



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

February 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

UPDATED PERSONNEL VETTING INTERVIEW METHODS	2
EXPANDED RAP BACK ENROLLMENT IN INDUSTRY	3
SECURITY REVIEW RATING RESULTS	3
INSIDER THREAT TRAINING MANDATE AND EXEMPTIONS	4
CITIZENSHIP VERIFICATION: A ONE-TIME REQUIREMENT	4
TOP REVIEW DEFICIENCY #4: DISS MANAGEMENT	5
OFFICE OF COUNTERINTELLIGENCE SVTC AND WEBINAR	7
SECURE VIDEO TELECONFERENCE (SVTC)	7
UNCLASSIFIED WEBINAR	7
PSI DATA COLLECTION FOR INDUSTRY THROUGH NISS	7
INTERNATIONAL OUTGOING VISITS OUTREACH	8
NAESOC	8
STAY CONNECTED WITH THE HELP DESK	8
CONTACT US	9
PERSONNEL VETTING REALIGNMENT UPDATES	9
SECURITY TRAINING	10
CDSE PULSE	10
NEW 2026 INDUSTRIAL SECURITY PROGRAM ANNUAL PLANNER	10
DD FORM 254: ISSUING SUBCONTRACTS	10
FISCAL YEAR 2026 SECURITY TRAINING COURSES	10
SOCIAL MEDIA	11
REMINDERS	11
CONTACTS	12



UPDATED PERSONNEL VETTING 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.



EXPANDED RAP BACK ENROLLMENT IN INDUSTRY

DCSA is expanding Rap Back enrollments to the broader industry population following a successful pilot program with select early adopters. Rap Back, a service provided by the FBI, enables real-time notifications of changes to an individual’s criminal record using the Automated Fingerprint Identification System (AFIS). This capability is a cornerstone of the Trusted Workforce 2.0 (TW 2.0) Continuous Vetting (CV) framework, ensuring cleared personnel are continuously monitored to maintain eligibility for access to classified information. The phased rollout will begin with industry personnel who already have fingerprints on file, followed by additional populations, and eventually those requiring new fingerprint submissions.

This expansion marks a significant step in modernizing personnel vetting operations, streamlining processes, and reducing administrative costs for industry partners. FSOs play a critical role in this effort by distributing mandatory FBI advisements to cleared employees and integrating these advisements into onboarding procedures. DCSA is committed to transparency and collaboration throughout the rollout, ensuring industry stakeholders are well-informed and prepared for future phases.

For more details, read the full story [here](#).

SECURITY REVIEW RATING RESULTS

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

Overall Fiscal Year Goal:	3,900
Rated Security Reviews Completed:	1,015 (26.0%)
Rated Security Reviews Remaining:	2,885 (74.0%)
Superior Ratings Issued:	96 (9.5%)
Commendable Ratings Issued:	350 (34.5%)
Satisfactory Ratings Issued:	563 (55.5%)
Marginal Ratings Issued:	2 (00.2%)
Unsatisfactory Ratings Issued:	4 (00.4%)

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.



INSIDER THREAT TRAINING MANDATE AND EXEMPTIONS

As previously announced, new training requirements went into effect in July 2025 for cleared industry's insider threat program personnel. A common question we have received is related to exemptions for current or previously appointed program personnel. This article is intended to answer those questions.

The Insider Threat Program Senior Official (ITPSO) is responsible for verifying personnel training status and ensuring compliance with these mandates.

Training Mandate - Program personnel who do not meet exemption criteria must complete one of the following training options:

- The 5-hour CDSE eLearning course, "Insider Threat for Industry Curriculum, INT333.CU"
- A custom contractor-developed program that fulfills all requirements of NISPOM 117.12(g)(1), including the pre-validated NISPPAC Industry Training slides.

Exemption Scenarios - Program personnel may be exempt based on the criteria below:

- **Appointed before July 1, 2025:** Must have proof of completing the CDSE "Establishing an Insider Threat Program" (INT122.16) or an equivalent contractor-developed program.
- **Reappointed after July 1, 2025:** Must have proof of completing the CDSE "Establishing an Insider Threat Program" (INT122.16) course prior to July 1, 2025.

Questions and Additional Resources

For additional details, please refer to the December 2025 "Insider Threat Program Training Requirements" [VOI article](#) and the Insider Threat Training for Cleared Industry Slick Sheet on the DCSA [NISP Tools and Resources](#) page.

If you have questions about your specific situation or eligibility, please email the NMP Division at: dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

CITIZENSHIP VERIFICATION: A ONE-TIME REQUIREMENT

Following the January 2026 Voice of Industry Newsletter, a common question emerged: Is U.S. citizenship verification required for every SF-86 submission, or is it a one-time event?

Key Takeaway: The FSO, or another designated representative, is only required to perform verification of U.S. citizenship in support of an individual's first application for Moderate Tier (MT) or High Tier (HT) investigations. This verification is not required for subsequent security clearance applications once initial eligibility for access to classified information is established.



Clearance Lifecycle: Citizenship Verification Requirements

Application / Citizenship Verification Required?	Reasoning
First Application Yes	This foundational step is mandated by 32 CFR Part 117 to confirm U.S. citizenship before DCSA starts an MT or HT investigation to determine eligibility for access to classified information. U.S. citizenship verification must be based on the list of acceptable documents outlined in 32 CFR 117.10(c). Refer to the January 2026 “Clarifying Guidance on U.S. Citizenship Verification” VOI article for additional guidance.
Subsequent Applications No	Once eligibility for access to classified is granted and verified in the Defense Information System for Security (DISS), subsequent MT or HT applications do not require re-verification of U.S. citizenship (such as for Continuous Vetting Eligibility Upgrades or New Eligibility after a Break-in-Employment). Clarification: If eligibility was not granted in the first application, a subsequent application (e.g., at a new company) is considered the 'first application' and the new FSO or authorized representative must verify citizenship. While it can be used to verify current or previous eligibility, DISS cannot be used to verify U.S. citizenship for a first application.

Optional Practices: When current or previous eligibility is verifiable in DISS, the contractor may choose to re-verify citizenship prior to submitting a subsequent application or granting an individual access to classified information, but they are not required to do so. The contractor may also choose to ask a new employee if there has been any change to their citizenship status since they last worked in a cleared position prior to granting them access to classified information.

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

TOP REVIEW DEFICIENCY #4: DISS MANAGEMENT

Proactive preparation is the key to a successful security review. To better equip our valued industry partners, this series breaks down the top five most common deficient findings from Fiscal Year 2025. Following last month’s article on Insider Threat Training, we now present Deficiency #4: DISS Management.

The Defense Information System for Security (DISS) is the DoW's enterprise-wide system of record for personnel security. Proper management of DISS information is not just an administrative task; it is a critical component of maintaining your facility's security posture and ensuring your personnel can access the classified information necessary for their work without delay.



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

- **Missing or Inactive Accounts:** **Failing to obtain and maintain** active DISS accounts for appropriate security staff. Without an account, your facility cannot manage records, verify clearances, or submit reports, which can halt mission-critical work.
- **Single Point of Failure:** **Neglecting to maintain** at least two active DISS users. Relying on a single user creates a bottleneck when they are unavailable. Since users cannot manage their own records, a second manager is essential for ensuring continuity for all personnel.
- **Outdated Access Levels:** **Forgetting to indoctrinate or debrief** U.S. and NATO access levels in DISS as soon as an individual's status changes. This is vital for maintaining an accurate, real-time record of access authorizations (see Pro-Tip below).
- **Delayed Separations:** **Failing to remove** an employee's access and Security Management Office (SMO) affiliation in DISS upon their termination. Delays in this process pose a significant and unnecessary security risk.

Pro-Tip - Maintaining SMO Affiliations: After debriefing an individual's access, you may maintain their record under your SMO if you determine there is a reasonable expectation they will require access again while employed at your facility. For complete details, refer to the DISS Management Guidance Job Aid.

Key Resources at Your Fingertips: DCSA provides a wealth of resources to help you build and maintain a compliant program. We strongly encourage your security staff to bookmark these pages and integrate them into your training schedule.

Resource	Description
DISS Resources Page	Your central hub for all things DISS. Find job aids, access request forms (PSSAR), training materials, and step-by-step video tutorials.
DISS Management Guidance Job Aid	An essential quick-reference guide with concise instructions for managing access and eligibility, including "break-in-access" and "break-in-employment."
CDSE FSO Toolkit	The Personnel Clearances Module is invaluable, containing checklists, templates, and course links to help build and maintain a fully compliant security program.

Focusing on these key areas and utilizing the available resources can significantly strengthen your security posture and ensure a successful security review. Stay tuned next month for Deficiency #3: Self-Inspections.



OFFICE OF COUNTERINTELLIGENCE SVTC AND WEBINAR

SECURE VIDEO TELECONFERENCE (SVTC)

DCSA invites cleared industry to participate in an SVTC entitled, "Defense Industrial Base Counterintelligence Threat Trends." Counterintelligence (CI) analysts from DCSA's Analysis Division and Cyber Mission Center will provide a classified presentation on DCSA CI products and tools, to include updates of the DCSA annual report "Targeting U.S. Technologies: A report of Threats to Cleared Industry." The SVTC is an in-person event at most DCSA field offices on Thursday, March 12, 2026, from 1:00 to 2:30 p.m. ET.

Please register [here](#) by Thursday March 5, 2026.

UNCLASSIFIED 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.

Please use [this link](#) to register for the event.

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 National Industrial Security System (NISS) Submission Site. Annual projections acquired from Industry through this collection are the key components in DoW program planning and budgeting for NISP security clearances.

The PSI Survey will go live in NISS on March 2, 2026.

In preparation for this upcoming data collection, our Industry partners are highly encouraged to ensure that they have an active NISS account and that they have the correct email and contact information in NISS to receive notifications with additional instructions and updates, or 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.



INTERNATIONAL OUTGOING VISITS OUTREACH

The DCSA International and Special Programs Division is pleased to invite you to a comprehensive webinar on Wednesday, March 25, 2026, at 1:00 p.m. ET.

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

- Completing international outgoing visit requests for cleared U.S. contractors traveling to classified sites
- Understanding when and how to submit requests
- Identifying common errors and how to avoid them
- Navigating different types of visits and required lead times
- Best practices for streamlined processing.

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

Please save the date on your calendar! Click the link [FSO International Visits Outreach](#) to join the meeting on Wednesday, March 25, 2026, at 1:00 p.m. ET.

NAESOC

STAY CONNECTED WITH THE HELP DESK

- **We're here for you!** The Help Desk is your primary point of contact and interaction with the National Access Elsewhere Security Oversight Center (NAESOC). Whether you want to reach a Chief, an ISR, or a Security Specialist, or just need industrial security support, address all your emails to dcsa.naesoc.generalmailbox@mail.mil and we will make sure your message is expedited.
- **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 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 February edition of the [CDSE 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

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

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)

July 26 - August 23, 2026 (Virtual)



INSIDER THREAT:

[Insider Threat Detection Analysis VILT](#) INT200.10

March 16 - 20, 2026 (Virtual)

April 13 - 17, 2026 (Virtual)

May 11 - 15, 2026 (Virtual)

June 8 - 12, 2026 (Virtual)

PHYSICAL SECURITY:

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

April 6 - 10, 2026 (Linthicum, MD)

May 11 - 15, 2026 (Linthicum, MD)

June 8 - 12, 2026 (Linthicum, MD)

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)

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



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

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