DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

January 2026

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

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).

COMMUNICATION ERROR WITH USPS IN eAPP RESOLVED

Recently, applicants may have experienced issues when Electronic Application (eApp) attempted to validate addresses via its connection to the U.S. Postal Service (USPS). On January 27, the National Background Investigation Services (NBIS) / eApp Team implemented a fix to resolve this problem.

If applicants continue to encounter issues, contact the Customer Engagements Team at:

- dcsa.ncr.nbis.mbx.contact-center@mail.mil
- 878-274-1765

DISS CONTINUOUS VETTING DATA CORRECTION

The recent deployment of Defense Information System for Security (DISS) Release 14.3 on January 22 led to incorrect records showing Continuous Vetting (CV) Unenrollment for some Department of War (DoW) customers in the DISS Joint Verification System (JVS) user interface.

A Data Quality Initiative (DQI) was swiftly completed on January 28, which corrected the statuses back to the previous enrollment date. The full correction of all affected records was finalized on January 29 with the deployment of DISS Release 14.3.1.

It is important to note that a new SF 86 submission is not necessary unless the individual's last SF 86 is more than 5 years old.

For any inquiries or assistance regarding DISS, please reach out to the Customer Engagements Team at 878-274-1765 or dcsa.ncr.nbis.mbx.contact-center@mail.mil.

SECURITY REVIEW RATING RESULTS

The following security review results are current as of January 28, 2026:

Overall Fiscal Year Goal:	3,900	
Rated Security Reviews Completed:	648	(16.6%)
Rated Security Reviews Remaining:	3,252	(83.4%)
Superior Ratings Issued:	64	(9.9%)
Commendable Ratings Issued:	217	(33.5%)
Satisfactory Ratings Issued:	365	(56.3%)
Marginal Ratings Issued:	1	(00.2%)
Unsatisfactory Ratings Issued:	1	(00.2%)

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.

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.

ADDRESSING SF 312 DIGITAL SUBMISSION ISSUE IN DISS

On January 20, DCSA announced on its website that the issue causing mass rejections of digitally signed Standard Form 312 (SF 312) in DISS is being addressed. While the root cause of the problem is being identified, a work around (manual review) process is being instituted. Effective immediately, DCSA is directing industry users to begin resubmitting the forms that were previously rejected to ensure that all personnel records are current and compliant.

ACTION REQUIRED FOR PREVIOUSLY REJECTED SF 312s

Please follow the instructions below to clear the backlog of rejected forms.

Affiliation Status	Action Required
Subject is still affiliated with the entity.	You may now resubmit the original, previously-rejected SF 312. Please verify the form's accuracy and ensure the digital certificate is not expired before submission.
Subject is no longer affiliated with the entity.	Do not attempt to resubmit an SF 312 for subjects separated from the entity. To cancel the open task, email DCSA NCR NBIS Mailbox Contact Center (dcsa.ncr.nbis.mbx.contact-center@mail.mil) with the person's name, your CAGE Code, and their last day of employment. They'll open a ticket and then it should be removed from your Task Inbox. If this solution doesn't clear the task within five business days, send an email to the PSMO-I email at dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil.
Subject is newly affiliated with the entity (post-rejection).	Prior to granting access, confirm the subject has a Nondisclosure Agreement (NDA) date on the person summary screen and validate that there is no pending SF 312 notification under accesses within the NDA History tab. If there is a pending SF 312, please execute and submit a new SF 312. This indicates that the subject likely had an SF 312 rejected at their last entity.

DCSA appreciates the patience and cooperation our industry partners have shown. We are committed to ensuring a stable and reliable process for all security clearance procedures.

A GUIDE TO PROPERLY EXECUTE THE SF 312

To ensure compliance and maintain the integrity of the security clearance process, all industry partners must adhere to the following procedures when executing the Standard Form 312 (SF 312), Classified Information NDA.

Step 1: Verify the Need for a New Agreement

Before an employee is granted access to classified information, you must first determine if they have a previously executed SF 312 on file. Log in to DISS JVS to confirm.

- If the employee's person summary screen shows an NDA date and there are no pending SF 312 notifications under the NDA history tab, then a new agreement is not required.

- If you find a "pending SF 312" notification under the NDA history tab, then it signifies that a previous SF 312 was likely rejected due to an administrative or digital signature issue and a new agreement must be executed.

Step 2: Employee Signature and Witnessing

The employee must sign and date the SF 312. This can be done in one of two ways:

- Using an authorized digital signature, or

- Signing in the presence of an authorized witness (can be done remotely via video technology like Teams, Zoom, etc.). Witnesses can be any authorized representative of the contractor or U.S. executive branch employee. Third parties such as notaries, outside legal counsel, or friends/family are strictly prohibited from acting as witnesses.

Step 3: Official Acceptance and Submission

To make the agreement official, the FSO, or their designee, must sign the acceptance block. This can be a traditional "wet" signature or an authorized digital signature. An SF 312 uploaded to DISS without this acceptance signature will be rejected.

Once fully executed, the FSO or designee should upload the SF 312 to the person summary screen in DISS. Contractors are authorized to maintain a copy for their administrative records.

PSI DATA COLLECTION FOR INDUSTRY THROUGH NISS

DCSA is responsible for projecting Personnel Security Investigations (PSI) requirements each year. The data collection for PSI projection requirements will be conducted March 2 through March 27, 2026, through the NISS Submission Site. Annual projections acquired from Industry through this collection are the key components in DoD program planning and budgeting for NISP security clearances.

In preparation for this upcoming data collection, our Industry partners are highly encouraged to register for their NISS accounts before March 2 to participate in the survey. Registration instructions are found on the NISS website under the Industry Registration section.

We look forward to your participation. If you have any questions, please contact: dcsa.ncr.dcsa.mbx.psiprogram@mail.mil.

SCHEDULING YOUR FIRST SELF-INSPECTION

As a new partner in the NISP, understanding your compliance responsibilities is paramount. Based on recent clarifications, this article provides the updated timeline for conducting your facility's very first self-inspection after being granted a Facility Clearance (FCL).

Your First Deadline: Self-inspection Within 12 Months of FCL

The updated guidance clarifies the timeline for a facility's initial self-inspection. A facility must conduct its first self-inspection within the first 12 months after being granted an FCL. This initial inspection is a foundational step to validate the effectiveness of your new security program and ensure all protocols are properly implemented from the start.

After this initial inspection, your facility will then move to an annual schedule, where a self-inspection is required once per calendar year thereafter.

Example Scenario: If your facility is granted an FCL on April 1, 2025, your first self-inspection must be completed by March 31, 2026. Your next self-inspection would then be due anytime during the 2027 calendar year.

Aligning with the DCSA Initial Security Review

The 12-month deadline for your initial self-inspection aligns perfectly with another critical milestone: the DCSA Initial Security Review. This formal assessment, conducted by your DCSA representative, typically occurs between 12 and 15 months after your FCL is granted.

Strategic Advantage in Completing of Your Self-Inspection

By completing your mandatory self-inspection within the 12-month window, you are simultaneously preparing for your official DCSA review. The internal audit serves as the perfect "dress rehearsal" for you to identify and mitigate any potential issues before the DCSA Initial Security Review. Completing your self-inspection on time demonstrates a proactive and mature security posture to DCSA right from the beginning. As a recommended resource, you may use the Self-Inspection Handbook for Contractors which can be found at NISP Tools & Resources.

OFFICE OF COUNTERINTELLIGENCE WEBINAR

DCSA invites cleared industry and academic professionals to an unclassified webinar on March 19, 2026, from 1:00 to 2:30 p.m. ET, entitled "CHASING CHI: The Historic Pursuit and Capture of Insider Threat Actors." Retired Federal Bureau of Investigation Supervisory Special Agent James E. Gaylord discusses how he, his squad, and other government agencies worked together using every available covert technique to overcome numerous internal obstacles and to investigate and convict six agents of China for stealing U.S. naval, aerospace, and space technologies. This session is designed for cleared industry and academic personnel, including leaders, security professionals, engineers, and cybersecurity experts.

The registration link will be available on the CDSE Webinar page in mid-February.

CLARIFYING GUIDANCE ON U.S. CITIZENSHIP VERIFICATION

To ensure full compliance and maintain the integrity of the security clearance process, we are providing essential clarification for our industry partners regarding the verification of U.S. citizenship for applicants requiring access to classified information. Adherence to these procedures is required.

Core Requirement: Your FSO or an authorized representative must verify the U.S. citizenship of every applicant. This verification must be based on the list of acceptable documents outlined in 32 CFR 117.10(c). To provide further clarity, please see the following guidance on specific documents and systems:

Document/ System	Acceptable Proof for PCL Applicants?	Reason
Enhanced Driver's License (EDL)	No	An EDL is a secure document issued by certain border states that serves as proof of both identity and citizenship for specific land and sea border crossings. However, the EDL is not listed as an acceptable document in the NISPOM to corroborate U.S. citizenship for security clearance applicants.
Form I-551 (Green Card)	No	Though referenced in 32 CFR 117.10(c)(2)(ii), the Form I-551 (Permanent Resident Card or passport stamp) confirms that a person is a lawful permanent resident (green card holder) or conditional resident, not a U.S. citizen.
Standard REAL ID	No	A REAL ID confirms identity and lawful presence, but since non-citizens can obtain one, it does not corroborate U.S. citizenship.
DISS Verification	No	The Defense Information System for Security (DISS) is an internal government database and cannot be used as an official source to validate U.S. citizenship for security clearance applicants.

Mandatory In-Person Verification: It is crucial that applicants present either the **original documents or certified copies** for verification. To confirm the integrity of the documentation, the FSO or representative must view the documents in person.

- **Prohibited Methods:** Using email, video technology, or any other remote method to view citizenship is **not authorized**.

Using a Third Party for Verification: In cases where operational needs prevent your FSO or representative from conducting the verification in person, you may authorize a trusted third party.

- **Authorized Parties:** Examples include notaries, outside legal counsel, or other government representatives.

- **Written Procedures Required:** Before a third party can act on your behalf, your company must establish clear, written procedures. These procedures must ensure the third party is fully aware of their obligation to validate U.S. citizenship using only the authorized documents and must outline exactly how they will communicate the successful validation back to your FSO.

We encourage you to review and update your internal procedures to align with this guidance.

TOP REVIEW DEFICIENCY #5: INSIDER THREAT TRAINING

Proactive preparation is the key to a successful security review. To better equip our valued industry partners, we are launching a series that breaks down the top five most common deficient findings from Fiscal Year 2025. As announced in our December 2025 VOI Newsletter, this series will count down the top five deficiencies over the next few months, offering insights and resources to bolster your security programs. This month, we begin our countdown with Deficiency #5: Insider Threat Training.

Common Issues to Avoid: To ensure your program is compliant, it is crucial to avoid these common oversights:

- **Initial Training Delays: Failing to provide** initial insider threat awareness training to all newly cleared employees *before* granting access to classified information can leave your organization vulnerable.
- **Annual Training Lapses: Neglecting to conduct** annual insider threat awareness training for all cleared employees is a common pitfall. This training must cover the minimum requirements outlined in 117.12(g)(2).
- **Insufficient Training for Program Personnel: Forgetting to provide** specialized training for your insider threat program personnel, including the Insider Threat Program Senior Official (ITPSO), is a critical error. This training must meet the specific requirements detailed in 117.12(g)(1).

Key Resources at Your Fingertips: To assist you in developing and maintaining a compliant training program, the DCSA provides a wealth of resources. We strongly encourage your ITPSO and security staff to leverage them. We recommend bookmarking these resources and integrating them into your training cycle today.

Resource	Description
eLearning: Insider Threat Awareness, INT101.16	This 1-hour course provides an option for contractors to train their cleared employees on insider threat, satisfying the requirements of 32 CFR 117.12(g)(2).
eLearning: Insider Threat for Industry Curriculum, INT333.CU	This 5-hour curriculum provides an option for contractors to train their insider threat program personnel, satisfying the requirements of 32 CFR 117.12(g)(1).
Insider Threat Training for Cleared Industry Slick Sheet	This slick sheet provides an overview of insider threat training requirements for program personnel and cleared employees.
Insider Threat Information Paper	This information paper highlights the changes to the DCSA designated training for insider threat program personnel that took effect on July 1, 2025.
CDSE Insider Threat Toolkit	The Training and Awareness Module within this toolkit provides a variety of resources to help you develop an effective program.

By focusing on these key areas and utilizing the available resources, you can significantly strengthen your defense against insider threats and ensure a successful security review. Stay tuned for our next article, where we will continue our countdown and explore Deficiency #4.

NAESOC

SECURITY REVIEWS WITH THE NAESOC

- An ISR with the National Access Elsewhere Security Oversight Center (NAESOC) will contact your facility to provide the requirements for your remote security review and to schedule a convenient time. These remote reviews work best if your facility has completed all pre-review activities beforehand. Feel free to reach out to the NAESOC Help Desk if you have any questions.
- Remember to report all changed conditions in the National Industrial Security System (NISS). Please include business documentation with your reports. If you have questions about your review, contact your ISR or the NAESOC Help Desk. For urgent issues, please use the Blue Button on the NAESOC website.

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

NISS REMINDER: 2026 ESSENTIAL PROFILE UPDATES

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.

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

OPEN STORAGE AREA SELF-APPROVAL AUTHORITY

In partnership with the National Industrial Security Program Policy Advisory Committee (NISPPAC) Industry Group, DCSA developed procedures for cleared defense contractors to self-approve their open storage areas (OSAs) at their facilities. These procedures became 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, see the Self-Approval Authority tab under Industry Tools of the NISP Tools & Resources page under National Industrial Security Program Oversight on DCSA.mil.

INTERNATIONAL VISIT REQUEST PROCEDURES UPDATE

Effective Monday, March 2, 2026, there is a new requirement for submitting all outgoing international visit requests, including those to NATO sites.

Here are the key details of this change:

- **New Template Required:** All requests must be submitted using the official Request for Visit (RFV) Instructions and Template.
- **Country-Specific Exceptions:** This new rule does not apply to countries that have their own specific template available on the DCSA website. Please check the website to ensure you are using the correct template.
- **Rejections:** Any submission that is not on the correct template will be rejected.

For any questions regarding this change, or to download the correct forms, please refer to the following resources:

- **Website:** Find the latest information and templates on DCSA's Outgoing International Visits Page.
- **Email:** For further assistance, contact the DCSA RFV office at dcsa.rfv@mail.mil.

PERSONNEL VETTING REALIGNMENT UPDATES

Over the past several years, the Department's personnel security enterprise has undergone significant organizational transformation to better align with evolving policy, mission requirements, and the Trusted Workforce framework.

Approximately 2 years ago, the DoD Consolidated Adjudications Services (CAS), Personnel Security Management Office (PSMO), and Continuous Vetting (CV) functions were merged into a single organization known as Adjudication and Vetting Services (AVS). This consolidation marked an effort to streamline operations and integrate closely related mission areas under one enterprise structure.

In 2025, the organization underwent another restructuring accompanied by a directorate name change. The directorate formerly known as Personnel Security has been renamed Personnel Vetting (PV) to better align with Trusted Workforce policy language and reflect the evolving scope of its mission. As part of this realignment, several mission areas that had previously been merged have since de-merged, while remaining under the broader Personnel Vetting umbrella.

As the organization continues to refine its mission scope and operational processes, stakeholders may notice updates to both workflows and the DCSA website, including changes to organizational names and terminology.

Key organizational updates include:

- CAS is now known as Trust Decisions (Adjudications).
- PSMO-I (also formerly known as VRO and DISCO) is recycling its pre-merger name. This office will continue to manage front-end Personnel Clearance Level (PCL) processing and some incident report management for our Industry population.
- Continuous Vetting (CV) is also keeping its original name and will continue to process CV alerts for DoD Industry and civilian populations as well as other government agencies across the federal enterprise.
- Background Investigation's (BI) name and mission remain unchanged.

As Personnel Vetting continues to evolve, leadership remains focused on finalizing process improvements and clearly defining mission responsibilities. Additional updates and clarifications will be communicated as these changes are implemented across the enterprise.

SECURITY TRAINING

CDSE PULSE

The January edition of The Pulse is now available in CDSE's Electronic Library. Stay in the loop with CDSE products and updates by subscribing to direct delivery!

NEW 2026 INDUSTRIAL SECURITY PROGRAM ANNUAL PLANNER

The new Industrial Security Program Annual Planner job aid serves as a supplemental tool to support industrial security training and awareness. The job aid combines performance support tools from a variety of security content areas that comprise the industrial security discipline to promote security awareness throughout the year.

DD FORM 254: ISSUING SUBCONTRACTS

The DD Form 254 is a critical tool for ensuring compliance. Check out CDSE's new video, "DD Form 254: Issuing Subcontracts," which covers key elements for a prime contractor to accurately complete and issue a subcontractor DD 254. This short video ensures that from the initial bid to final termination, every party involved in a classified contract understands their security obligations.

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)

May 4 - 8, 2026 (Linthicum, MD)

INDUSTRIAL SECURITY:

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

March 24 - 27, 2026 (Virtual)

May 12 - 15, 2026 (Virtual)

July 21-24, 2026 (Virtual)

INFORMATION SECURITY:

Activity Security Manager VILT IF203.10

April 19 - May 17, 2026 (Virtual)

INSIDER THREAT:

Insider Threat Detection Analysis VILT INT200.10

February 9 - 13, 2026 (Virtual)

March 16 - 20, 2026 (Virtual)

April 13 - 17, 2026 (Virtual)

May 11 - 15, 2026 (Virtual)

PHYSICAL SECURITY:

Physical Security and Asset Protection PY201.01

February 2 – 6, 2026 (Linthicum, MD)

April 6 – 10, 2026 (Linthicum, MD)

May 11 – 15, 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 10 – 13, 2026 (Hawaii)

April 21 – 24, 2026 (Linthicum, MD)

May 12 – 15, 2026 (Linthicum, MD)

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.

CONTACTS

DCSA Knowledge Center - 1-878-274-2000

National Background Investigation Services (NBIS) -

Support Help Desk/Customer Engagements 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