DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

July 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

USE OF CAC FOR DCSA PERSONNEL IDENTIFICATION

Effective August 10, 2026, DCSA field personnel will transition from badges and credentials to the Department of War (DoW) Common Access Card (CAC) for official identification. This modernization applies to ISRs, Information System Security Professionals (ISSPs), and Counterintelligence Special Agents (CISAs). The shift streamlines facility visits and aligns with broader federal security standards without altering DCSA's authority to conduct NISP oversight.

DCSA personnel will present their DoW CAC for Industry visits. For visits involving access to classified material, clearance eligibility will now be verified via a one-time look-up in the Defense Information System for Security (DISS), or through advance Visit Access Requests (VARs) submitted via DISS for longer-term access requirements.

IMPLEMENTATION GUIDANCE

To ensure security compliance during DCSA facility visits, FSOs should refer to the following protocols regarding facility access and verification for DCSA personnel:

Identity Verification

- Visual CAC Inspection - Upon arrival, the DCSA representative will present their CAC. FSOs should visually inspect the card to verify that the photo and name match the individual.
- Use of CAC - DoW prohibits the use of CACs for badge exchange (e.g., exchanging it for a local visitor badge), nor are they allowed to be scanned or photocopied.

Clearance Verification & DISS Use

- Clearance Verification - Clearance verification is only required when personnel access classified material or hold classified discussions. Onsite activities that do not involve classified information or discussions do not require clearance verification. DCSA personnel will coordinate in advance whether a one-time look up or a visit access request will be utilized for scheduled NISP-related oversight visits to cleared contractor facilities.
- One-Time Look-Up - For routine visits, the FSO can verify the representative's security clearance by performing a one-time look-up in DISS. DCSA personnel will provide the necessary information (such as SSN) at the location where DISS verification is being conducted.
- Visit Access Requests (VARs) - For long-term or frequent visits (e.g., a week-long team security review), DCSA will submit a VAR in advance via DISS.
- Servicing Relationships - Contractors should only use the long-term DISS visit request for DCSA personnel and should not establish a "servicing" relationship with DCSA personnel in DISS.
- System of Record - DISS is the system of record for verifying DCSA personnel clearance and records. Any removal of DISS data must comply with the DISS Account Management Guide.

- Access Agreements - Generally, DCSA personnel are not required to sign additional local access agreements to perform security oversight. Facility access is already established under the executed DD Form 441 Security Agreement. (Note: Additional special briefing requirements may still apply for access to SAP and ACCM).

Points of Contact

- For questions regarding DCSA Industrial Security personnel or visits, please contact the field office chief of your supporting DCSA field office.

- For questions regarding DCSA Counterintelligence personnel or visits, please contact the CI Regional Mission Director supporting your facility.

U.S. CITIZENSHIP DOCUMENTS UPDATE

Previous Guidance: Statements published in the January 2026 VOI indicating that verification must be conducted strictly "in-person" and outlining "prohibited methods" are incorrect and should be disregarded.

The Office of the Under Secretary of War for Intelligence and Security has provided clarification on the interpretation of the requirements established in DoDM 5200.02 ("Personnel Security") and 32 CFR Part 117 (NISPOM) on the verification of citizenship documents. FSOs or designated representatives will verify evidence of employee U.S. citizenship documents through physical inspection, digital review, or other contractor-managed methods. Please note that this update does not alter the list of authorized U.S. citizenship documents specified in the NISPOM.

SECURITY REVIEW RATING RESULTS FISCAL YEAR 2026

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

Overall Fiscal Year Goal:	3,900	
Rated Security Reviews Completed:	3,411	(87.5%)
Rated Security Reviews Remaining:	489	(12.5%)
Superior Ratings Issued:	384	(11.3%)
Commendable Ratings Issued:	1,241	(36.4%)
Satisfactory Ratings Issued:	1,771	(51.9%)
Marginal Ratings Issued:	5	(00.1%)
Unsatisfactory Ratings Issued:	10	(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 Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

INDUSTRIAL SECURITY LETTER 2026-01

INSIDER THREAT PROGRAM: MINIMUM STANDARDS

DCSA has officially released Industrial Security Letter (ISL) 2026-01 which provides a consolidated overview of minimum standards, resources, and training to assist contractors in establishing and tailoring their insider threat programs. The ISL incorporates guidance previously provided in the Insider Threat Training for Cleared Industry Slick Sheet, Insider Threat Training Information Paper, and VOI Newsletter.

A releasable copy of the ISL is available on the DCSA website here.

OFFICE OF COUNTERINTELLIGENCE SVTC & WEBINAR

EXPLOITATION OF EDGE DEVICES CLASSIFIED INDUSTRY SVTC

As the defense industrial base (DIB) and academia increasingly rely on distributed networks, edge devices have become a critical frontier in our national security posture. Yet, our adversaries—ranging from state-sponsored actors to sophisticated ransomware syndicates—are aggressively targeting these very devices, exploiting vulnerabilities and supply chain weaknesses to compromise critical networks and operations.

DCSA invites cleared members of the DIB industrial base and academia to participate in a classified Secure Video Teleconference (SVTC) for this month's presentation titled "Exploitation of Edge Devices." This presentation will dive into the overarching trends targeting edge devices, including pressing supply chain concerns. The brief will cover trend analysis of frequently targeted devices, an overview of commonly exploited vulnerabilities, and specific case studies involving both state-sponsored and ransomware actors. Briefers can discuss actionable defensive measures and ways you can help, whether you are in cybersecurity, IT, procurement, facility security, or program management.

The SVTC is an in-person event at most DCSA field offices on August 13, 2026, from 1:00 to 2:30 p.m. Register at SVTC Registration no later than August 7, 2026.

SUPERCHARGING THE DIB: DOW BATTERY SUPPLY CHAINS WEBINAR

The 2026 National Defense Strategy called for supercharging the U.S. DIB to ensure the readiness, lethality, range, and survivability of our military. Batteries are essential to maintaining U.S. advantage in military operations across the land, sea, air, and space domains. Yet our adversaries seek to sabotage DoW battery supply chains and DIB competitiveness, targeting nodes across the value chain from upstream materials to military end items. DCSA invites cleared members of the DIB to join us for an unclassified webinar with the Office of the Secretary of War's Industrial Base Policy (IBP) office and other guests to discuss a comprehensive study on the essential role batteries have in powering our advanced military, the threat of PRC non-competitive policies including export controls, and new DoW authorities to solve supply chain threats.

The September CI webinar will be held virtually via CDSE Adobe Connect on September 24, 2026, from 1:00 to 2:30 p.m. The registration link will be provided once activated.

COUNTERINTELLIGENCE FOCUS: THE REMOTE THREAT

COUNTERING STATE-SPONSORED FRAUDULENT IT OPERATIVES

North Korean state-sponsored threat actors are expanding their attack vectors beyond traditional network breaches to exploit a new vulnerability: fraudulent remote employment.

Increasingly, North Korea is deploying a highly skilled army of IT workers to infiltrate Western companies, not through complex hacking, but by getting hired. These operatives are circumventing heavy international sanctions to generate millions in revenue for the regime's illicit ballistic missile and nuclear programs, all while working from the payroll of unsuspecting businesses.

First observed in 2017, the operation has rapidly escalated from simple employment fraud into a highly organized cyber offensive operation. This maturation reached a critical turning point by 2024, when these illicit IT workers began collaborating directly with state-sponsored cyber actors, actively abusing their legitimate corporate credentials to steal data, deploy ransomware, and establish persistent backdoors. Reporting from 2025 to 2026 exposed an evolution, revealing that these threat networks are no longer loose collections of rogue actors, but highly organized entities operating under corporate-style frameworks that mirror the exact structures, quotas, and high-pressure environments of typical U.S. technology sales departments.

These illicit operations foster a highly competitive environment. Individual teams are driven by strict performance metrics, subjected to a system of collective praise, material rewards, and swift disciplinary actions to maximize output. At the execution level, specialized IT operatives leverage unique technical skillsets and past professional connections to generate revenue. These workers report directly to a team manager, who bears ultimate responsibility for the cell's productivity and reports metrics directly to regime leadership.

The Infiltration Vector - The deployment of fraudulent IT workers relies on exploiting standard remote-hiring logistics and leveraging domestic proxy infrastructure such as:

- Fraudulent Persona Generation: Applicants synthesize stolen U.S. identities, AI-generated headshots, and fabricated credentials. They target freelance platforms and corporate job portals using proxy IP addresses.

- Interview Manipulation: Candidates utilize real-time AI tools to alter facial features, voices, and backgrounds during video interviews to align with their synthetic personas.

- Domestic Proxy Infrastructure: Company-provided hardware is shipped to unwitting U.S. facilitators or consolidated "laptop farms" managed by witting U.S. facilitators. Operatives access these machines via unauthorized Remote Desktop Protocol (RDP) or KVM-over-IP (Keyboard, Video, Mouse) devices to spoof domestic network origination.

- Post-Hire Exploitation: Once authenticated, fraudulent operatives leverage legitimate access to deploy malware, map network topography, and establish persistent backdoors for secondary exploitation by state-sponsored advanced persistent threats (APTs).

North Korea has heavily invested in this strategy. In March 2025, the North Korean Government established a formal training program that identifies promising students as early as elementary school, funneling them into a rigorous pipeline of specialized education. A new organization, "Research Center 227," was also created to develop advanced AI-powered cyber tools for data theft and financial crime.

How to Protect Your Company - U.S. government agencies and cybersecurity firms urge organizations to adopt a multi-layered defense. They recommend some of the following mitigation tactics:

- Verify, Then Trust: Organizations must implement stringent identity verification during hiring. This includes cross-checking résumés for duplicate contact information, mandating on-camera interviews with unobscured backgrounds, and conducting deep background checks using biometric verification services.

- Prepare Your HR for AI Deception: During the interview process, HR teams must actively attempt to identify the use of AI to alter appearances. Interviewers should require physical interaction during video interviews to break AI filters, such as having candidates turn their heads rapidly, pass a hand in front of their face, or hold up a unique, physical object.

- Enforce Strict Technical and Logistical Policy: Companies must enforce rigid shipping hardware protocols, such as strictly prohibiting employees from changing the shipping address of corporate hardware after an offer letter is signed. Furthermore, organizations should prohibit the use of virtual private networks (VPNs) on personal devices connecting to the corporate network.

- Monitor Network Activity and Practice Least Privilege: IT security teams must actively monitor for unusual login patterns, unauthorized software installations (especially remote-access tools), and suspicious data exfiltration to cloud drives or private repositories. Additionally, ensuring employees only have access to the data and systems necessary for their jobs is critical. Companies should disable local administrator accounts and limit software installation privileges.

- Train Your Team: Finally, organizations must educate all employees on the latest social engineering tactics and create a robust whistleblowing system to encourage the reporting of suspected fraud.

This evolving threat highlights the critical need for companies to look beyond traditional perimeter security and focus on the risks posed by insider threats through credential/identity fraud and state sponsored infiltration.

NAESOC

Welcome to NAESOC: Seamless Oversight Transition

We would like to extend a warm welcome to all the facilities joining the National Access Elsewhere Security Oversight Center (NAESOC)! Our goal is to provide centralized, consistent, and efficient security oversight for facilities.

As you integrate into our operations, we are committed to ensuring a seamless transition and providing the proactive support your facility needs to maintain a strong security posture.

Transition Timeline

The transition of newly assigned facilities into the National Industrial Security System (NISS) under the NAESOC will occur on a rolling basis over the next three months. We appreciate your patience and cooperation as we work through this migration.

Look for:

- A "Welcome to the NAESOC" email from us to you with key information and resources that will be immediately available.
- Notification from NISS that your status has changed *("NISS Alert – Oversight Team Reassignment"*). You can then check your NISS profile to see that you are now assigned to the NAESOC.

Action Required: Verify Your Oversight Team

To ensure you receive timely support, guidance, and official communications, it is highly recommended that you verify your current oversight assignment in NISS.

1. **Log in to NISS** - Navigate to your facility profile.
2. **Oversight Team** - Locate your assigned oversight team.
3. **NAESOC Assignment** - When you validate that your oversight team is now listed as **NAESOC**, please begin coordinating directly with the NAESOC Helpdesk for all future inquiries, administrative updates, and safeguarding support.

Important NAESOC ServiceNow Access Reminder

We have been receiving feedback that many members across industry are experiencing account lockouts. To avoid being locked out of your account, please ensure you log in at least once every 30 days. Accounts that remain inactive beyond 30 days will be automatically locked.

For assistance regaining access, please contact the ServiceNow Helpdesk at 878-274-1003.

Contacting the NAESOC

- **Online Resources** - Visit the NAESOC website for direct access to job aids, user guides, and answers to common questions.
- **E-mail Inquiries** - dcsa.naesoc.generalmailbox@mail.mil
- **Live Phone Support** - (878) 274-1800
  - Monday – Thursday: 9:00 a.m. to 3:00 p.m. ET
  - Friday: 8:00 a.m. to 2:00 p.m. ET

SHAPING THE FUTURE OF NI2 TOGETHER

Collaborating on Next-Generation Capabilities

We are excited to announce the creation of the new National Industrial Security Program Policy Advisory Committee (NISPPAC) Systems Sub-Working Group, established under our existing Operational Requirements Working Group!

Our mission is to increase transparency, actively involve industry partners in the development process, and ensure your voices are directly heard as we build NISS Increment II (NI2). We are actively refining our collaborative processes so that industry users can participate directly in shaping these critical systems. Your feedback is vital to ensure NI2 meets the operational realities of our joint mission, and we look forward to building this capability together.

Keep an eye out for upcoming feedback sessions, surveys, and collaborative opportunities!

NISS Reminders: Essential Profile Updates and Upcoming Data Collection

The National Industrial Security System (NISS) remains the primary system of record and the central hub for the National Industrial Security Program. As we progress through the year, DCSA wants to remind all FSOs of their critical role in maintaining accurate facility data to ensure seamless oversight, security reviews, and communication.

Ensure Your NISS Facility Profile is Up-to-Date

Maintaining an accurate facility profile in NISS is not just a compliance measure; it is essential for effective steady-state oversight. FSOs are required to regularly review and update their NISS profiles to reflect any organizational changes.

Recommended Action: Please log in to NISS and review the following items this month:

- Key Management Personnel (KMP) - Ensure all KMP listings are current, with accurate contact information and clearance statuses.
- Facility Contact Information - Verify that email addresses and phone numbers for the FSO and Insider Threat Program Senior Official (ITPSO) are completely up-to-date so your facility does not miss critical DCSA correspondence.
- Business Structure - Promptly report any changed conditions, including ownership transitions, joint ventures, or adjustments to your facility's physical address.

System Latency and Help Desk Support

DCSA continues to deploy updates to NISS to improve system performance and user experience. If you encounter system latency or require technical assistance with your facility profile, please submit a ticket through the Enterprise Service Delivery portal or contact the DCSA Help Desk.

SECURITY TRAINING

REGISTRATION OPEN: 2026 VIRTUAL DCSA SECURITY CONFERENCE

September 14 – 18, 2026

Join us virtually for cutting-edge insights, collaborative problem-solving, and expert-led discussions. This year's conference is designed to maximize value by dedicating specific days to the unique needs of security professionals.

To ensure you experience the most relevant and impactful programming, the week is organized into focused tracks. Review the schedule below and register for the days that best align with your mission and professional focus:

DATES	FOCUSED PROGRAMMING	IDEAL AUDIENCE
Monday, 9/14 Tuesday, 9/15	**INDUSTRIAL SECURITY TRACK** These sessions focus on specific topics, challenges, and compliance standards impacting Industrial Security.	Industrial Security professionals
Wednesday, 9/16 Thursday, 9/17 Friday, 9/18	**DoW AND FEDERAL GOVERNMENT TRACK** These sessions deliver strategic content tailored to military and government operations, interagency collaboration, and national defense priorities.	DoW and federal government security professionals **.gov, .mil, or government-affiliated .edu e-mail required*

Register today!

INDUSTRIAL SECURITY TRAINING AND RESOURCES

Clearances in Industrial Security: Putting it All Together (IS125.16)

This updated Clearances in Industrial Security: Putting it All Together course provides a high-level overview of personnel security clearances, facility clearances, and foreign ownership, control, or influence (FOCI). The course is tailored for security specialists with industrial security responsibilities and DCSA industrial security personnel.

Refresh your workspace with newly released security posters:

- Protecting America's Warfighters
- Bad Security Practice is the Pits
- Good Security Practices are Peachy Keen

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.

SETA PULSE

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

TRAINING & UPDATES FOR INDUSTRY

Watch the recorded CDSE Training Product Updates for Industry webinar to learn about new and updated products beneficial to cleared industry.

NEW INSIDER THREAT PRODUCTS

- Insider Threat Security Short - Learn about these insider threat topics in just 10 minutes or less: Human Resources, Cybersecurity, and Law Enforcement.
- Case Studies - Learn about behavioral indicators and impacts of insider threats with U.S. defense contractor Craig Klund who carried out an extensive fraud scheme and dual citizen Xiaoqing Zheng who stole trade secrets.

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)

PHYSICAL SECURITY:

Physical Security and Asset Protection PY201.01

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)

Orientation to SAP Security Compliance Inspections SA210.01

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

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

WEBINARS

AI and Cybersecurity: Adversarial Techniques and Managing Risk

August 5, 2026 | 10- 11 a.m. ET

SOCIAL MEDIA

Connect with us on social media!

DCSA X: @DCSAgov

DCSA Facebook: @DCSAgov

DCSA LinkedIn: @DCSAgov

CDSE X: @TheCDSE

CDSE Facebook: @TheCDSE

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 osd.pentagon.ogc.mbx.doha-status@mail.mil