline the vetting system and provide a more modern, straightforward form.

DCSA has been rigorously testing the PVQ form over the past year to ensure its effectiveness and user-friendliness. This extensive testing period has allowed for refinements and improvements based on real-world feedback and data analysis.

On November 18, NBIS leadership approved the deployment of the PVQ forms for a small population of only DCSA personnel for production verification. Through this verification process, the SLM Team will work closely with the DCSA Security Office to initiate several DCSA employees for Five-Year updates and walk them through end to end processing.

DCSA will analyze results of this small population to assess the potential for expanding the use of these forms to other customer groups and will provide updates and notifications when available. Please check the [DCSA News page](#) for future updates.



SECURITY REVIEW RATING RESULTS FISCAL YEAR 2025

Security review results for Fiscal Year 2025 were current as of October 24 (due to the furlough, rating coordination remains for additional security reviews):

Overall Fiscal Year Goal:	4,000	
Rated Security Reviews Completed:	4,616	(115.4%)
Superior Ratings Issued:	709	(15.3%)
Commendable Ratings Issued:	1,632	(35.4%)
Satisfactory Ratings Issued:	2,235	(48.4%)
Marginal Ratings Issued:	19	(00.4%)
Unsatisfactory Ratings Issued:	21	(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.

Results for Fiscal Year 2026 security reviews will commence in the next Voice of Industry.

UPDATED: SENIOR MANAGEMENT OFFICIAL SLICK SHEET

The NISP Mission Performance Division has published an updated Senior Management Official (SMO) Slick Sheet that provides added clarity related to parent-subsidary relationships. While we encourage you to review the job aid in its entirety, a few highlights include:

- A Multiple Facility Organization (MFO) is a single legal entity composed of two or more cleared facilities (i.e., a home office facility (HOF) identified on the DD Form 441 “DOD Security Agreement” and at least one branch/division identified on the DD Form 441-1 “Appendage to DOD Security Agreement”).
- Within an MFO, the designated SMO for the HOF is the individual with ultimate authority over the legal entity’s operations as outlined in the governance documents.
- Due to the unique nature of MFOs, the governing HOF may choose to either maintain the HOF SMO as the SMO for one or more cleared branch/division facility or may appoint another cleared employee at each branch/division as the facility SMO.
- Although ultimate accountability cannot be delegated from the HOF SMO, security related duties can be performed by an appointed branch/division SMO. Refer to the frequently asked questions for more information.
- Although part of the same corporate family, a parent-subsidary relationship is not considered an MFO since they are separate legal entities (indicated by executing separate DD Form 441s). As such, the SMO for each legal entity’s HOF will be based on the entity’s governance documents.

A copy of the SMO Slick Sheet is located within the [NISP Tools & Resources](#) section of the DCSA website.



NEW: NATO BRIEFING JOB AID

The NISP Mission Performance Division is pleased to announce the availability of a new job aid for cleared contractors under DCSA cognizance that provides guidance related to North Atlantic Treaty Organization (NATO) briefing requirements.

While we encourage you to review the job aid in its entirety, a few highlights include:

- A DCSA representative, usually the assigned ISR, will provide an initial NATO security briefing to a contractor representative when item 10(g) is selected on the DD Form 254 and access to NATO classified information is required in support of the contract.
- The contractor representative, or another briefed contractor designee, will then provide the initial NATO security briefing to other employees requiring access to NATO classified information in performance of the contract, prior to granting them access.
- The contractor representative will receive an annual NATO refresher briefing from another briefed contractor designee, **or** a DCSA representative. For purposes of NATO refresher briefings, "annual" means once a calendar year.
- The contractor representative, or another briefed contractor designee, will provide annual NATO security refresher briefings to only those employees requiring continued access to NATO classified information in performance of the contract.
- The contractor must enter the initial NATO security briefing date in the Defense Information System for Security (DISS). There is no requirement to enter annual NATO security briefing dates in DISS or to upload a copy of the briefing certificates.

A copy of the NATO Job Aid is located within the [NISP Tools & Resources](#) section of the DCSA website.

SELF-APPROVAL FOR OPEN STORAGE AREAS

DCSA and the National Industrial Security Program Policy Advisory Committee (NISPPAC) Industry Group are partnering to reinstate self-approval authority for Open Storage Areas within Industry, offering increased efficiency and flexibility for cleared contractors. The DCSA/NISPPAC working group has reconvened to finalize the guidelines and procedures, paving the way for FSOs and security staff to request self-approval authority for Open Storage Areas. This change will increase efficiency by streamlining the approval process for routine changes within Open Storage Areas and provide companies with greater flexibility to meet contract requirements.

The process will be introduced in an NCMS Live presentation being scheduled for early to mid-December. Watch for upcoming announcements about the specific date and time! Full implementation is planned for January 1, 2026. Check the DCSA Website as we get closer to January 1 for more detailed information and updates.



OFFICE OF COUNTERINTELLIGENCE SVTC

DCSA invites cleared industry to participate in a Secure Video Teleconference (SVTC) with the Defense Industrial Base entitled "Defense Industrial Base Counterintelligence Threat Trends." Counterintelligence analysts from DCSA's Analysis Division and Cyber Mission Center 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." Also, information will be provided for cleared personnel participating in the 2026 World Defense Show, being held 8 to 12 February, 2026 in Riyadh, Saudia Arabia.

The SVTC with cleared industry is an in-person event at most DCSA field offices on Thursday, January 8, 2026, from 1:00 to 2:30 p.m. ET. Please use the following link to register [here](#) by **December 31, 2025**.

NAESOC UPDATES

STEADY-STATE OVERSIGHT

With the end of the recent government furlough, we want to let you know as a Facility Security Officer that the NAESOC is back at 100% operations and requests and issues you submitted during the furlough continue to be processed. All furlough-delayed actions are prioritized based on their identified risk and their potential impact to the National Industrial Security Program. You can expect:

- Remote Security Reviews. If you were contacted prior to the furlough by an ISR about a scheduled or upcoming remote security review, that ISR will be in contact with you about scheduling or re-scheduling that event. The furlough did not affect the requirement for you to have the review, only the timing of it. Please continue to complete all pre-Remote Security Review (RSR) activities (NISS Facility Profile Updates, security program documentation submissions) to ensure you are ready for your security review. If you have any questions related to preparing for the RSR, please reach out to the ISR conducting your review or the NAESOC Help Desk.
- Changed Conditions. Please continue to formally report all changed conditions in NISS. Ensure all reporting is supported by business documentation.
- Advice and Assistance, Safeguarding Requests, Policy Clarifications and Questions/General Mailbox Inquiries. Issues or requests you presented during the furlough to which the Help Desk team replied in email, "When the furlough ends, an Industrial Security Representative will contact you," have been prioritized and assigned for action. You will soon be hearing from an ISR.

As per normal operations, if you have an issue of urgency identified during the furlough that needs to be escalated, please use the Blue Button on the NAESOC web site.

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



NCCS UPDATE

We implemented the NISP Contract Classification System (NCCS) v2.9.4 update on November 6, 2025 which fixed identified bugs and updated some components to the platform's hierarchy capabilities. This update provides a more granular view of the organization's user base.

The NCCS upload feature is being reworked to ensure smooth ingestion of released DD Form 254s. New and Improved NCCS training materials to be added to our external website soon!

Please download the NCCS Help Desk Job Aid, and updated User Guides for Government and Industry users [here](#).

When requesting an account to NCCS, please download the DD 2875 SAAR Form from the DCSA [NCCS Training Materials](#) website. You will need to right click and "save link as" to save the SAAR to your computer, then open it from there to complete the form.

Please remember to sign into NCCS every 30 calendar days to keep your account active!

Questions? Contact us at dcsa.quantico.is.mbx.nccs-support@mail.mil.

INTERNATIONAL OUTGOING VISITS OUTREACH

The DCSA International and Special Programs Division is pleased to invite you to a comprehensive webinar on Wednesday, December 10, 2025, at 1:00 PM EST.

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

- Completing international outgoing visit for cleared U.S. contractors traveling to classified sites
- 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.

Please save the date on your calendar! Click the link [FSO International Visits Outreach](#) to join the meeting on Wednesday, December 10, 2025, at 1:00 p.m. ET.



NISS PHONE NUMBER ISSUE RESOLVED

ENSURE YOUR NISS FACILITY PROFILE IS UP-TO-DATE

The National Industrial Security System (NISS) was updated on November 21 to resolve an issue with updating the Phone Number field on facility profiles. Previously, users were unable to update certain phone numbers and submit a proper Industrial Facility Profile Update (IFPU). Now that the issue is resolved, please log into NISS and verify that your facility profiles are up-to-date with accurate information and correct phone numbers.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

CDSE PULSE UPDATE

Due to the recent government shutdown, publication of the CDSE Pulse was suspended for the month of November. Look for the next issue of the Pulse to be published on schedule and posted to CDSE's [Electronic Library](#) in early December or [subscribe](#) to have the newsletter delivered directly to your inbox.

FISCAL YEAR 26 SECURITY TRAINING COURSES

Find a complete list of CDSE offerings [here](#) with links to course descriptions and requirements.

CYBERSECURITY:

[Assessing Risk and Applying Security Controls to NISP Systems](#) CS301.01
February 2 - 6, 2026 (Linthicum, MD)

INDUSTRIAL SECURITY:

[Getting Started Seminar for New Facility Security Officers \(FSOs\) VILT](#) IS121.10
January 13 - 16, 2026 (Virtual)
March 24 - 27, 2026 (Virtual)

INFORMATION SECURITY:

[Activity Security Manager VILT](#) IF203.10
January 25 - February 22, 2026 (Virtual)

INSIDER THREAT:

[Insider Threat Detection Analysis VILT](#) INT200.10
January 12 - 16, 2026 (Virtual)
February 9 - 13, 2026 (Virtual)
March 16 - 20, 2026 (Virtual)



PHYSICAL SECURITY:

[Physical Security and Asset Protection](#) PY201.01

February 2 – 6, 2026 (Linthicum, MD)

[Physical Security and Asset Protection VILT](#) PY201.10

February 23 - March 13, 2026 (Virtual)

SPECIAL ACCESS PROGRAMS:

[Introduction to Special Access Programs](#) SA101.01

March 3 – 6, 2026 (Korea)

March 10 – 13, 2026 (Hawaii)

[Introduction to Special Access Programs VILT](#) SA101.10

December 1 - 9, 2025 (Virtual)

[Orientation to SAP Security Compliance Inspections](#) SA210.01

February 18 - 19, 2026 (Linthicum, MD)

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.