DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

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

TABLE OF CONTENTS

NBIS LAUNCHES SIMPLIFIED LOGIN PROCESS TO eAPP

On December 8, 2025, National Background Investigation Services (NBIS) launched a streamlined method for personnel to access the Electronic Application (eApp) using Multi-Factor Authentication (MFA). The new process enhances the user experience and significantly reduces the workload for personnel at DCSA, benefiting everyone involved.

Before the new process, applicants using MFA received two separate verification emails before they could access the DCSA Information Systems Agency Identity, Credential, and Access Management (D-ICAM) verification system. This dual-email system often confused applicants and led to an influx of calls to the DCSA Help Desk.

Now, applicants receive just one verification email, which simplifies the login process and makes it much easier for them to access eApp and complete their vetting requests. Since the launch of the new login system a few weeks ago, the DCSA Help Desk has experienced a decrease in calls for assistance with logging into eApp.

For more information about the new process, visit the Multi-Factor Authentication Assistance page on DCSA.mil.

SECURITY REVIEW RATING RESULTS FISCAL YEAR 2025

As of December 23, 2025, DCSA has exceeded its Fiscal Year 2025 security review goal by 16.3%, completing 4,652 rated reviews against a target of 4,000. Over 99% of all completed reviews were rated Satisfactory or higher. DCSA extends our congratulations to the 711 facilities that achieved a “Superior” security rating, with 141 facilities receiving a perfect score. These organizations are the gold standard.

A breakdown of the security review ratings for Fiscal Year 2025 is provided below. This information is current as of December 23 records:

Overall Fiscal Year Goal:	4,000	
Rated Security Reviews Completed:	4,652	(116.3%)
Superior Ratings Issued:	711	(15.3%)
Commendable Ratings Issued:	1,637	(35.2%)
Satisfactory Ratings Issued:	2,263	(48.6%)
Marginal Ratings Issued:	20	(00.4%)
Unsatisfactory Ratings Issued:	21	(00.5%)

If you have questions related to this notification, please email the NISP Mission Performance (NMP) Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

TOP 10 DEFICIENCIES FROM DCSA SECURITY REVIEWS

To assist industry partners in preparing for upcoming DCSA security reviews, we have compiled the ten most common deficient findings from Fiscal Year 2025 security reviews relative to requirements in the National Industrial Security Program Operating Manual (NISPOM). Proactively addressing these areas now will strengthen a facility's security posture and lead to a more efficient review. Additional information will be highlighted in next month's edition of the Voice of Industry newsletter.

Order	Reference	Description
1	117.18(b)	Information System Security Program
2	117.8(c)	Reporting to DCSA
3	117.7(h)	Self Inspections
4	117.10(a)	Defense Information System for Security (DISS) Management
5	117.12(g)	Insider Threat Training
6	117.12(k)	Refresher Training
7	117.12(e)	Initial Security Training
8	117.19(g)	NATO Security Requirements
9	117.15(a)	Safeguarding Classified Information
10	117.7(b)	Contractor Security Officials (SMO, FSO, ITPSO, and ISSM)

If you have questions related to this notification, please email the NMP Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

OPEN STORAGE AREA SELF-APPROVAL AUTHORITY

DCSA, in partnership with the National Industrial Security Program Policy Advisory Committee (NISPPAC) Industry Group, has developed procedures for cleared defense contractors to self-approve their open storage areas (OSAs) at their facilities. These procedures will become effective on January 1, 2026, to increase efficiency and empower contractors to respond more rapidly to evolving contract requirements.

Contractor self-approval of OSAs offers advantages and requires a strong commitment to fundamental security practices, robust management, rigorous oversight, and clear communication with the assigned DCSA representative. Under this system, companies can implement OSAs as needed, provided they adhere to established procedures. DCSA retains the authority to review all facilities, including those with self-approved OSAs, to ensure compliance with security policies and physical construction requirements.

DCSA and NISPPAC working groups have finalized the program's guidelines and procedures so FSOs or their designated security staff can request self-approval for OSAs. Participation in this program is voluntary and dependent on contract requirements. Key benefits include enabling rapid responses to new or changing contract needs and empowering industry security professionals.

For more information, visit National Industrial Security Program Oversight on DCSA.mil, navigate to NISP Tools & Resources, and find Self-Approval Authority under the FSO Guides dropdown.

SECURITY ELIGIBILITY VS. ACCESS AUTHORIZATION: UNDERSTANDING THE DIFFERENCE

An important aspect of security compliance is understanding the difference between eligibility and access authorization. While related, these terms are not interchangeable and carry different implications.

Eligibility is an official adjudicative determination by an authorized U.S. Government entity, such as DCSA, that an individual is trustworthy and may be granted access to classified national security information up to a specified level. This determination is the foundational prerequisite for any individual who will work with classified materials and is required for certain Key Management Personnel (KMP) as a condition of the facility's clearance, regardless of their day-to-day duties.

Conversely, access authorization is the contractor's affirmative action of granting an individual with the appropriate eligibility level the ability to handle (or access) classified information in the Defense Information System for Security (DISS). This action is contingent upon two critical factors: the individual must have a valid, signed Nondisclosure Agreement (SF 312) on file, and their assigned job duties must create a valid need to access classified information. It is important to distinguish ‘need to access’ from the principle of 'need-to-know,' which is also a prerequisite for an individual receiving classified information but is a separate determination made by an authorized holder of specific classified information prior to release.

It is common for a KMP to have eligibility without having an access authorization if their role does not require it. For example, an Insider Threat Program Senior Official (ITPSO) must maintain eligibility as part of their key position but may not have a need to access classified data, attend classified meetings, or have unescorted access within classified spaces. In this instance, the contractor would not grant access authorization. This distinction ensures that access to classified information is strictly limited based on operational and job-related requirements. In this case, the contractor remains fully responsible for maintaining the individual’s security record in DISS, ensuring their enrollment in Continuous Vetting, and managing the submission of an updated Standard Form (SF) 86 every 5 years for Continuous Vetting purposes. For detailed guidance on maintaining this relationship in DISS, including the process for managing 'break in access' or 'break in employment,' please refer to the February 2025 VOI and the DISS Management Job Aid available in the NISP Tools & Resources section of the DCSA website.

If you have questions related to this notification, please email the NMP Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

ANNUAL SELF-INSPECTION TIMELINE REMINDER

Cleared contractors are required to conduct a formal self-inspection of their security program at least annually. DCSA officially interprets “annually” as once per calendar year. This means that a facility would be compliant if it conducted a self-inspection on any date in 2024 and the next on any date in 2025, as each inspection occurred in a consecutive calendar year.

While the calendar year interpretation allows flexibility, DCSA recommends a more routine and consistent self-inspection schedule. Contractors are encouraged to tailor their self-inspection schedule based on risk factors such as the complexity of their classified contracts, their volume of classified material, and findings from their previous security reviews. High-risk programs or areas with previously identified vulnerabilities may warrant more frequent or targeted inspections beyond the annual requirement. This proactive stance is a key component of a robust security program.

It is critical to distinguish this guidance from the separate, stricter requirement for facilities with classified information systems. For these facilities, the self-inspection of classified system components must be conducted at least every 12 months, without the flexibility of the 'calendar year' interpretation.

The self-inspection is a key tool in fostering a proactive security culture. It is an opportunity to engage with both cleared and non-cleared personnel to reinforce their security responsibilities and validate that internal procedures are understood and effectively implemented across the organization. This highlights that security is a shared responsibility and demonstrates a facility-wide culture of security that starts with management and involves all personnel.

If you have questions related to this notification, please email the NMP Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

NATO AWARENESS BRIEFINGS FOR SIPRNET ACCESS

The NMP Division recently released a job aid covering NATO Security Briefing requirements. Contractors are encouraged to use this job aid as a consolidated list of briefing requirements for personnel who require formal access to NATO classified information.

This job aid does not provide guidance on NATO Awareness Briefings required for SIPRNet access only. To prevent confusion, the following table officially distinguishes the two briefing types.

Briefing Type	Intended for Personnel	Cite in DD 254	Signed Certificate Required?	DISS Entry?	Briefing Responsibility
NATO Security	Who require access to NATO classified information.	Item 10(g)	Yes, it is a mandatory requirement.	Yes	A DCSA ISR provides the initial briefing to a contractor representative. This individual, or a designee they briefed, then provides initial and annual briefings only to employees requiring access to NATO classified.
NATO Awareness	Who require access to a system (like SIPRNet) that can handle NATO data, but do not need to access the data themselves.	Item 13	Maybe. It is a common practice, but not a NISPOM requirement. Refer to the specific GCA requirements for the contract.	No	The Government Contracting Activity (GCA) or a representative of the contractor are likely able to provide awareness briefings. Refer to the specific GCA requirements for the contract.

If you have questions related to this notification, please email the NMP Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

INSIDER THREAT PROGRAM TRAINING REQUIREMENTS

Effective Date and Exemptions: Mandatory training is required for all insider threat program personnel appointed on or after July 1, 2025. Personnel appointed before this date who have completed training aligned to previous guidance are exempt.

Audience and Responsibility: "Program personnel" are individuals who manage the insider threat program, including the Insider Threat Program Senior Official (ITPSO). The ITPSO is responsible for identifying all program personnel and ensuring they complete the required training.

Training Options: Insider threat program personnel must complete one of the following two options to satisfy the DCSA training requirement:

Option	Training Program	Description	Key Considerations
CDSE	CDSE "Insider Threat for Industry Curriculum, INT333.CU"	A comprehensive 5-hour eLearning curriculum available through the Center for Development of Security Excellence (CDSE).	This curriculum is designed by DCSA to meet minimum NISPOM requirements.
Contractor	Contractor-Developed Program	A custom training solution covering all required 32 CFR 117.12(g) topics. This can be a proprietary solution or the pre-validated NISPPAC Insider Threat Working Group (WG) slides.	When using the NISPPAC Insider Threat WG slides: • They must not be altered • The DCSA validation letter must be kept on file.

If you have questions related to this notification, please email the NMP Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

INDUSTRIAL SECURITY LETTERS

DCSA has rescinded all outdated Industrial Security Letters (ISLs) that referenced the previous NISPOM, DoD Manual 5220.22.

Please refrain from using these in reference to the current NISPOM, 32 CFR Part 117. The current applicable ISLs that provide guidance are:

- ISL 2024-02: NBIS eApp System of Record for SF 86 Submission
- ISL 2024-01: Commercial Cloud Services Authorization
- ISL 2021-02: SEAD 3 Clarification and Guidance on Reportable Activities

These ISLs align with the current regulatory framework.

For more information, visit National Industrial Security Program Oversight on DCSA.mil, navigate to NISP Tools & Resources, and find Industrial Security Letters in the NISP Resources dropdown box.

NAESOC

SECURITY REVIEWS WITH THE NAESOC

The National Access Elsewhere Security Oversight Center (NAESOC) is actively scheduling Remote Security Reviews (RSRs) with facilities falling under NAESOC's oversight criteria. Facilities will be contacted directly by our team to schedule their RSR.

To facilitate a comprehensive and efficient review, each facility will be formally required to complete the following pre-review activities:

- **Review and Update NISS:** Thoroughly review your facility's profile in the National Industrial Security System (NISS).
    - Submit a facility profile update request**.** This update must include current company information and an account of all active classified contracts corresponding with their DD Form 254s.
    - Ensure any changed conditions have been reported by submitting a changed condition package with the necessary business documentation to substantiate the change.
- **Provide Security Program Information:** Submit all requested documentation pertaining to your security program.
- **Coordinate Interviews:** Arrange and schedule interviews with relevant employees.

This required pre-review submission is an integral part of the overall Remote Security Review and must be completed before the scheduled start date.

STAY CONNECTED WITH YOUR ENHANCED HELP DESK

- We want you to get the most from the NAESOC Help Desk. Our web site provides you a direct line to the information you need.
- There you can find job aids, user guides, and answers to common questions.
- To get all critical updates, please add dcsa.naesoc.generalmailbox@mail.mil to your email's safe sender list. This ensures our messages reach your inbox. Also, make sure your NISS profile lists your current points of contact.

CONTACT US

- (878) 274-1800 for 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 MIGRATION TO NI2 GOES LIVE JANUARY 30, 2026!

We're excited to announce that the NISP Contract Classification System (NCCS) will be the first feature launched into the National Industrial Security System Increment 2 (NI2) application on **January 30, 2026!** This migration supports DCSA's ongoing effort to streamline and enhance its industrial security offerings for Government and industry partners.

What This Means for You:

- **Minimal Impact:** Current NCCS users will experience minimal disruption.
- **Automatic Migration:** All existing users and data will be migrated automatically.
- **No Data Re-creation:** You will not need to re-create any data.
- **Familiar Functionality:** System functionality is intended to remain consistent with the current NCCS.
- **New Web Address:** The primary change for users will be accessing NCCS through a new web address: https://niss.dcsa.mil (Go-Live Date: January 30, 2026).

Benefits of NI2:

- **Enhancements to User Experience and System Performance:** As the integration of NCCS with NI2 progresses, DCSA will prioritize releasing new features and enhancements within the NCCS Capability, resulting in a more efficient and user-friendly experience for authorized personnel.
- **Streamlining Interoperability:** DCSA is actively working to integrate future Industrial Security applications into the NI2 solution. The integration of these tools will be the foundation for facilitating a cohesive and interconnected environment for enhanced situational awareness and collaborative analysis.
- **Consolidation and Modernization:** Functionality from NISS is planned to be integrated into NI2 in March 2028, further consolidating and modernizing our industrial security systems.

Important Reminder Regarding Account Activity: Please remember to sign into NCCS at least once every 30 calendar days to maintain your account's active status.

Questions?

For any questions or assistance, please contact us at dcsa.quantico.is.mbx.nccs-support@mail.mil (note: the email address will change with the transition to dcsa.meade.peo.list.ni2-support@mail.mil).

NISS REMINDER: 2026 ESSENTIAL PROFILE UPDATES

Happy Holidays from the NISS Team! We wish you a season filled with joy, warmth, and quality time with loved ones.

As we look forward to 2026, we kindly request that you take a few moments to ensure your facility profiles are accurate and up-to-date. Please log in and verify the following information:

- Addresses: Double-check that your physical and mailing addresses are correct.
- Key Management Personnel (KMP): Confirm that all KMPs listed are current and hold the appropriate positions.
- Contact Information: Ensure that all phone numbers and email addresses are accurate and monitored.

The maintenance of accurate information is crucial for effective communication and important updates. Thank you for your cooperation!

Wishing you a happy and healthy New Year!

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.” 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 January 5, 2026**.

OFFICE OF ENTITY VETTING

ESSENTIAL KMP INFORMATION REQUIREMENT

DCSA asks each facility in cleared industry to include personal email addresses for all essential KMP within its initial facility clearance (FCL) package to facilitate the prompt processing of personnel security clearances within the Defense Industrial Base. This contact information is necessary to initiate the eApp request for completing the SF 86. DCSA currently must obtain that information by phone or email after the FCL package is submitted, which slows down processing. Providing all essential KMP addresses in the FCL package will prevent any potential account issues as it associates the account with the individual and not the employer. Personal email addresses should be provided in the National Industrial Security System (NISS) database when submitting an initial FCL request. For questions, please contact the Office of Entity Vetting at 878-274-2000 (Option 2, then Option 1) or via email at: dcsa.fcb@mail.mil.

TOP ITEMS DELAYING FCL PACKAGE PROCESSING

DCSA processes approximately 1,500-1,700 packages annually, of which 67% percent are returned to the facility for additional information or updates due to missing or incomplete information. The following list provides the top reasons for package return so industry can avoid these common mistakes.

1. **Incomplete or Missing Organizational Charts and Ownership Details:**

   - Many companies provide organizational charts of personnel rather than of companies and the individuals who own and control them. Industry is required to provide organizational charts showing all entities in the corporate structure and ownership of those entities.

   - Common missing items are the full ownership and control structure for the entire organization, including all parents, resolving to the individuals who own and control the ultimate parent. This is especially prevalent in complex organizational structures including fund investment, where the most common missing information includes ultimate beneficial ownership; complete ownership and control structures for limited partnerships (limited partners and general partners) and limited liability companies (members and managers, where applicable); foreign ownership in an individual fund and all funds in aggregate; and details on foreign subsidiaries.

2. **Insufficient Explanations on the Standard Form 328:** Insufficient explanations for affirmative SF 328 responses are very common, especially concerning:

   - **Question 1 (Foreign Ownership):** Vague or incomplete explanations of the full ownership and control structure, resolving to the individuals who own and control the ultimate parent entities (this is like the corporate organizational charts noted above).

   - **Question 5 (Foreign Contracts or Agreements):** Vague or incomplete explanations for this question is the most common reason for returning a package due to the SF 328. Common missing items include contracts broken down by country and the percent of revenue derived (for facilities with a large number of involvements); the full name of the foreign individual or entity with which the facility has a contract or agreement, the country, and the percent of revenue derived; the nature of the involvement; the purpose of the contract or agreement; and information on foreign employees and those the facility has sponsored for H-1B visas.

   - **Question 6 (Foreign Indebtedness or Obligations):** Incomplete or missing information concerning the facility’s financial health, assets, liabilities, and loan agreement information including indebtedness or obligation type, amount, length, collateral identification, full names of the foreign parties involved, and the extent of their involvement.

3. **Lack of Clarity on KMP and Governance:** Industry typically identifies the individuals who are essential KMP requiring a personnel security clearance in connection with the facility’s FCL. Proper identification of KMP is essential to ensure the timely processing of an FCL package, including ensuring all essential KMP identified are consistent with the roles and requirements identified in governance documentation. Common errors include identifying the wrong individuals as essential KMP, identifying roles on the KMP List which are not reflected in the governance documentation, and full details on managing board composition.

For questions, please contact the Office of Entity Vetting at 878-274-2000 (Option 2, then Option 1) or via email at: dcsa.fcb@mail.mil.

DCSA INDUSTRY STAKEHOLDER ENGAGEMENT (ISE)

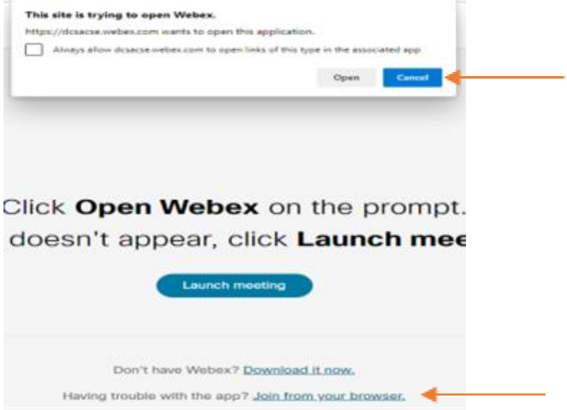
The DCSA Customer & Stakeholder Engagement (CSE) team will host the next quarterly Industry Stakeholder Engagement (ISE) on January 13, 2026, from 10:30 a.m. to 12:00 p.m. ET for all Industry FSOs and Security Professionals. The last engagement, held on July 10, 2025, resulted in an outstanding attendance of over 500 FSOs and industry security professionals and focused on best practices for FSOs, Catch'em-in CONUS processes, and Personnel Vetting Metrics and updates.

The January ISE will be held virtually via Webex and a dial in number. The tentative agenda for the meeting will consist of:

- Introduction/Welcome
- Personnel Vetting (PV) – Background Investigation, Continuous Vetting, and Adjudication Metrics and Updates
- NBIS Service Level Management – NBIS Updates
- NISS – NISS issue resolutions and NISS Increment 2 (NI2) updates
- NCCS – NCCS and onboarding processes
- Conclusion.

Note: When logging into Webex, please use your government/company email (vs. personal email) and First/Last name. This is beneficial to us to help address individuals and their questions.

Logging into Webex Meetings: After clicking on the meeting link or copy/pasting the link into your browser, click Cancel and then Join from your browser.



This site is trying to open Webex.

https://dcsacse.webex.com wants to open this application.

□ Always allow dcsacse.webex.com to open links of this type in the associated app

Click **Open Webex** on the prompt.

doesn't appear, click **Launch mee**

Don't have Webex? Download it now.

Having trouble with the app? Join from your browser.

If you are still experiencing issues, please use the dial in information using your phone:

Phone: +1-415-527-5035

Access Code: 2828 786 8813

Join from the meeting link: DCSA Industry Stakeholder Engagement (ISE) Meeting

SECURITY TRAINING

CDSE PULSE

The December edition of The Pulse is now available in the Center for Development of Security Excellence (CDSE) Electronic Library. Stay in the loop with CDSE products and updates by subscribing to direct delivery here!

FISCAL YEAR 2026 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)

Orientation to SAP Security Compliance Inspections SA210.01
February 18 - 19, 2026 (Linthicum, MD)

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.

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/

CONTACTS

DCSA Knowledge Center - 1-878-274-2000

National Background Investigation Services (NBIS) -

Support Help Desk/Customer Engagement Team (CET): 878-274-1765 or dcsa.ncr.nbis.mbx.contact-center@mail.mil

NBIS ServiceNow Help Desk: https://dcsa.servicenowservices.com/nbis

NAESOC Help Desk - (878) 274-1800 for Live Queries Monday through Thursday - 9:00 a.m. to 3:00 p.m. ET and Friday - 8:00 a.m. to 2:00 p.m. ET or dcsa.naesoc.generalmailbox@mail.mil

Background Investigations (BI) -

To Verify an Agent's / Investigator's Identity or Status: 878-274-1186 or dcsa.boyers.bi.mbx.investigator-verifications@mail.mil

DCSA Industry Agency Liaisons: dcsa.boyers.dcsa.mbx.industry-agency-liaison@mail.mil

Personnel Vetting (PV) - 667-424-3850 (SMOs and FSOs ONLY, No Subject Callers) or dcsa.meade.cas.mbx.call-center@mail.mil

Applicant Knowledge Center: 878-274-5091 or DCSAAKC@mail.mil

All Other PCL Related Inquiries: dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil

DOHA - 866-231-3153, 703-696-4599, or dohastatus@ssdgc.osd.mil