DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

September 2025

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

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

DISS CLOUD MIGRATION

DCSA is taking a significant step in its digital transformation journey by migrating the Defense Information System for Security (DISS) to the Amazon Web Services (AWS) Cloud platform. This strategic transition, which took place between August 29 and September 1, 2025, is a cornerstone of DCSA's overarching "Cloud Smart" strategy. As an integral component of the broader NBIS program, this move underscores DCSA's commitment to modernizing its critical infrastructure, enhancing system resilience, and leveraging the advanced capabilities of cloud technology to better serve national security interests.

Over the lifecycle of DISS, this migration to AWS will deliver significant improvements in performance, scalability, and cybersecurity posture, directly benefiting the vast network of users that depend on the system for security clearance processes. By embracing cloud-native solutions, DCSA aims to optimize operational efficiencies, reduce latency, and ensure a more robust and responsive platform for managing sensitive information. Be on the lookout for further NBIS systems migrating to the AWS Cloud during Fiscal Year 2026.

For ongoing access to DISS functionalities and official information, users may visit the dedicated DISS portal.

DISS TRAINING THROUGH CET

Are you looking to gain a better understanding of the functionality of the Defense Information System for Security – Joint Verification System (DISS-JVS)? DCSA's Customer Engagements Team (CET) is pleased to provide a valuable opportunity for users to access DISS training. These sessions are specifically designed to help you navigate and utilize the system more effectively, and for your convenience, all training classes will be conducted virtually via Microsoft Teams.

This is an excellent chance to sharpen your DISS skills with expert guidance. Registering for these training sessions is straightforward. Simply visit the DCSA Investigative Systems Training website. Once there, please select the DISS tab to find the registration form. After completing the form with your details, kindly email it to DCSAAgencyTraining@mail.mil.

NISS TIME RESTRICTIONS LIFTED; WEBSITE REFRESHED

Latency issues stemming from the National Industrial Security System (NISS) v2.7.3 update have been resolved. Therefore, the previous access time restrictions are no longer necessary and have been lifted.

Thank you for your patience and understanding during this period as we worked to optimize the system for all users.

If you experience any performance issues while using the system, please continue to follow the standard trouble ticket process through NISS operations or call the Knowledge Center at 667-424-3903.

Don't forget to check out the refreshed NISS page on the DCSA website! We've updated the look and are continuously adding the latest system updates. Visit the NISS Page here.

SECURITY REVIEW RATING RESULTS

The following security review results are current as of September 24, 2025:

Overall Fiscal Year Goal:	4,000	
Rated Security Reviews Completed:	4,480	(112.0%)
Rated Security Reviews Remaining:	0	(00.0%)
Superior Ratings Issued:	676	(15.1%)
Commendable Ratings Issued:	1,587	(35.4%)
Satisfactory Ratings Issued:	2,178	(48.6%)
Marginal Ratings Issued:	19	(00.4%)
Unsatisfactory Ratings Issued:	20	(00.5%)

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.

NISP CYBERSECURITY OFFICE (NCSO)

RELEASE OF THE DAAG

DCSA's Industrial Security NISP Cybersecurity Office (NCSO) is releasing the new DCSA Assessment and Authorization Guide (DAAG) to replace the DCSA Assessment and Authorization Process Manual (DAAPM) on October 1, 2025. The DAAG is available for download in the NISP Enterprise Mission Assurance Support Service (eMASS) system. Industry partners and other stakeholders may also obtain a digital copy of the DAAG from NCSO by submitting a request to dcsa.quantico.hq.mbx.nao@mail.mil.

Industry partners that do not yet have an eMASS account please visit the DCSA NISP Cybersecurity Office (NCSO) page and scroll to the eMASS information section for information. The DCSA NCSO page may also be reached from the DCSA Home Page by selecting the NISP Cybersecurity Office (NCSO) link from the Industrial Security dropdown.

Cleared contractors processing classified information under the cognizance of DCSA shall follow the guidance contained within the DAAG to complete the Risk Management Framework (RMF) process to obtain system authorization. The DAAG includes process updates to align with applicable Committee on National Security Systems (CNSS) instructions, as well as updated templates and job aids, and a reformatted document numbering scheme for ease of use by industry stakeholders.

The contents of this guidance document do not have the force and effect of law and do not bind the public in any way. This guidance document only intends to provide clarity to the public regarding existing requirements under law or regulation and supersedes all versions of the DAAPM. This document is considered Cognizant Security Agency (CSA)-provided guidance in accordance with Title 32 Code of Federal Regulations Part 11718(a), National Industrial Security Program Operating Manual (NISPOM).

CLARIFICATION FOR OFFLINE SOFTWARE LICENSING REGISTRATION

Industry requested clarification on whether a customer risk acceptance memo is required to move the software activation code from a classified system using the DCSA Assured File Transfer (AFT) Procedure to support offline activation.

Response: A customer risk acceptance memo is not required to move an unclassified vendor activation code from a classified system using the DCSA approved AFT process for American Standard Code for Information Interchange (ASCII) text verification. ASCII text is an approved DCSA format.

The AFT procedures must be authorized as part of the system authorization to operate.

ENHANCING QUALITY WITH FSO SURVEY CALLS

DCSA has launched a new initiative to enhance the quality and effectiveness of its contractor security reviews by conducting telephonic surveys with FSOs that have recently undergone a security review.

This program underscores DCSA's commitment to providing valuable and accurate security reviews that help safeguard our nation's critical assets. The surveys will play a vital role in ensuring the quality of DCSA's services and provide crucial feedback for continuous improvement.

Each month, DCSA selects a sample of contract companies that have undergone a security review within the past 60 days. FSOs at these companies are then contacted to participate in a brief telephonic survey.

The purpose of these surveys is to:

- Verify the accuracy and thoroughness of the security review process.
- Gather feedback from FSOs on their security review experience and identify areas where DCSA can improve its processes and communication.
- Use insights gained from these surveys to continuously refine and improve DCSA's security review processes to ensure their relevance and effectiveness in a constantly evolving threat landscape.

When your company is selected, a DCSA representative will contact you via telephone to conduct the survey. The survey will consist of questions related to your experience with the recent security review, covering topics such as:

- Entrance and Exit briefings conducted by the ISR.
- Confirmation that the ISR reviewed Security Education, Access Authorizations, Insider Threat Program, Reporting Requirements, Self-Inspection, DD 254(s), and Safeguarding (as applicable).
- Whether employee interviews were conducted and the method (in-person or phone).
- The approximate length of the review.
- Receipt of the Letter to Management, the FSO Comment Sheet, and the Security Rating.

Participation in the survey is voluntary, but your input is highly valued and will directly contribute to improving the quality and effectiveness of DCSA's security reviews.

The Importance of Quality Assurance: By actively soliciting feedback from FSOs, DCSA is taking a proactive approach to ensure the ongoing quality and relevance of its security review process. This initiative reinforces DCSA's dedication to partnering with Industry to protect national security interests and maintain a robust and resilient defense industrial base.

DCSA encourages FSOs to participate in these surveys as their feedback is essential in helping DCSA deliver the best possible security review services. Your partnership is vital in ensuring a secure and resilient national security posture.

DCSA FORM 147, JANUARY 2025 - IMPLEMENTATION

DCSA announced the 90-day transition period in July for the recently released DCSA Form 147, Open Storage Area and Vault Approval Checklist, dated January 2025. This revision significantly reduced the time required to complete the form and reduced the page count by more than half. The form's purpose remains the same: to provide a sufficient description of an approved open storage area and increase the transition of older closed areas to current policy standards throughout industry.

DCSA Form 147 is available for download at NISP Tools & Resources (under the Industry Tools FSO Forms dropdown). DCSA's "soft-landing" approach concludes on September 30, 2025. As of October 1, 2025, only the January 2025 version of DCSA Form 147 should be submitted.

Important Notes

Open storage areas and vaults approved using DCSA Form 147, April 2022 version, will remain valid.

Each closed area approved using the obsolete one-page DCSA Form 147 must be updated and documented as an "open storage area" using the new form. The deadline for this transition has been extended to October 1, 2027. Industry must submit the DCSA Form 147 to their assigned ISR to complete this transition for each approved space.

If you have any questions or need assistance, please contact HQ DCSA, NISP Mission Performance (NMP) Division at dcsa.quantico.dcsa.mbx.isd-operations@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.

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 CONTAINER USE AFTER DECOMMISSIONING

The container 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.

INTERNATIONAL REQUESTS FOR VISITS PROCESSING

The DCSA International and Special Programs (ISP) office processes requests for visits (RFVs) for cleared U.S. contractors who are traveling internationally to access foreign classified sites and/or classified information up to the Top Secret, collateral level.

To ensure your RFV can be processed, please follow these steps:

1. Download the Latest DCSA Template: Every RFV *must* use the most current template from the DCSA Outgoing International Visits website. **Do not reuse old templates; they will be rejected.**

2. Adhere to Country-Specific Requirements: Foreign governments mandate specific requirements that change frequently. Failure to meet these requirements *guarantees* rejection. **Thoroughly review and comply with all country-specific rules before submitting *any* RFV.**

3. Meet All Lead Times by Planning Meticulously: Allow adequate time for both DCSA internal processing (5 business days) and the relevant country-specific lead time. While the standard lead time for most countries is 30 calendar days, the following exceptions apply:
    - 45 calendar days: Italy
    - 24 calendar days: Australia
    - 21 calendar days: France, Israel, and Sweden
    - 15 calendar days: Albania, Austria, Czech Republic, Poland, and Romania
    - 10 calendar days: Slovakia and South Korea

    Note: These lead times are subject to change, so always verify the most current information before submitting. **Submissions that do not meet the required lead times will not be processed.**

4. Know Your Visit Type: The correct visit type must be indicated on your RFV or it will be rejected.
    - One-Time: For visits lasting 30 days or less.
    - Recurring: For visits lasting between 30 and 364 days. Visits exceeding 364 calendar days are not permitted.
    - Emergency: For short-notice visits that do not meet standard lead times and require an emergency letter of justification. Visit duration cannot exceed 30 days.
    - Amendment: Used only to add or remove visitors from an existing visit. Dates and sites cannot be changed using an amendment.

5. Submit Securely Through Approved Channels: All visit requests must be submitted through one of the following methods:
    - Email: Send a password-protected scanned PDF to dcsa.rfv@mail.mil. Provide the password in a separate email.
    - Fax: 878-274-4862
    - DoD Secure Access File Exchange (SAFE): When encrypting files, email the passphrase to dcsa.rfv@mail.mil (CAC required).

Tracking Your Submission. Within five business days of submitting your RFV, you should receive *either* a rejection email from our office outlining the necessary corrections, *or* a confirmation email indicating that your visit request has been forwarded to the respective foreign government. If you do not receive either email within this timeframe, please contact our office to confirm receipt of your RFV.

Adhering to these guidelines is *mandatory* to minimize delays, ensure your international missions proceed smoothly, and safeguard U.S. national security interests. **RFVs that do not meet these requirements are at risk of rejection.**

For more information, please visit our Outgoing International Visits website.

NCCS: NEW AND IMPROVED!

We implemented the NISP Contract Classification System (NCCS) v2.9.3 update on September 10, 2025 which added Treasury, Africom, and some components of the Army to the platform's hierarchy capabilities. This update also provides a more granular view of an organization's user base.

We're pleased to announce the release of the new NCCS System Authorization Access Request (SAAR) Process Job Aid, the new NCCS Help Desk Job Aid, and updated User Guides for Government and Industry users! These materials may be downloaded from the DCSA NCCS Training Materials website.

When requesting an account to NCCS, please download the DD 2875 SAAR Form from the DCSA NCCS Training Materials website. You will need to right click and "save link as" to save the SAAR to your computer, then open it from there to complete the form.

Please remember to sign into NCCS every 30 calendar days to keep your account active!

Questions? Contact us at dcsa.quantico.is.mbx.nccs-support@mail.mil.

OFFICE OF COUNTERINTELLIGENCE SVTC

DCSA invites cleared industry to participate in a Secure Video Teleconference (SVTC) with the Defense Industrial Base entitled, "Lessons from Protecting Additive Manufacturing." Air Force Office of Special Investigations (AFOSI) agents and analysts will be providing classified insights into the additive manufacturing sector. The brief will focus on counterintelligence information that can assist cleared industry in protecting intellectual property and technologies. Although focused on additive manufacturing, these lessons are broadly applicable across many industry sectors.

Army Counterintelligence Command agents will also provide a brief for cleared employees scheduled to attend the AUSA Annual Meeting & Exposition, held October 13-15, 2025 in Washington D.C.

The SVTC with cleared industry is an in-person event at most DCSA field offices on Thursday, 9 October, 2025, from 1:00 to 2:30 p.m. ET. Please register for the SVTC here by October 2, 2025.

NAESOC UPDATES

GET READY FOR THE NAESOC HELP DESK'S NEW LOOK

This fall, the National Access Elsewhere Security Oversight Center (NAESOC) will be unveiling an enhanced customer Help Desk service. Planned with industry partner support and aligned with the DCSA customer experience focus, we will be introducing a Help Desk update that will provide all our partners and customers with:

- A knowledge base packed with job aids, user guides and answers to the most frequently asked questions.
- A reduced dependency on "tracking and searching email traffic" to get you the answers you need.
- A personalized history of all the tickets you submit along with the status of each ticket.
- An option to use a virtual chat feature to connect with a member of our team.

You will still have access to our Live Agents to answer your questions.

What you can do to prepare for this rollout:

- Make sure your NISS profile has all current points of contact identified. The "contacts" section on the company NISS profile lists the name, phone number and email address for each of your authorized contacts. If you need to update the contacts list, please submit a Facility Profile Update.
- To ensure you receive all critical updates related to the Help Desk rollout, please add dcsa.eastern.dcsa.mbx.general-mailbox@mail.mil to your email system's safe sender list. These communications may include time-sensitive information, and we want to make sure they reach your inbox—not your junk or spam folder.

Be sure to also check the NAESOC website and future VOIs for key updates about this exciting new feature!

CONTACT US

- (878) 274-1800 for your 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

QUARTERLY INDUSTRY STAKEHOLDER ENGAGEMENT

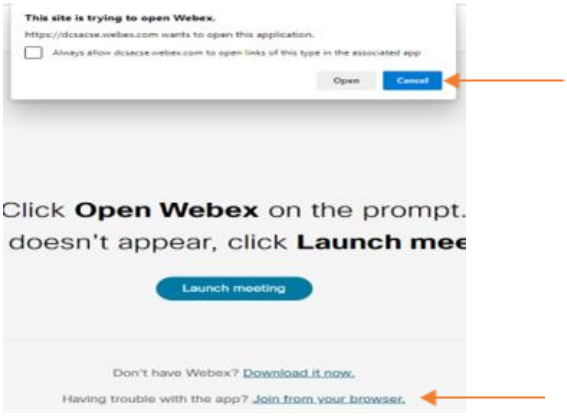
The DCSA Customer & Stakeholder Engagement (CSE) team will host the next quarterly Industry Stakeholder Engagement (ISE) on October 14, 2025, from 10:30 a.m. to 12:00 p.m. ET for all Industry FSOs and Security Professionals. The last engagement, held on July 10, 2025, resulted in an outstanding attendance of over 500 FSOs and industry security professionals and focused on best practices for FSOs, Catch'em-in CONUS processes, and Personnel Vetting Metrics and updates.

The October ISE will be held virtually via Webex and a dial in number. The tentative agenda for the meeting will consist of:

- Introduction/Welcome
- Personnel Vetting (PV) – Background Investigation, Continuous Vetting and Adjudication Metrics and Updates
- NBIS Program Executive Office – NBIS Updates
- NISS – NISS issue resolutions and NISS Increment 2 (NI2) updates
- NCCS – NCCS and onboarding processes
- Conclusion.

Note: When logging into Webex, please use your government/company email (vs. personal email) and First/Last name. This is beneficial to us to help address individuals and their questions.

Logging into Webex Meetings: After clicking on the meeting link or copy/pasting the link into your browser, click Cancel and then Join from your browser.



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

Phone: +1-415-527-5035

Access Code: 2820 312 1469

Join meeting

ADJUDICATION AND VETTING SERVICES (AVS)

AVS CALL CENTER NUMBER

The AVS Call Center can now be reached at 667-424-3850. The legacy CAS Call Center number is still active but will be deactivated soon.

As a reminder, the AVS Call Center will continue to provide direct support and timely adjudicative updates to Senior Management Officials (SMOs) and FSOs worldwide. The AVS Call Center is available to answer phone and email inquiries from SMOs/FSOs, provide instant resolution on issues identified by Security Offices whenever possible, and serve as the POC for HSPD12/Suitability Inquiries.

The AVS Call Center is available from Monday through Friday between 6:30 a.m. and 5:00 p.m. ET to answer phone and email inquiries from FSOs only. Contact the AVS Call Center by phone at 667-424-3850 (SMOs and FSOs ONLY; no subject callers), or via email at dcsa.meade.cas.mbx.call-center@mail.mil.

For Industry PIN Resets, contact the Applicant Knowledge Center at 878-274-5091 or via email at DCSAAKC@mail.mil.

SF 312 JOB AID

NISP contractor personnel may now sign SF 312s using a DoD Sponsored/Approved External Certificate Authority (ECA) Public Key Infrastructure (PKI):

- The use of digital signatures on the SF 312 is optional. Manual or wet signatures will still be accepted by AVS.
- If the Subject digitally signs the SF 312, the witness block does not require a signature.
- Digital signatures must be from the list of DoD Sponsored/Approved ECA PKI located here.
- The public list of DoD approved external PKIs that are authorized to digitally sign the SF 312 can be located here.

The Job Aid and OUSD I&S Memorandum are available on the DCSA Website.

REMINDER ON TIMING OF ELECTRONIC FINGERPRINT TRANSMISSION

As we move closer to full implementation of Trusted Workforce 2.0, AVS continues to work diligently to partner with Industry to get cleared people to work faster and more efficiently all while effectively managing risk. To maintain our interim determination timeliness goals, we ask that electronic fingerprints be submitted at the same time the investigation request is sent to the subject for completion. **Note:** this is an update to previous guidance that instructed FSOs to submit FPs at the same time the eApp is released to DCSA.

Fingerprint results are valid for 120 days, the same amount of time for which eApp signature pages are valid. Therefore, submitting electronic fingerprints at the same time or just before you complete your review for adequacy and completeness, should prevent an investigation request from being rejected for missing fingerprints.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

SEPTEMBER PULSE NOW AVAILABLE

DCSA recently released the September CDSE Pulse, a monthly newsletter that features topics of interest to the security community as well as upcoming courses, and webinars. The latest edition focuses on National Insider Threat Awareness Month (NITAM). View the Pulse in CDSE's Electronic Library or subscribe to have the newsletter sent directly to your inbox.

INSIDER THREAT

CDSE Releases 100th Case Study. CDSE hit a major milestone by recently releasing the 100th case study profiling Ji Chaoqun. Chaoqun is a Chinese citizen who came to the U.S. from Beijing, China in August 2013 on an F1 visa. Chaoqun holds a master's degree in electrical engineering from the Illinois Institute of Technology in Chicago.

In 2016, Ji enlisted in the U.S. Army Reserves under the Military Accession Vital to the National Interest (MAVNI) program. During his time in the reserves, high-level intelligence officers from the Jiangsu Province Ministry of State Security (JSSD) recruited Chaoqun as part of an effort to obtain access to advanced aerospace and satellite technologies being developed by U.S. companies. Chaoqun was convicted in 2023 of acting illegally within the United States as an agent of the People's Republic of China and was sentenced to eight years in prison.

With the release of the 100th case study, CDSE cements the position as the premier providers of security training to the federal government and industry partners. Audrey Gutierrez, CDSE director, remarked "reaching 100 case studies reflects not just hard work, but creativity, persistence, and a real commitment to excellence. I'm grateful for the standard set by our team I'm proud of the impact this work continues to have."

This achievement is not only a credit to the instructors, instructional system designers, and curriculum managers, but also to the web team, editors, designers, and outreach and engagement. CDSE case studies have had over 120,000 views on the CDSE website.

Case studies profile individuals sentenced for counterintelligence, cyber, or insider threat crimes and include a short summary of the crime, indicators, and outcome or conviction.

Two New Courses Coming Soon!

- Supervisor and Command Leader Awareness of Insider Threat Risk (INT215) is under development to be released soon. The course will provide realistic scenarios and examples of insider threat behavior and how organizational culture, proactive engagement, and leadership actions play a role in risk mitigation.
- A new Establishing an Insider Threat Program for Your Organization (INT122.16) e-Learning course is planned for release in November. The course will provide practical guidance on developing compliant insider threat programs.

SPECIAL ACCESS PROGRAMS (SAP)

FY26 Special Access Programs Course Released. The FY26 Special Access Program (SAP) for "Introduction to SAPs" is now available. The course introduces new SAP security professionals to the security requirements outlined in the DoDM 5205.07 utilizing practical exercises. Both in person and virtual training options are available.

SAP Markings Short. The CDSE SAP team released an updated SAP Markings short. This short covers SAP specific markings as outlined in DoDM 5200.01 volume 2. This short will outline the appropriate markings, as well as how to recognize and apply control markings.

INFORMATION SECURITY

Activity Security Manager INFOSEC VILT Course Schedule for FY26. The Activity Security Manager INFOSEC VILT course (IF203.10) provides students with knowledge to implement information security policies and procedures to mitigate and manage risks associated with developing, managing, and evaluating an information security program (ISP). Lessons emphasize key activity security manager responsibilities in relation to protecting classified national security information and controlled unclassified information (CUI).

This mid-level course includes security classification, downgrading, declassification, safeguarding and handling, access and dissemination control, accountability, storage, disposal, destruction, transmission and transportation, security incidents, and security education and training awareness. Register here to secure your spot!

Updated Products. CDSE has published updated versions of the following products:

- The Transmission and Transportation for DOD (IF107.16) eLearning course offers a more interactive scenario based instructional course to effectively implement regulatory guidance.
- The NOFORN REL/TO job aid replaces the CDSE NOFORN/REL trifold with quick reference and scenario-based examples to support implementing regulatory guidance and dissemination control markings.
- The Original Classification Authority (OCA) desktop reference reflects new policy guidance for the original classification process communicated in the January 2025 issuance of DODM 5200.45, Original Classification Authority and Writing a Security Classification Guide. It provides a quick reference and scenario-based examples regarding original classification process.
- The Marking Syntax for U.S. Classified Information job aid addresses the correct marking syntax for classified information in accordance with regulatory guidance. The job aid supports the CDSE Marking Syntax short.

FISCAL YEAR 2025 UPCOMING COURSES

CDSE courses are a great way to gain security knowledge, gain awareness, and expand skill sets.

Secure your spot now as classes fill quickly! Available instructor-led training (ILT) or virtual instructor-led training (VILT) courses are listed below.

INDUSTRIAL SECURITY

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

Oct. 21-24, 2025 (virtual)

CYBERSECURITY

Assessing Risk and Applying Security Controls to NISP Systems (CS301.01)

Nov. 3-6, 2025 (Linthicum, Md.)

CDSE NEWS

Get the latest CDSE news, updates, and information. You may be receiving the Pulse through a subscription already, but if not and you would like to subscribe to the Pulse or one of our other products, visit CDSE News and sign up or update your account.

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.