DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

March 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

NI2 "GO LIVE"

The refactored and enhanced National Industrial Security System (NISS) Increment II (NI2) "Go Live" deployment occurred on January 30, marking a significant step forward in DCSA's mission to streamline and enhance industrial security for our government and industry partners. We extend our sincere gratitude to our stakeholders, whose invaluable participation in User Acceptance Testing and User Validation was instrumental to this achievement.

As of January 30, 2026, the legacy NCCS application was disabled, and all capabilities, including the DD 254 workflow, was successfully migrated to the new NI2 environment.

Accessing the New System & Resources

Resource	Link
NI2 Environment	https://niss.dcsa.mil
NI2 Information Page	https://www.dcsa.mil/Systems-Applications/NI2-National-Industrial-Security-System-Increment-II/
Support & Issue Reporting	dcsa.meade.peo.mbx.ni2@mail.mil

Important Information for a Smooth Transition

- **No Re-registration Required**: Your existing profile has been migrated. You will only need to perform a profile check upon your first login.
- **Profile Changes:** Please refrain from making any changes to your profile at this time.
- **Role Verification:** You may not see all of your assigned roles during the initial verification process. However, all roles will be visible once you are in the application.
- **Browser Issues?** If you experience any browser-related problems, please try the following:
  1. Clear your browser's cache and re-enter the URL.
  2. If the issue persists, try a different browser.
  3. If you still experience problems, please contact the helpdesk at the email address listed above.

What's Next?

To continue modernizing our industrial security systems, we plan to integrate functionality from the NISS into the NI2 in the first quarter of fiscal year 2027. This will create a more secure and accessible NI2 ecosystem on the Cloud.

Important Information

To ensure your account remains active, please sign into NI2 at least once every 30 calendar days.

For any questions or assistance, please contact us at dcsa.meade.peo.mbx.ni2@mail.mil.

For additional information, please visit DCSA's NI2 (National Industrial Security System, Increment II) website.

CRITICAL INDUSTRY RAP BACK ENROLLMENT TASKS

DCSA officially announced the expansion of Rap Back enrollment, a crucial step in our transition to the Trusted Workforce 2.0 continuous vetting model in which FSOs were requested to complete three critical and time-sensitive tasks by April 1, 2026. If you have not already done so, please take action as soon as possible to:

1. Distribute FBI Advisements:

   - Provide the following advisements to all cleared employees associated with your SMO/CAGE Code:

     - FBI Privacy Act Notice

     - Noncriminal Justice Applicant's Privacy Rights.

   - Maintain documentation of advisement distribution for potential audits. This process must be completed by April 1, 2026.

     - It is important to note that while providing the advisement is mandatory, there is no requirement for personnel to sign the form. Consider documenting the distribution method and date for internal records.

2. Update Onboarding Procedures:

   - Integrate FBI advisements into onboarding processes for new personnel.

3. Acknowledge Completion:

   - Please click on the following link when the FBI advisements have been distributed to your employees and provided the information being requested to acknowledge completion: FBI Advisements Acknowledgment.

For complete details on the phased rollout and program background, please review the full DCSA announcement.

Any questions pertaining to Rap Back for Industry, please reach out to your Industry Liaisons at dcsa.boyers.dcsa.mbx.industry-agency-liaison@mail.mil.

PERSONNEL VETTING UPDATED INTERVIEW METHODS

DCSA has implemented significant updates to its interview procedures as part of its transition to the 2022 Investigative Standards (INVS). These changes, which prioritize remote interview methods, are designed to increase efficiency, reduce investigation timelines, and get personnel into their roles faster.

New Preferred Interview Methods

To provide more flexibility based on the type of investigation and associated risk level, DCSA has established new preferred methods for conducting subject and source interviews.

Interview Type	Preferred Method
Subject Interviews	Video Teleconferencing (VTC)
Source Interviews	VTC or Telephone

Boosting Efficiency and Reducing Delays

This strategic shift to remote interviews aims to streamline the entire vetting process. By reducing the reliance on travel, DCSA anticipates a significant reduction in delays, leading to a more efficient experience for both cleared facilities and their covered individuals. The core benefits of these updates include:

- **Faster Timelines:** Reducing travel and scheduling constraints will directly contribute to shorter investigative periods.
- **Increased Flexibility:** Investigators can now select the most appropriate and effective method for each specific case.
- **Reduced Waste:** The changes are expected to eliminate waste associated with unnecessary travel and logistical hurdles.

The Continued Role of In-Person Interviews

While VTC and telephone interviews are now the preferred standard, in-person interviews will continue to be a vital tool. They will be utilized when it is determined to be more effective, required by the INVS, or deemed necessary to resolve issues related to known behaviors. This ensures that the integrity of the investigation is maintained while still prioritizing efficiency.

DCSA's modernization of its interview process marks another step forward in its commitment to transforming and improving personnel vetting for the entire industry.

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

NBIS HOSTS SECOND PRODUCT DAYS

NBIS hosted its second Product Days event on March 3 and 4. Approximately 78 attendees participated in person, representing various agencies and industries. Product Days represents NBIS' commitment to developing a modernized, customer-centric suite of systems that supports the Trusted Workforce 2.0 initiative. By bringing together stakeholders from federal agencies and Industry, NBIS ensures products are designed with real-world needs in mind.

Product Owners from the Vetting Risk Determination (VRD), the Individual Engagement Portal (IEP), and the Adjudication Management Platform (CATS) provided updates and insights on the future NBIS Suite of Systems. During the event, NBIS leadership asked attendees to be honest and share feedback on system improvements. Attendees participated in hands-on breakout sessions focused on user experience (UX) and user interface (UI) design. Working in small groups, they conceptualized their ideal product features, which were then transformed into wireframes by the NBIS UX/UI Team. These wireframes were presented for real-time feedback, fostering a dynamic and iterative design process.

Product Days was valuable for NBIS personnel and attendees alike, fostering open communication and collaboration. NBIS will continue to host Product Days to ensure they develop products with a customer-centric approach.

INDIVIDUAL ENGAGEMENT PORTAL (IEP) STATUS TRACKER DEBUT

As of March 5, any new individuals undergoing an investigation process will use the IEP Status Tracker.

The IEP Status Tracker is an intuitive tool that modernizes an individual's interaction with the federal personnel vetting process. Developed as part of the Trusted Workforce 2.0 reforms, it is an optional shared service that replaces legacy systems with a single, transparent interface allowing individuals to:

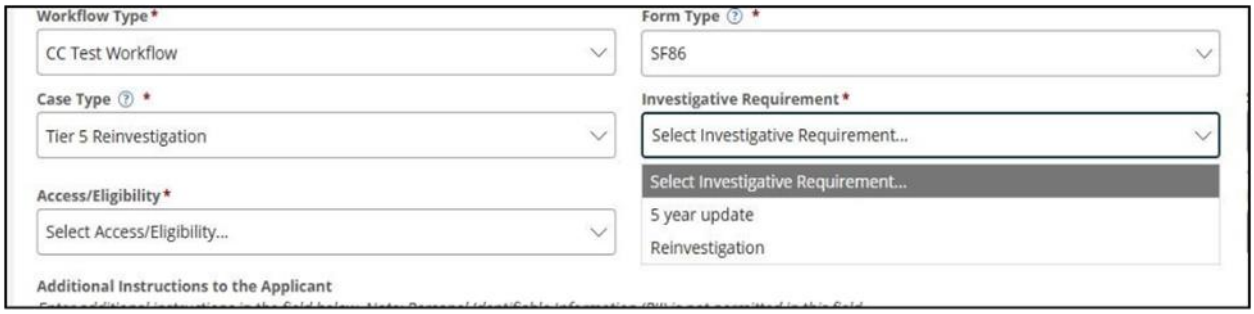
- Securely self-report information
- Track the status of current and past investigations
- Receive updates throughout the vetting lifecycle
- Communicate securely with government personnel.

These features simplify the process, reduce administrative burdens, and improve the overall user experience. The platform delivers a modern, transparent vetting experience that onboards trusted personnel faster, helping customers to attract and retain top-tier talent. By improving the speed and quality of the vetting process, the IEP directly safeguards our Nation's information.

The platform will continue to be improved to enhance the user experience. As the Status Tracker is enhanced, additional user groups will use it.

NBIS RELEASES NEW FIVE-YEAR UPDATE GUIDANCE

On March 5, NBIS updated the Order Form to simplify the submission process for reinvestigations and Continuous Vetting (CV) enrollments. Industry stakeholders must select the '5 year update' option unless a Government authority explicitly directs them to choose 'Reinvestigation.' Additionally, when submitting, industry stakeholders should continue to use 'CV Update' in the Contract Number Field.



Key Updates:

- A new '5 year update' option has been added to the Investigative Requirement Field.
- The "Initial" option has been removed for the following case types:
  - Tier 2 Reinvestigation (T2R)
  - Tier 3 Reinvestigation (T3R)
  - Tier 4 Reinvestigation (T4R)
  - Tier 5 Reinvestigation (T5R).

Purpose of Request	Case Type Selection	Investigative Requirement Selection	Outcome (Selection is modifiable before release)
5-Year Update / CV Enrollment / Form Collection*	Tier 2 Reinvestigation Tier 3 Reinvestigation Tier 4 Reinvestigation Tier 5 Reinvestigation	5 year update	The request will be routed directly to CV
Standard Reinvestigation	Tier 2 Reinvestigation Tier 3 Reinvestigation Tier 4 Reinvestigation Tier 5 Reinvestigation	Reinvestigation	The request will be processed as a standard reinvestigation

*Industry partners must use the '5 year update' option unless explicitly directed to select 'Reinvestigation' by DCSA or another Government authority.

Future Transition to DISS

NBIS is transitioning to the NBIS Agency platform for the Defense Information System for Security (DISS) to handle all Initiate, Review, and Authorize (I/R/A) functions. NBIS appreciates Industry's cooperation and patience as it works to modernize and improve the personnel vetting process.

DCSA INDUSTRY STAKEHOLDER ENGAGEMENT

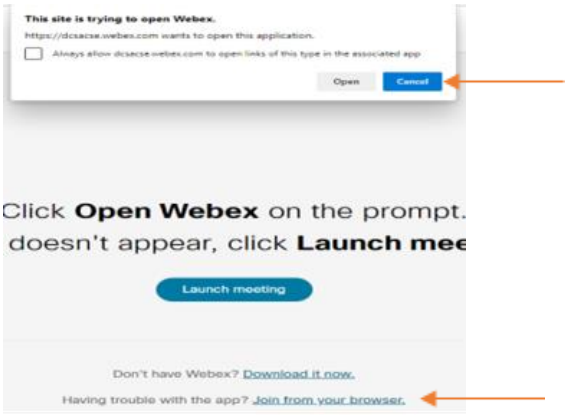
The DCSA Customer & Stakeholder Experience (CSE) Team will host the next quarterly Industry Stakeholder Engagement (ISE) on April 14, 2026, from 10:30 a.m. to 12:00 p.m. ET for all Industry FSOs and Security Professionals. The last engagement, held on January 13, resulted in an outstanding attendance of over 650 FSOs and Industry Security Professionals and focused on CMMC, NI2, and NISS.

The April 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 Metrics and Updates
  - Continuous Vetting and Trust Decision Metrics and Updates
- NBIS Service Level Management – NBIS Updates
- Counterintelligence – MCMO - Methods of Contact, Methods of Operation
- 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.



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

Phone: +1-415-527-5035

Access Code: 2825 040 8871

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

OFFICE OF COUNTERINTELLIGENCE SVTC

DCSA invites cleared members of the defense industrial base to participate in a classified SVTC. In partnership with the Federal Bureau of Investigations (FBI), agents and analysts will present on "Potential Disruption of Sensitive and Classified Shipments in Commercial and Government Shipping." The presentation will inform industry partners about vulnerabilities and documented incidents affecting shipments of sensitive or classified information, hardware, and components.

The SVTC will be hosted in-person at most DCSA field offices on Thursday, April 9, 2026, from 1:00 to 2:30 p.m. ET. Please register here by Thursday, April 2, 2026.

SECURITY REVIEW RATING RESULTS FISCAL YEAR 2026

The following security review results are current as of March 25, 2026:

Overall Fiscal Year Goal:	3,900	
Rated Security Reviews Completed:	1,455	(37.3%)
Rated Security Reviews Remaining:	2,445	(62.7%)
Superior Ratings Issued:	140	(9.6%)
Commendable Ratings Issued:	491	(33.7%)
Satisfactory Ratings Issued:	818	(56.2%)
Marginal Ratings Issued:	2	(00.1%)
Unsatisfactory Ratings Issued:	4	(00.3%)

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.

TOP REVIEW DEFICIENCY #3: SELF-INSPECTIONS

Proactive and thorough self-inspections are your best defense against security vulnerabilities and one of the surest paths to a successful DCSA security review. As part of our series on the top five security review deficiencies from Fiscal Year 2025, this month we're tackling #3: Contractor Self-Inspections.

Think of your annual self-inspection not as a chore, but as a critical health check-up for your security program. It's your opportunity to find and fix issues on your own terms before they become findings in an official DCSA review. A strong self-inspection process is the foundation of a robust security posture, ensuring you are consistently safeguarding classified information and contributing to National Security.

Common Issues to Avoid: Avoid these common issues to keep your program on track:

- **Missing or Delayed Reviews: Failing to conduct** a formal self-inspection at least once every calendar year and, if you have classified information systems, reviewing their components every 12 months. For newly cleared entities, your first inspection is due within 12 months of receiving your facility clearance.

- **Incomplete Reviews: Neglecting to include** all elements of the industrial security program based on the facility's operations and involvement with classified activity (scope) at a sufficient level that could reasonably identify deficiencies (depth). This includes a review of the classified activity, classified information, classified information systems, conditions of the overall security program and the insider threat program, and samples representing the facility's derivative classification actions, as applicable.

- **Missing Formal Report: Forgetting to prepare** a formal report that details the self-inspection findings and how any discovered issues were resolved. You must retain this report for evaluation during your next DCSA security review.

- **Lack of Management Support: Failing to have** management support during the self-inspection and during remedial actions taken because of the self-inspection. This includes the Senior Management Official (SMO) certifying to DCSA annually that a self-inspection has been conducted, that other cleared Key Management Personnel (KMP) have been briefed on the results of the self-inspection, that appropriate corrective actions have been taken, and that management fully supports the security program at the cleared facility.

Key Resources at Your Fingertips: DCSA provides a wealth of resources to support your self-inspection process. We strongly encourage you to bookmark these links and use them in your regular training and preparation.

Resource	Description
Self-Inspection Handbook for Contractors	A step-by-step guide to building a compliant and thorough self-inspection process.
CDSE Self-Inspection Course (IS130.16)	A free eLearning course that covers the A-to-Z of preparing for, conducting, and documenting your self-inspection.
CDSE FSO Toolkit: "Self-Inspections" Module	Provides practical checklists, templates, and job aids directly related to self-inspections.
DCSA Security Review & Rating Process Page	Resources to help align your self-inspection with DCSA's official review and rating criteria to ensure you're looking for what we're looking for.

By mastering your self-inspection process, you transform it from a simple requirement into a powerful tool for continuous improvement.

Coming Up Next: Our next article we will explore **Top Deficiency #2: Reporting Requirements**. If you have questions related to this article, please email the NMP Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

DIGITAL SIGNATURE OPTION FOR DD 441 & SF 328

Good news for our industry partners. DCSA now accepts digital signatures on two more forms:

- DD Form 441 (DoD Security Agreement)
- SF 328 (Certificate Pertaining to Foreign Interests).

This change is part of a government-wide effort to make processes simpler and more efficient. It means the rules for these forms now match the rules for the SF 312.

What You Need to Know

1. What kind of digital signature can I use?

You must use a signature from a DoW-approved source. This includes:

- A DoW Common Access Card (CAC)
- An approved certificate from the External Certification Authority (ECA) Program (this is the most common option for industry partners who don't have CACs)
- Other DoW-approved external PKI.

2. Where can my company get an approved ECA certificate?

You can find a list of approved providers on the DoD Cyber Exchange website.

3. Do I have to use a digital signature?

No. use of a digital signature is optional. We will still accept traditional "wet" (ink) signatures.

4. If I use a digital signature, do I still need a witness?

No. An approved digital signature does not require a witness.

Where to Find More Information

- For detailed instructions, please see the Job Aid for Digital Signatures on the Standard Form 312 dated February 20, 2024.
- The FCL Orientation Handbook will also be updated with this new information to help companies that are new to the facility clearance process.

UPDATED NSA/CSS POLICY MANUAL

In February 2026, the National Security Agency/Central Security Service (NSA/CSS) updated their NSA/CSS Policy Manual 9-12, Storage Device Sanitization and Destruction Manual for disposal or recycling of devices that store information ranging from Unclassified to Top Secret and may include compartmented, sensitive, or limited-distribution material.

NSA/CSS also just updated their Evaluated Products Lists (EPLs). These EPLs cite equipment that meets NSA specifications, apply to all NSA/CSS elements, contractors, and personnel using information systems, and pertain to all information system storage devices that they use.

The NSA/CSS Policy Manual and EPLs are instrumental reference documents for industry partners to effectively manage classified information systems. Please contact your representative with any questions

NEWLY RELEASED SF 89 REPLACES FORMER VERSION

The new General Services Administration (GSA) Standard Form 89 (SF 89), Maintenance Record for Security Equipment, has just been released. It is a fillable PDF form and the official document to record all maintenance, repairs, and inspections for GSA-approved security containers, vault doors, and pedestrian door locks. The GSA Standard Form 89 is cited in FED-STD-809E and replaces the now obsolete Optional Form 89 (OF 89) cited in the superseded FED-STD-809D.

The GSA Standard Form 89 serves as a complete historical log of all servicing activities performed on the container, which is critical for maintaining the integrity of the security equipment. This form should be stored inside the container or vault.

Although the technician performing the work will fill out the technical repair details, the container's custodian (e.g., Security Manager, Special Security Officer) is ultimately responsible for the form's accuracy and maintenance.

The GSA Standard Form 89 may be found on the DoW Lock Program website here or in the GSA Forms Library.

PROCURING GSA-APPROVED CONTAINERS

Only containers certified and badged by the General Services Administration (GSA) may be used to secure classified information. Federal Standard 809E (FED-STD-809E) establishes uniform procedures for the inspection, maintenance, neutralization, and repair of GSA-approved security containers to ensure their integrity for the protection of classified material. FED-STD-809E contains critical provisions regarding the purchase or transfer of these containers.

PURCHASE OF GSA-APPROVED CONTAINERS

Information Security Oversight Office (ISOO) Notice 2014-02: Procurement of Security Equipment states "GSA approved" security containers and vault doors must now be procured through GSA Global Supply or the GSA Schedule for IPS containers.

Regarding the procurement of GSA-approved security equipment, FED-STD-809E states that products tested and qualified under GSA-approved, limited use specifications are to be sold only to the Federal Government, Government contractors specifically authorized to purchase them, or other organizations or persons specifically authorized or required by the Government to use them.

To summarize, GSA-approved security containers can only be purchased directly through GSA Global Supply. You cannot buy a security container from an unauthorized third-party vendor and have it approved for storing classified information.

DIRECT SALE OR TRANSFER BETWEEN CLEARED ORGANIZATIONS

Per Fed-STD-809E, direct sales or transfers of current Red Label GSA approved security containers between two U.S. Government or industrial organizations that both have active Facility Security Clearances can be authorized by the cognizant Security Authority without the removal of the GSA approval label provided:

1. The transfer of the GSA approved security containers can be securely accomplished (escorted movement), and,
2. The security containers are inspected upon arrival within the accredited facility by a GSA Certified Inspector prior to the storage of classified information.

This recertification inspection ensures that the security integrity of the container was maintained during transport and that it continues to meet GSA standards for safeguarding sensitive contents. The GSA Certified Inspector uses detailed criteria from FED-STD-809E and related GSA documentation to ensure the security container meets stringent requirements for recertification. The inspection is comprehensive, covering the container's physical integrity, the locking mechanism, and all associated documentation.

DOCUMENTATION AND RECERTIFICATION

Proper documentation is essential for maintaining the security and accountability of the container. The inspector will verify the presence and correct completion of SF 700, Security Container Information; SF 702, Security Container Check Sheet; and GSA SF 89, Maintenance Record for Security Equipment.

If the container meets all the necessary criteria, the GSA Certified Inspector will affix a new GSA-approved recertification label. This label serves as the official confirmation that the container is authorized for the storage of classified information.

When a container has been opened or repaired in an unauthorized manner, it will not be recertified and the GSA labels must be removed. Additionally, older "black label" containers (manufactured before 1990) have been phased out and are no longer eligible for recertification or use for storing classified materials. Refer to ISOO Notices 2022-03, 2021-01, and Black Label Letter for additional information.

NAESOC

ENHANCED HELP DESK SUPPORT IS COMING!

Select FSOs have been contacted by the National Access Elsewhere Security Oversight Center (NAESOC) to assist in identifying NAESOC Help Desk services upgrades. We're developing, and will be implementing, a ServiceNow-based capability for NAESOC facilities and customers.

What does this mean for you?

This enhanced capability can provide an improved experience where you:

- Request Services - Quickly request services that are available for you.
- Track Progress - View your current and past requests and collaborate directly with us on your requests.
- Manage Your Information - View your profile, services you have received, and much more.

We are now opening this development testing to additional NAESOC facilities. If you are interested in helping identify how this enhancement will work, please email Aneka Francis at dcsa.naesoc.generalmailbox@mail.mil. Volunteers will get early access to the system. Our team will work with you to test and improve the system and any commitment on your part in its development will provide you outsized value and require only a fraction of your time.

STAY CONNECTED WITH THE HELP DESK

- Online Resources - Visit the NAESOC website for direct access to job aids, user guides, and answers to common questions.
- Receive Critical Updates - To ensure you receive all important communications, add dcsa.naesoc.generalmailbox@mail.mil to your email's safe sender list.
- Update Your Profile - Please make sure your NISS profile lists your current points of contact.
- Urgent Issues - For time-sensitive matters, please use the Blue Button *(Escalate an Existing Inquiry)* on the NAESOC website.

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

PERSONNEL VETTING

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) also keeping its original name and will continue to process CV alerts for DoW 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 March 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!

NCMS ANNUAL TRAINING: GETTING STARTED SEMINAR

On June 8, CDSE will host a "Getting Started Seminar (GSS) for Facility Security Officers (FSO)" at the NCMS Annual Training Seminar. This course is not only a great way to get started as a new FSO, but also a way for experienced FSOs to keep informed on industrial security guidance and emerging trends and work in collaboration with other security professionals to explore security topics through practical exercises. Topics include DD 254, insider threat, reporting requirements, counterintelligence, security and contractor reviews, security training and briefings, and personnel security.

Register and complete pre-requisites at Getting Started Seminar for New Facility Security Officers (FSOs) IS121.01. Registration closes on May 15, 2026, and only fully registered participants will be allowed to attend. Registration confirmation will be emailed directly from CDSE. Bring confirmation of GSS registration and a photo ID for class entry on June 8th. You must also be registered for the NCMS Annual Training Seminar to attend the GSS. You will not be fully registered for the GSS until you complete the pre-requisites and submit attestation of NCMS registration in STEPP. *No walk-ins will be allowed*. The GSS is free, and fills up fast, so register today!

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

May 4 - 8, 2026 (Linthicum, MD)

August 17 - 21, 2026 (Linthicum, MD)

INDUSTRIAL SECURITY:

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

May 12 - 15, 2026 (Virtual)

July 21 - 24, 2026 (Virtual)

INFORMATION SECURITY:

Activity Security Manager VILT IF203.10

April 19 - May 17, 2026 (Virtual)

July 26 - August 23, 2026 (Virtual)

INSIDER THREAT:

Insider Threat Detection Analysis VILT INT200.10

April 13 - 17, 2026 (Virtual)

May 11 - 15, 2026 (Virtual)

June 8 - 12, 2026 (Virtual)

PHYSICAL SECURITY:

Physical Security and Asset Protection PY201.01

May 11 - 15, 2026 (Linthicum, MD)

June 8 - 12, 2026 (Linthicum, MD)

SPECIAL ACCESS PROGRAMS:

Introduction to Special Access Programs SA101.01

April 21 - 24, 2026 (Linthicum, MD)

May 12 - 15, 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