



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY

DCSA MONTHLY
NEWSLETTER

August 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

INDUSTRY RAP BACK EXPANSION PROGRESSION	2
OFFICE OF COUNTERINTELLIGENCE SVTC & WEBINAR	2
SUPPLY CHAIN SECURITY AND SUPPLIER RISK MANAGEMENT SVTC	2
SUPERCHARGING THE DIB: DOW BATTERY SUPPLY CHAINS WEBINAR	3
SECURITY REVIEW RATING RESULTS FISCAL YEAR 2026	3
BLACK LABEL GSA CONTAINER PHASE-OUT	4
BLACK LABEL PHASE-OUT PLAN	4
BLACK LABEL CONTAINER USE AFTER DECOMMISSIONING.....	5
BLACK LABEL CONTAINER DISPOSAL	5
INDUSTRIAL SECURITY LETTER 2026-01	6
INSIDER THREAT PROGRAM: MINIMUM STANDARDS	6
NAESOC.....	6
SECURITY TRAINING.....	7
COUNTDOWN TO COLLABORATION: 2026 DCSA SECURITY CONFERENCE.....	7
TRAINING AND RESOURCES.....	8
FY26 INSTRUCTOR-LED COURSES	8
SETA PULSE.....	8
SOCIAL MEDIA	9
REMINDERS	9
CONTACTS.....	10



INDUSTRY RAP BACK EXPANSION PROGRESSION

In February 2026, DCSA [announced](#) the expansion of Rap Back enrollment to the broader industry population using a phased implementation plan.

Rap Back, an FBI-provided service, utilizes the Integrated Automated Fingerprint Identification System (IAFIS) to enable real-time notifications of changes to an individual's criminal record. As the cornerstone of the Trusted Workforce 2.0 (TW 2.0) Continuous Vetting (CV) framework, this capability ensures cleared personnel are continuously monitored to maintain their eligibility for access to classified information.

The phased rollout began with industry personnel who already had fingerprints on file (Phase I and II) and has progressed to industry personnel without fingerprints on file (Phase III). Industry partners with personnel falling into this category have received lists of their Phase III personnel as well as specific instructions via email on how to proceed.

- Not all Industry Security Management Offices (SMO) received a list of Phase III personnel. Only SMOs who have ownership of individuals who do not have fingerprints on file have received a list.
- Enrollment of individuals in another Agency's Rap Back does not automatically exclude those individuals from a need to enroll in DCSA Rap Back. If an individual appears on a Phase III list, their fingerprints are required by DCSA for enrollment.

For questions associated with the Rap Back Fingerprint Voucher process, vendor locations, or scheduling issues, please contact BioMetrics4All directly at dcsa@applicantservices.com.

For any questions regarding lists of individuals requiring fingerprints for DCSA Rap Back enrollment, how this transition impacts your facility or your personnel, and general DCSA Rap Back enrollment subscriptions, please reach out directly to the DCSA Industry Account Manager email box at dcsa.boyers.dcsa.mbx.industry-agency-liaison@mail.mil.

OFFICE OF COUNTERINTELLIGENCE SVTC & WEBINAR

SUPPLY CHAIN SECURITY AND SUPPLIER RISK MANAGEMENT SVTC

DCSA invites cleared members of the defense industrial base (DIB) to participate in a classified Secure Video Teleconference (SVTC) presentation focused on "Supply Chain Security and Supplier Risk Management." Our guest presenter is from the Defense Intelligence Agency's Supply Chain Risk Management – Threat Analysis Center (SCRM-TAC).

In today's global economy, few organizations operate without some degree of foreign involvement in their supply chains. For the DIB, that reality creates both opportunity and risk. Adversarial nations and other malign actors understand that supply chains can provide access, influence, and insight into sensitive technologies, programs, and business relationships. As a result, supplier vetting and supply chain security are no longer simply procurement concerns, they are national security issues.

This presentation examines the importance of understanding who is in your supply chain, how foreign relationships can create hidden vulnerabilities, and why early awareness is critical to protecting sensitive



programs and technologies. The briefing also highlights key considerations for evaluating supplier risk, recognizing potential warning signs, and strengthening internal coordination among security, procurement, legal, compliance, and program personnel. Whether your role is in counterintelligence, industrial security, acquisitions, supply chain management, or program oversight, this brief provides valuable context for protecting your organization from supply chain-related threats.

The SVTC is an in-person event at most DCSA field offices on September 10, 2026, from 1:00 to 2:30 p.m. ET. Register at [SVTC Registration](#) no later than September 4, 2026.

SUPERCARGING 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 Department of War (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. ET. Register at [Webinar Registration](#).

SECURITY REVIEW RATING RESULTS FISCAL YEAR 2026

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

Overall Fiscal Year Goal:	3,900
Rated Security Reviews Completed:	3,826 (98.1%)
Rated Security Reviews Remaining:	74 (1.9%)
Superior Ratings Issued:	455 (11.9%)
Commendable Ratings Issued:	1,412 (36.9%)
Satisfactory Ratings Issued:	1,944 (50.8%)
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.



BLACK LABEL GSA CONTAINER PHASE-OUT

The phase-out of black label General Services Administration (GSA) containers began October 1, 2024. GSA determined that agencies must phase out all GSA-approved security containers and vault doors manufactured from 1954 through 1989 (“black labels”) to store classified information and materials. GSA’s detailed phase-out plan can be viewed in [ISOO Notice 2021-01](#) or the [DoW Lock Program](#).

Disposal of GSA-approved security containers is left to the discretion of the agency, command, company security officer, or equivalent authority. The phase-out removes the authorization to use these containers to protect and store classified material but does not require disposal if the containers are used for an unclassified purpose. All containers must be decommissioned but may still be used to store classified within an approved Open Storage Area because the required security measures are already in place. In this case, the container is essentially used as a lockable filing cabinet.

BLACK LABEL PHASE-OUT PLAN

GSA CLASS	FEDERAL SPECIFICATION	REVISION	YEARS PRODUCED	YEARS OF SERVICE	END OF SERVICE
2	AA-F-357 - Filing Cabinets	A - F	1954 - 1970	50 - 70	1 October 2024
3	AA-F-358 - Filing Cabinets	A - F	1956 - 1968	52 - 69	1 October 2025
4	AA-F-358 - Filing Cabinets	A - F	1956 - 1968	52 - 69	1 October 2025
1	AA-F-357 - Filing Cabinets	A - F	1968 - 1982	46 - 60	1 October 2028
5	AA-F-358 - Filing Cabinets	A - F	1968 - 1989	31 - 60	1 October 2028
6	AA-F-358 - Filing Cabinets	A - F	1968 - 1989	52 - 60	1 October 2028
5	AA-F-363 - Map & Plan	A - B	1963 - 1989	57 - 65	1 October 2028
5	AA-D-600 - Vault Doors	A - B	1963 - 1989	57 - 65	1 October 2035*
6	AA-D-600 - Vault Doors	A - C	1963 - 1989	57 - 65	1 October 2035*

*[ISOO Notice 2022-03](#) states the phase-out of all black label vault doors has been extended until 1 October 2035.



Black label containers on the list for with an “End of Service” date of 1 October 2028 or vault doors with a date of 1 October 2035, remain approved for classified storage until their designated date. A manufacturers label, usually located inside the drawer with the lock, will provide the manufacturer, model number, serial number, date of manufacture, and federal specification. Using the list, validate that your black label containers are still authorized to store classified information.

BLACK LABEL CONTAINER USE AFTER DECOMMISSIONING

All containers identified with End of Service in October 2024 and 2025 are not approved for classified storage. The owner must do the following to continue use of a decommissioned black label container:

1. Thoroughly search to ensure all classified materials have been removed.
2. Remove all exterior GSA-approval black labels and interior certification and identification labels.
3. Place this notice on front of container, “No Longer GSA Approved (Standard File Cabinet Use Only).” (Order a magnetic sticker using the [Phase Out Sticker Request](#) on the [DoD Lock Program website](#)).
4. Visit the website in the future for disposition guidance when the container is no longer needed.

BLACK LABEL CONTAINER DISPOSAL

The latest disposal guidance for black label containers from the General Services Administration, Interagency Advisory Committee on Security Equipment (GSA/IACSE) and DoD Lock Program is as follows:

1. Thoroughly search to ensure all classified materials have been removed.
2. Remove all exterior GSA-approval black labels and interior certification and identification labels.
3. Remove any “limited use” electromechanical combination locks. Destroy or return them to the U.S. Government in accordance with DoD Lock Program [Security Equipment Disposal](#) guidance.
4. Directly render the container to a steel recycling facility for destruction and steel reclamation.
5. Do not auction off or resell any intact decommissioned black label security equipment as it could be inappropriately resold, creating a security risk. This black label equipment end-of-service process must be followed to ensure supply chain integrity and protect classified information.

For specific questions or assistance, please contact the DoD Lock Program, Technical Support Hotline:

Toll-free: (800) 290-7607

DSN: 551-1212

Commercial: (805) 982-1212

Or Use the [Technical Support Request Form](#)

To purchase an approved replacement container, go to [Ordering Security Containers | GSA](#).



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](#).

NAESOC

Welcome to NAESOC: Seamless Oversight Transition

The National Access Elsewhere Security Oversight Center (NAESOC) is pleased to welcome our newest facilities! Our mission remains focused on delivering centralized, consistent, and streamlined security oversight to ensure facilities maintain a strong security posture from day one. We appreciate your continued patience and partnership as we are committed to ensuring a seamless transition.

Transition Expectations

The migration of newly assigned facilities into the National Industrial Security System (NISS) under NAESOC oversight is ongoing. Important Information about the current transition phase:

- Timeline: Migrations will continue to occur on a rolling basis over the coming months.
- Email Notification: Watch your inbox for a "Welcome to the NAESOC" introductory email detailing essential resources that are immediately available to you.
- System Alert: Look for an automated NISS notification titled "NISS Alert – Oversight Team Reassignment."

Action Recommended: Verify Your Oversight Team

To guarantee timely support, guidance, and uninterrupted official communications, it is highly recommended that you verify your oversight team in NISS using the following steps:

1. **Log in to NISS** - Navigate to your facility profile.
2. **Oversight Team** - Locate your assigned oversight team, to see if it shows "NAESOC."
3. **When you have validated that**, please begin coordinating directly with the NAESOC Helpdesk for all future inquiries, administrative updates, and safeguarding support.



Action Recommended: Check for Key Information and Updates You May Need

The NAESOC maintains key resources at your fingertips. For FAQs and critical information online resources, visit the [NAESOC website](#). There you will find direct access to job aids, user guides, and answers to common questions, all key to assist you with your non-possessor facility program. There are also links to Webex products hosted by CDSE, based on real-world learnings identified by non-possessor FSOs.

Important NAESOC Government Services Portal Access Reminder

We have been receiving feedback that many members across industry are experiencing account lockouts at the NAESOC [Government Services Portal](#). **To avoid being locked out of your account, please 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

- 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

SECURITY TRAINING

COUNTDOWN TO COLLABORATION: 2026 DCSA SECURITY CONFERENCE

September 14 – 18, 2026

We are just a few weeks away from kicking off the 2026 DCSA Security Conference. Join us virtually for actionable insights, collaborative problem-solving, and expert-led discussions.

To maximize value, the schedule is structured into tracks dedicated to the unique needs of security professionals. Review the specialized tracks below and register for the days that directly align with your operational mission and professional focus:

DATES	FOCUSED PROGRAMMING	IDEAL AUDIENCE
Monday, 9/14 Tuesday, 9/15	<u>INDUSTRIAL SECURITY TRACK</u> 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	<u>DoW AND FEDERAL GOVERNMENT TRACK</u> 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

[View the agenda and register today!](#)



TRAINING AND RESOURCES

Introduction to Industrial Security (IS011.16)

CDSE has updated the most popular industrial security course! The one-hour [Introduction to Industrial Security](#) eLearning course introduces National Industrial Security Program (NISP) requirements, roles, and contracting processes. Designed for facility security officers and industrial security specialists, this concise training clarifies critical contractor requirements in both government and private facilities. [Register here](#).

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

This one-hour eLearning course provides a high-level overview of Personnel Security Clearances, Facility Clearances, and Foreign Ownership, Control, or Influence (FOCI). [Register here](#).

CUI Training Frequency Reduced

In a move to restore mission focus, the Department of War changed the frequency of mandatory Controlled Unclassified Information (CUI) training from an annual to a biennial (every two years) requirement. CUI training, materials, and policy will be updated to adhere to this change.

Additional Resources

Watch the recorded [CDSE Training Product Updates for Industry webinar](#) to learn about new and updated products beneficial to cleared industry or 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.

FY26 INSTRUCTOR-LED COURSES

Find a complete list of CDSE offerings [here](#) with links to course descriptions and requirements.

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

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

SETA PULSE

The August 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!



SOCIAL MEDIA

Connect with us on social media!

DCSA X: [@DCSAGov](https://twitter.com/DCSAGov)

CDSE X: [@TheCDSE](https://twitter.com/TheCDSE)

DCSA Facebook: [@DCSAGov](https://www.facebook.com/DCSAGov)

CDSE Facebook: [@TheCDSE](https://www.facebook.com/TheCDSE)

DCSA LinkedIn: [@DCSAGov](https://www.linkedin.com/company/DCSAGov)

CDSE LinkedIn: [@CDSE](https://www.linkedin.com/company/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