



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

May 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

- OFFICE OF COUNTERINTELLIGENCE SVTC2**
- SECURITY REVIEW RATING RESULTS FISCAL YEAR 20262**
- CLASSIFIED MATERIAL DESTRUCTION BY INCINERATION3**
- TOP REVIEW DEFICIENCY #1: CLASSIFIED INFORMATION SYSTEMS4**
- EXTERNAL SYSTEMS AND SECURE MOBILE PLATFORMS5**
- LEGACY HARDWARE EVOLVES TO MODERN MOBILE PLATFORMS5**
- CURRENT PROCEDURES & OVERSIGHT.....5**
- NI2 UPGRADES, NEW TOOLS, STRONGER PARTNERSHIPS6**
- NEW DISS “UNENROLLED” CV STATUS/PROCESS.....7**
- DCSA UPDATES NISP CONTRACTOR CONTINUOUS VETTING PROCESS.....8**
- NAESOC.....8**
- SERVICENOW IMPLEMENTATION ANNOUNCEMENT8**
- WHAT TO EXPECT FROM THE SERVICENOW EXPERIENCE:.....8**
- CONNECT WITH THE NAESOC9**
- CONTACT US.....9**
- SECURITY TRAINING.....9**
- NEW ELEARNING COURSE9**
- INDUSTRIAL SECURITY OFFERINGS.....9**
- CDSE PULSE9**
- FISCAL YEAR 2026 SECURITY TRAINING COURSES.....10**
- SOCIAL MEDIA11**
- REMINDERS11**
- CONTACTS12**



OFFICE OF COUNTERINTELLIGENCE SVTC

In today's global security environment, with rising tensions across multiple regions and an increasingly complex worldwide threat landscape, the safety and security of cleared personnel operating overseas is critical. DCSA invites cleared members of the defense industrial base to join us for a classified Secure Video Teleconference (SVTC) featuring two important presentations.

The "Force Protection Detachment (FPD) Program" is for cleared personnel that regularly operate abroad—where foreign intelligence threats are active and immediate. The FPD Program provides force protection and CI services to safeguard cleared contractors and private industry personnel operating globally. Their services include CI awareness briefings, foreign travel briefs and debriefs, suspicious activity reporting, and CI support to events attended by cleared personnel in their respective area of responsibility. Knowing that trained CI support is available when your personnel are operating OCONUS is critical.

In the "Reporting Rundown," DCSA analysts provide and discuss country-specific threat products highlighting the latest methods and actors utilized by adversarial nations to exploit cleared industry. Products depict activities of threat actors reported during the last fiscal quarter.

The SVTC is an in-person event at most DCSA field offices on Thursday, June 11, 2026, from 1:00 to 2:30 p.m. ET. The overall classification of the briefing is SECRET// NOFORN. Please register [here](#) by Thursday June 4, 2026.

SECURITY REVIEW RATING RESULTS FISCAL YEAR 2026

The following security review results are current as of May 26, 2026:

Overall Fiscal Year Goal:	3,900	
Rated Security Reviews Completed:	2,384	(61.1%)
Rated Security Reviews Remaining:	1,516	(38.9%)
Superior Ratings Issued:	251	(10.5%)
Commendable Ratings Issued:	849	(35.6%)
Satisfactory Ratings Issued:	1,274	(53.4%)
Marginal Ratings Issued:	4	(00.2%)
Unsatisfactory Ratings Issued:	6	(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 Operations Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.



CLASSIFIED MATERIAL DESTRUCTION BY INCINERATION

In accordance with [32 CFR Part 117.15\(g\), National Industrial Security Program Operating Manual \(NISPOM\)](#), cleared contractors must destroy classified material completely to prevent recognition or reconstruction. While many contractors utilize mechanical destruction equipment (e.g., shredders, disintegrators), incineration is a fully authorized method. However, because incineration processes are not evaluated mechanically by the National Security Agency (NSA), contractors often seek clarification on how to remain compliant with DCSA and NISP requirements when using this method.

Since January 1, 2011, only "equipment" listed on an Evaluated Products List (EPL) issued by NSA (found [here](#)) may be utilized to destroy classified information using any method covered by an EPL. Cleared contractors are advised that the NSA/CSS EPL does not include incinerators.

Rather than procuring "approved equipment," contractors must ensure their incineration process meets the minimum temperature thresholds established in the [NSA/CSS Policy Manual 9-12, Storage Device Sanitization and Destruction](#) to achieve complete destruction (e.g., >233°C for paper to be reduced to ash, >670°C for hard disk drives). The contractor is responsible for verifying that the facility used can consistently reach and maintain these temperatures.

When utilizing incineration, cleared contractors must strictly adhere to the following security protocols:

- **Continuous Control:** Classified material must remain under the continuous control of appropriately cleared contractor personnel until the incineration process is complete.
- **Off-Site / Commercial Incinerators:** If a contractor utilizes a municipal, commercial, or off-site incinerator, the material must be transported securely by cleared personnel. The cleared escort(s) must maintain positive control of the material and visually witness its introduction into the incinerator.
- **Witnessing Requirements:** The destruction of Top-Secret material requires two cleared witnesses. The destruction of Secret and Confidential material requires one cleared witness. The escort/witness must verify the material is actively being consumed by the fire/furnace and cannot be recovered before departing the facility.
- **Environmental Compliance:** DCSA reminds contractors that while incineration is a security-approved method, contractors must independently ensure compliance with all applicable Environmental Protection Agency (EPA) and local clean air regulations. DCSA does not waive environmental requirements.

Contractors intending to use incineration (especially off-site commercial facilities) should document this process in their facility's Standard Practice Procedures (SPP). DCSA's prior written approval is required for the use of public destruction facilities. Furthermore, records of destruction must be maintained for Top Secret material (and Secret material, if required by the Government Contracting Activity).

Cleared contractors should contact their assigned Industrial Security Representative or Information System Security Professional (ISSP) for facility-specific questions regarding the safeguarding and transport of classified material for incineration.



TOP REVIEW DEFICIENCY #1: CLASSIFIED INFORMATION SYSTEMS

To help our industry partners prepare for successful security reviews, we conclude our countdown of the top FY25 deficient findings with Deficiency #1: Classified Information Systems.

Interestingly, while 32 CFR 117.18(b) was our most-cited reference, it applied to only 13.5% of NISP facilities—those with current or pending authorized systems. For these facilities, managing this critical area requires constant vigilance.

Common Issues to Avoid: To ensure compliance, avoid these common oversights. (Note: This list is not exhaustive; industry must review [32 CFR 117.18\(b\)](#) in its entirety).

- **Inadequate Risk Controls:** Failing to fully implement the required Risk Management Framework or an overall risk-based set of management, operational, and technical security controls.
- **Lifecycle Vulnerabilities:** Lacking policies and procedures that reduce information security risks throughout the entire system life cycle.
- **Spill Management Failures:** Missing plans and procedures to assess, report, isolate, and contain data spills, including sanitization and recovery methods.
- **Insufficient Training & Awareness:** Not providing required security training or failing to reinforce user responsibilities via system banners and user agreements.
- **Insider Threat Gaps:** Neglecting key insider threat policies, such as user activity monitoring, information sharing, continuous monitoring, and restricting automated log access to privileged users.
- **Change Control Deficiencies:** Lacking change control processes for configuration management and identifying security-relevant changes that require re-authorization.

Key Resources at Your Fingertips: Utilize these key resources to strengthen your security posture and integrate them into your training schedule:

Resource	Description
DCSA Assessment and Authorization Guide (DAAG)	An essential guide available for download in eMASS . Digital copies are also available by contacting the DCSA NISP Cybersecurity Office (NCSO).
CDSE ISSM Toolkit & eLearning	The CDSE offers an invaluable toolkit and dedicated courses that make a tangible difference in your team's security readiness.

Questions or Feedback: If you have questions related to this article, please email the NISP Operations Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.



EXTERNAL SYSTEMS AND SECURE MOBILE PLATFORMS

Federal Information Systems, designated as “External Systems,” and government-provided secure mobile platform devices are owned and authorized by the issuing U.S. Federal Agency and do not fall under the security oversight of DCSA. As technology evolves, government components, such as the Air Force Civil Reserve Air Fleet (CRAF) Program, are modernizing how they provide secure network access to their commercial partners. This update clarifies current terminology, modern deployment methods, and oversight boundaries to ensure Industry has the most up-to-date guidance.

LEGACY HARDWARE EVOLVES TO MODERN MOBILE PLATFORMS

Technology	Description
The Old Way: "Flyaway Kits"	An antiquated term from the early days of remote deployments. It referred to bulky, physical hardware setups—routers, switches, and encryption gear packed into transit cases—designed to stand up a physical network remotely. Because these setups presented significant risks for unauthorized "backside" access to the SIPRNet, DCSA policy strictly prohibited them at cleared contractor facilities.
The New Way: CSfCs	Today, government components deploy secure, NSA-approved mobile platforms, such as classified tablets, smartphones, and laptops using Commercial Solutions for Classified (CSfC) technology. This allows commercial partners secure access without the massive hardware footprint or the legacy network vulnerabilities of the past. DCSA policy does not prohibit them at cleared contractor facilities.

CURRENT PROCEDURES & OVERSIGHT

Even with these modernized technologies, the core oversight rule remains the same: DCSA does not have cognizant security office authorities over government-provided mobile platform devices.

Area of Focus	Guidance & Responsibility
Government Responsibility	The government agency issuing/sponsoring the device (e.g., the Air Force) assumes all security responsibility and oversight for the device and its network connection, not DCSA.
The User Agreement	Contractors who are issued these devices must sign a User Agreement with the government customer. This agreement explicitly dictates how the device must be used, safeguarded, and reported on.
Device-Specific Issues	Because these devices are not under DCSA cognizance, contractors must direct all questions, exceptions, or security issues regarding the use of the mobile platform device directly to their government customer.
Industry Coordination	If cleared facilities have broader questions, concerns, or need to clarify oversight boundaries, they should coordinate with their DCSA Information Systems Security Professional (ISSP) for NISP Cybersecurity Office (NCSO) support.



NI2 UPGRADES, NEW TOOLS, STRONGER PARTNERSHIPS

Spring brings massive momentum to the National Industrial Security System Increment II (NI2)! We are launching major upgrades to enhance your experience and give you the tools you've requested to succeed.

Leveling Up IT Support: ESD is Coming Soon

Say goodbye to the old email inbox! NI2 is officially moving to a modern, automated ticketing system powered by the Enterprise Service Delivery (ESD) platform.

NI2 users will be able to easily submit and track requests. The ESD platform will streamline how we evaluate, route, and prioritize requests for new features and enhancements. The result? Faster routing, better transparency, and the top-tier customer service you expect. Training guides are coming soon.

Amplifying Industry Voices: The NISPPAC Sub-Working Group

Building a world-class system requires world-class feedback. To ensure NI2 truly serves our entire ecosystem, we are forming a dedicated sub-working group with individuals from under the National Industrial Security Program Policy Advisory Committee (NISPPAC).

This group will capture crucial operational feedback from our Industry partners and feed it straight back to our product teams. This direct pipeline will shape NI2's future development, ensuring we build a product that is useful, intuitive, and efficient for all stakeholders. Currently, NI2 is only deployed for the DD 254 Workflow (formerly NCCS). The platform will also house NISS and the 847 process, but both are future deployments to be developed.

The NI2 Training Environment is LIVE!

We heard your requests, and the brand-new NI2 Training Environment is officially operational.

Successfully authenticating with both E-ICAM and D-MFA, this environment is an exact replica of our live system. It provides a secure, risk-free "sandbox" where users can safely test new features, establish functional baselines, and conduct hands-on troubleshooting—without ever touching live mission data. We are actively working with the community to map out a phased onboarding approach.

We Want to Hear From You

For ongoing support, questions, or tracking system issues, please reach out to us at our official team mailbox: dcsa.meade.peo.mbx.ni2@mail.mil.

Stay tuned for more updates as we continue to modernize and expand NI2.



NEW DISS “UNENROLLED” CV STATUS/PROCESS

On April 2, Defense Information System for Security (DISS) Release 14.5 introduced the new "unenrolled" Continuous Vetting (CV) status/process. Under this process, when an individual loses their affiliation with a Security Management Office (SMO) in DISS, a 45-day grace period will begin, and if a new SMO does not take over the relationship within this timeframe, the individual's CV status will automatically change to "unenrolled."

How is the CV status/process changed?

To provide a more streamlined experience, DCSA simplified the CV enrollment process in DISS to three the statuses:

- Enrolled: The individual is actively enrolled in the DCSA CV Program.
- Unenrolled: The individual was previously enrolled in the DCSA CV Program but is no longer enrolled.
- Not Enrolled: The individual has never been enrolled in the DCSA CV Program.

Key Change: The "continued enrollment" status has been removed. To assist with this transition, tooltips will be added to DISS to provide clear definitions for the "unenrolled" and "not enrolled" statuses. The CV Enrollment Date and the Personnel Vetting Questionnaire (PVQ) Date displayed in the CV section of JVS will update when a new PVQ is processed by DCSA.

How It Works: The 45-Day Grace Period

When an individual loses their SMO relationship in DISS, a 45-day grace period will start during which their CV enrollment continues. After 45 days without an active SMO affiliation, the individual's CV status in DISS/NBIS will change to "unenrolled." This change aims to minimize gaps in CV for individuals undergoing a transfer of trust. The individual's eligibility will not be affected unless there is mitigatable unresolved derogatory information.

How Do I Re-Enroll Individuals in CV?

An individual will be automatically re-enrolled in CV once they establish an active SMO relationship, provided they remain eligible. Individuals will not need to complete new security forms (e.g., SF 86 or PVQ) to be re-enrolled in CV.

Action Required

To ensure a seamless transition and maintain accurate CV enrollment and billing for all personnel, it is critical that users promptly update or remove SMO ownership information in DISS.

Note: Non-DoW users do not need to take action at this time. However, the 45-day grace period may apply in the future as CV enrollment/unenrollment is automated.



DCSA UPDATES NISP CONTRACTOR CONTINUOUS VETTING PROCESS

The Defense Counterintelligence and Security Agency (DCSA) has announced important changes to its personnel vetting process, superseding previous guidance from August 2022 and reflecting updates from DISS Release 14.5.

Under the new policy, periodic reinvestigations for National Industrial Security Program (NISP) contractor national security personnel will no longer be required. Instead, all individuals must now submit an updated Personnel Vetting Questionnaire (PVQ or SF-86 eApp and releases) every five years, regardless of their eligibility level. The timing for this five-year update is now based on the "PVQ Date" recorded in DISS, which is equivalent to the SF-86 date.

To help organizations identify which personnel are due for this update, the DISS Subject Report should be used, with the PVQ Date serving as the key reference point. Once identified, organizations should submit the necessary information to the Personnel Security Management Office for Industry (PSMO-I) to ensure compliance with the new requirements.

Read the full guidance [here](#).

NAESOC

SERVICENOW IMPLEMENTATION ANNOUNCEMENT

The National Access Elsewhere Security Oversight Center (NAESOC) is pleased to announce the implementation of ServiceNow as part of our continued efforts to enhance communication, service management, and operational efficiency. NAESOC FSOs can be on the lookout for and expect an upcoming email containing important information, access details, and next steps regarding the new platform.

WHAT TO EXPECT FROM THE SERVICENOW EXPERIENCE:

This upgraded platform is designed to provide greater transparency and put you in the driver's seat. The new system will allow you to:

- **Effortlessly Request Services** - Seamlessly locate and submit requests for the specific services you require.
- **Monitor Real-Time Progress** - Keep a close eye on the current status of all your active and historical inquiries.
- **Oversee Your Data** - Take charge of your user profile, access comprehensive service records, and explore additional self-service features.

Please be sure to visit [our website](#) for all things "NAESOC."



CONNECT WITH THE NAESOC

- **Online Resources** - Visit the [NAESOC website](#) for direct access to job aids, user guides, and answers to common questions.
- **Stay Informed** - To guarantee you receive critical notifications and updates, please add dcsa.naesoc.generalmailbox@mail.mil to your email's safe sender list.
- **Profile Maintenance** - Verify that your NISS profile reflects your current points of contact to ensure seamless communication.
- **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

SECURITY TRAINING

NEW ELEARING COURSE

CDSE recently updated the [Visits and Meetings in the NISP IS105.16](#) eLearning course. This 1-hour course covers the requirements and procedures for incoming and outgoing classified visits and classified meetings for facilities participating in the NISP. The course also discusses the NISP requirements and best practices for maintaining security controls.

INDUSTRIAL SECURITY OFFERINGS

Visit CDSE's [Industrial Security Training Page](#) to browse all available curricula, courses, job aids, games, posters, videos and toolkits pertaining to the IS discipline.

CDSE PULSE

The May 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!



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

August 17 - 21, 2026 (Linthicum, MD)

INDUSTRIAL SECURITY:

[Getting Started Seminar for New Facility Security Officers \(FSOs\) VILT](#) IS121.10

July 21 - 24, 2026 (Virtual)

INFORMATION SECURITY:

[Activity Security Manager VILT](#) IF203.10

July 26 - August 23, 2026 (Virtual)

INSIDER THREAT:

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

June 8 - 12, 2026 (Virtual)

July 13- 17, 2026 (Virtual)

August 17- 21, 2026 (Virtual)

September 21 - 25, 2026 (Virtual)

PHYSICAL SECURITY:

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

June 8 - 12, 2026 (Linthicum, MD)

September 14 - 18, 2026 (Linthicum, MD)

SPECIAL ACCESS PROGRAMS:

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

August 4 - 7, 2026 (San Diego, CA)

August 25 - 28, 2026 (Cincinnati, OH)

September 8 - 11, 2026 (El Segundo, CA)

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

June 1- 9, 2026 (Virtual)

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

August 10- 11, 2026 (San Diego, CA)

August 31- September 1, 2026 (Cincinnati, OH)

[SAP Mid-Level Security Management](#) SA201.01

July 13- 17, 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: [@DCSAGov](#)

CDSE LinkedIn: [@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 Personnel Security Clearance (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 Industrial Security Representative. 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 Senior Management Official 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