DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

June 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

MODERNIZING TRUST: CHANGES TO DCSA CREDENTIALS

For cleared entities participating in the NISP, trusting the personnel who walk through your doors is the first line of defense in protecting national security. FSOs and cleared personnel interact daily with DCSA representatives. Historically, establishing this trusted identity relied on the presentation of a physical badge and credential.

To streamline identification practices, align with broader security enterprise standards, and minimize access requirements, DCSA is modernizing its identification model. Over the next months, DCSA will fully transition to using our Department of War (DoW) issued Common Access Card (CAC) as the primary identification for our ISRs, Industrial Security Systems Professionals (ISSPs), and Counterintelligence Special Agents (CISAs). DCSA representatives will no longer have the folio badge and credential.

What Facility Security Officers Need to Know

To ensure a seamless transition and to prevent any confusion or delays during facility visits, DCSA is rolling out this change in two phases. Depending on the type of DCSA representative visiting your facility, you will see new forms of official identification:

- Phase 1 (By July 31, 2026): DCSA ISRs, ISSPs, and CISAs will transition to using their CAC as their sole, official form of identification credential during official visits. In addition, DCSA will be processing Visit Access Requests (VAR) in DISS to each cleared possessing facility. DCSA will work closely with NISPPAC Industry on the process.
- Phase 2 (By Dec. 30, 2026): Our background investigation workforce will present a new folio containing an official badgeless credential document. This folio will be presented alongside their CAC to establish their identity and authority.

Authorities and NISPOM Compliance Remain Unchanged

While the physical form of DCSA credentials is changing, the operational authority of DCSA personnel to carry out DCSA missions remains the same.

For the Industrial Security workforce, the DD Form 441, “Security Agreement,” is required to be executed by each cleared contractor. The agreement in Section II addresses access for designated representatives of the Government, in this case DCSA, to conduct reviews of your cleared contractor facility for the purpose of oversight of the requirements established by 32 CFR Part 117, the National Industrial Security Program Operating Manual (NISPOM).

For the investigate workforce, the NISPOM requires cleared contractors to cooperate with officially credentialed U.S. Government and contractor representatives of Federal agencies as outlined in Part 117.7(f).

Continued Commitment to Verification

DCSA recognizes that verifying the identity of our personnel is critical to maintaining your facility's security posture. If your security staff ever needs to definitively confirm the identity of a DCSA background investigator, they can call 878-274-1186. FSOs may also verify the identity of an ISR, ISSP, or CISA, in the National Industrial Security System (NISS).

As we transition away from badges, these verification methods will continue to operate without interruption, ensuring you can always validate a DCSA representative's authority with confidence.

DCSA values its trusted partnership with cleared industry. By modernizing our credentialing process, we aim to make facility visits more efficient and secure, allowing us to collaboratively focus on our shared mission of protecting national security.

UPCOMING GAO SURVEY ON TRUSTED WORKFORCE 2.0

The U.S. Government Accountability Office (GAO) will soon be distributing a survey to selected federal contractors regarding the implementation of the Trusted Workforce 2.0 personnel vetting reform initiative. We greatly appreciate your timely cooperation with GAO in this matter.

The U.S. GAO is an independent, nonpartisan agency that reports to Congress on the efficiency and effectiveness of federal programs. GAO provides Congress, the heads of executive agencies, and the public with timely and fact-based information to improve government and save taxpayers billions of dollars.

Congress directed GAO to review the government-wide implementation of the Trusted Workforce 2.0 personnel vetting reform initiative to assess (1) the strengths and weaknesses of the initiative and (2) risk management during the vetting of federal and contractor personnel. GAO is currently conducting the second of three surveys and is requesting input from federal contractors with active security clearances on the implementation of Trusted Workforce 2.0. For reference, GAO included the results of the first survey in a report issued in May 2025, available at GAO-25-107325.

To inform GAO's response to Congress for this second iteration of the survey, GAO is surveying a generalizable sample of contractors to understand the benefits and challenges related to the implementation of Trusted Workforce 2.0. Those selected for the sample will be invited to attend one of two optional discussions about survey participation and will receive the survey link in an email from a gao.gov email address as early as July.

GAO greatly appreciates your generous time and support in their efforts and looks forward to including the contractor perspective on Trusted Workforce 2.0 implementation in its report.

SECURITY REVIEW RATING RESULTS FISCAL YEAR 2026

The following security review results are current as of June 30, 2026:

Overall Fiscal Year Goal:	3,900	
Rated Security Reviews Completed:	2,989	(76.6%)
Rated Security Reviews Remaining:	911	(23.4%)
Superior Ratings Issued:	324	(10.8%)
Commendable Ratings Issued:	1,081	(36.2%)
Satisfactory Ratings Issued:	1,571	(52.6%)
Marginal Ratings Issued:	5	(00.2%)
Unsatisfactory Ratings Issued:	8	(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.

UPDATES TO THE SECURITY REVIEW RATING SCORE TOOL

DCSA is rolling out an enhanced version of the Security Review Rating Score Tool beginning July 1, 2026. **Please note that the Scorecard – including all gold standard criteria and associated elements – remains unchanged.** These updates apply to the calculation tool itself, focusing on streamlining the user experience, introducing smart automation, and making minor structural layout adjustments to improve clarity and communication. The goal is to improve our industry partners' awareness of how their security rating was calculated and ensure they clearly understand their areas of success and opportunities for growth.

Below is a quick overview of what you need to know:

- **What is Changing?** The calculation Tool now features criterion element lettering, color-coded statuses, automated dependency links (auto-links), and reorganized tabs for a cleaner, "one-stop-shop" experience. The DCSA Security Rating Gold Standard Criteria Reference Card has also been reformatted to better support effective communications.
- **What is NOT Changing?** The DCSA Security Rating Gold Standard Criteria and associated elements themselves and the standard artifacts provided post-security review remain the same.
- **Who Should Use This Tool?** DCSA ISRs will begin using the Tool for post-security review calculations as soon as comfortable during the soft-launch phase. FSOs are highly encouraged to use the Tool for self-inspection rating calculations.
- **When is the Tool Effective?** Soft launch begins on July 1, 2026. Full implementation will come later in Q4, 2026 based on feedback from the field. During the soft launch phase, both versions of the Tool and reference card will be available on the DCSA website for reference.
- **How Will DCSA Communicate This to Industry?** In addition to this VOI article, DCSA has posted a copy of the enhanced Tool, reformatted reference card, and associated Comprehensive User Guide on the Security Review and Rating Resource page.

Visit the DCSA Security Review and Rating Process page (Resources tab) to access the following resources:

- DCSA Security Review Rating Score Tool 2.0
- DCSA Security Rating Gold Standard Criteria Reference Card 2.0
- Comprehensive User Guide: DCSA Security Review Rating Score Tool 2.0

For questions related to this article, please contact the DCSA NISP Operations Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

OFFICE OF COUNTERINTELLIGENCE SVTC & WEBINAR

DOW ADVANCED BATTERIES CLASSIFIED INDUSTRY SVTC

The 2026 National Defense Strategy called for supercharging the U.S. defense industrial base (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 a classified Secure Video Teleconference (SVTC) with the Office of the Secretary of War's Industrial Base Policy (IBP) Office on threats to DoW battery supply chains. The IBP battery team will explain what makes DoW battery supply chains unique, the adversarial techniques, tactics and procedures used to hold DoW and industry at risk, and what DoW is doing about the threat. Briefers will identify ways you can help, whether you are in security, contracting, procurement, R&D, or another role.

The SVTC is an in-person event at most DCSA field offices on July 9, 2026, from 1:00 to 2:30 p.m. ET. Register at SVTC Registration no later than Monday, July 6, 2026.

THE NEXUS BETWEEN COUNTERINTELLIGENCE AND FRAUD WEBINAR

The Center for Development of Security Excellence (CDSE) DCSA Counterintelligence Curriculum Manager and Certified Fraud Examiner will provide a presentation on the nexus between counterintelligence and fraud that will address how threat actors including foreign intelligence entities and adversaries utilize illicit fraud activities to try and acquire access to personnel, information, systems, and facilities as well as fund their illicit activities.

The webinar will be held virtually via CDSE Adobe Connect on July 16, 2026, from 12:00 to 1:30 p.m. ET. Please register at CDSE Events.

INTERNATIONAL OUTGOING VISITS OUTREACH

The DCSA International and Special Programs Division is pleased to invite you to a comprehensive webinar on July 22, 2026, at 1:00 p.m. ET.

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

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

You'll have the opportunity to ask questions directly, and we welcome your input on how DCSA can better support your needs. Please save the date on your calendar! Click the link FSO International Visits Outreach to join the meeting on July 22, 2026 at 1:00 p.m. ET.

DCSA INDUSTRY STAKEHOLDER ENGAGEMENT

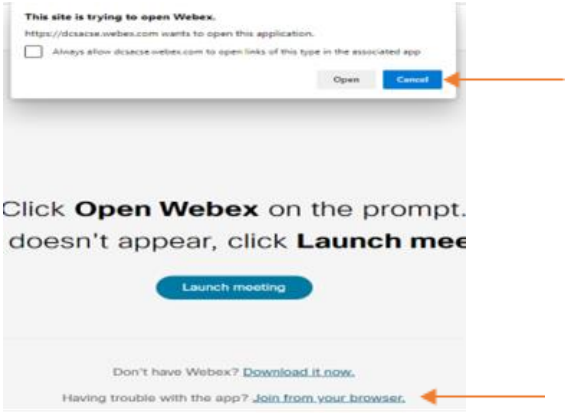
The DCSA Customer & Stakeholder Experience (CSE) Team will host the next quarterly Industry Stakeholder Engagement (ISE) on July 14, 2026, from 10:30 a.m. to 12:00 p.m. ET for all Industry FSOs and Security Professionals. The last engagement, held on April 14, resulted in an outstanding attendance of over 760 FSOs and Industry Security Professionals and focused on Background Investigation, Trust Decision, and NBIS updates along with information on Methods of Contact, Methods of Operation (MCMO).

The July ISE will be held virtually via Webex and a dial-in number. The agenda for the meeting consists of:

- Introduction/Welcome
- Personnel Vetting (PV)
  - Background Investigation Metrics and Updates
  - Continuous Vetting and Trust Decision Metrics and Updates
- NBIS Service Level Management – NBIS Updates
- Customer Engagements Team – IRA to DISS Demo
- 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: 2824 121 5999

Join from the meeting link: DCSA Industry Stakeholder Engagement (ISE) Meeting

NAESOC

THE GOVERNMENT SERVICE PORTAL - SERVICENOW IS LIVE!

The National Access Elsewhere Security Oversight Center (NAESOC) is excited to roll out ServiceNow, our new hub for streamlined communication and faster service delivery.

NAESOC FSOs now have the direct option to submit inquiries and track issues through the DCSA Government Service Portal. This launch officially transitions our support into a more transparent, real-time interactive experience.

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**

GETTING STARTED & ESSENTIAL STEPS

To ensure successful navigation and utilization of this new capability, please complete the following steps:

1. **Access the Portal**: Log in and submit your queries via the DCSA Government Service Portal.
2. **Review the Job Aid**: Refer to the Ticket Submission Job Aid attached to our previous *Government Services Portal* email to assist you with the new submission process.
3. **Stay Informed**: To guarantee you receive critical notifications and updates, please add dcsa.naesoc.generalmailbox@mail.mil to your email's safe sender list.
4. **NISS Profile Maintenance**: Verify that your NISS profile reflects your current points of contact to ensure seamless communication.
5. **Urgent Issues**: For time-sensitive matters, please use the **Blue Button** *(Escalate an Existing Inquiry)* on the NAESOC website.

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

NATIONAL BACKGROUND INVESTIGATION SERVICES

THE FUTURE OF PERSONNEL VETTING: A UNIFIED PATH FORWARD

The coming months will mark a significant transformation in the personnel vetting landscape as we move toward a single, integrated, and efficient system. Our goal is to deliver on the promise of Trusted Workforce 2.0, transitioning from fragmented systems to a unified platform in the Defense Information System for Security (DISS). Here is what you need to know about the upcoming changes.

1. RETURNING INITIATION, REVIEW, AND AUTHORIZE (IRA) TO DISS

This summer, the IRA functionality will return to DISS, a move designed to create a seamless, end-to-end personnel vetting process within a single system. This consolidation eliminates the need for security managers to switch between DISS and the National Background Investigation Services (NBIS), a practice often referred to as the "swivel chair."

Benefits for Industry:

- A Single System: All vetting activities—from a new member's initial form submission to status management and continuous vetting enrollment—will occur in DISS. This creates a single source of truth and streamlines the entire process.
- Familiar Territory: The industry is well-positioned for this transition. Your hierarchies are already established in DISS, and many of you have experience with the previous iteration of IRA in the system.
- Minimal Preparation: To facilitate a smooth transition, a one-time script will be run in July to grant "Initiate" and "Review" permissions to Security Managers and Security Officers. Hierarchy and Account Managers will retain the ability to modify these permissions as needed.

Note: The applicant experience will not change; eApp will remain the portal for individuals to access and complete their vetting forms.

2. EARLY ADOPTION OF THE PERSONNEL VETTING QUESTIONNAIRE

The Standard Forms (SF) are being replaced by the new Personnel Vetting Questionnaire (PVQ), a single, modernized form built for all Trusted Workforce 2.0 vetting scenarios. The PVQ is designed to be more efficient and user-friendly.

Key Updates:

- Streamlined Content: The "look-back" period for most questions is reduced from 7–10 years to 5 years, aligning with the five-year continuous vetting update cycle.
- Modernized Questions: Questions have been updated to be more common-sense. For example, mental health inquiries are now focused on a 5-year window and target specific conditions that could impact judgment, removing the stigma from routine counseling. The PVQ also separates marijuana from other drugs and shortens its look-back period.

- Reduced Redundancy: Secondary questions about physical characteristics (height, weight, eye/hair color) and Selective Service Registration have been removed.

The rollout began on June 1 with a small group of 10 companies initiating the PVQ for 5-year updates. A broader rollout will follow.

3. SELF-REPORTING IN THE INDIVIDUAL ENGAGEMENT PLATFORM

The Individual Engagement Platform (IEP) is a live, applicant-facing system that provides individuals with greater transparency into the status of their application. The next major feature, expected in September, is self-reporting. This will empower individuals to report required life events and updates (e.g., foreign travel, financial changes) directly through an intuitive, categorized menu.

This new functionality is NOT intended to remove the Facility Security Officer (FSO) from the process. The plan is for self-reported information to be presented in DISS for review and action by the appropriate security personnel, ensuring they remain fully informed.

4. KEY DATES AND UPCOMING MILESTONES

Please keep these critical upcoming milestones in mind as we transition to the new, unified system.

DATE	EVENT
June 25	DISS Release 14.8 goes into production, finalizing authorization and system connections.
June 29	A small group of industry early adopters begins using the new IRA functionality in DISS.
Late June	Training materials (guides, videos) become available on STEPP and other platforms.
July 14	A DISS IRA walkthrough and screen share session will be hosted during the Industrial Security Engagement (ISE) meeting.
July 23-24	A one-time script runs to enable Initiate and Review permissions for Security Managers in DISS.
Late July	An NCMS Live event will feature another Defense Industrial Base (DIB) Security DISS-JVS user walkthrough.
Early August	Ad-hoc ISE sessions will be available as needed.
September 30	New initiations will no longer be possible in NBIS Agency.
November 30	NBIS Agency will be shut off. All remaining NBIS-Agency cases in an IRA phase must be re-initiated in DISS.
September	Development for IEP Self-Reporting is scheduled to be completed and deployed for use.
Fiscal Year (Target)	Initiation of initial investigations using the PVQ is planned to be available in DISS.

TRUST DECISION (ADJUDICATIONS)

KEY CHANGES FOR DISS NATIONAL SECURITY DETERMINATION VALUES

To ensure clarity and consistency across the enterprise, DCSA is updating the National Security Determination Values within DISS. These changes align the terminology seen in DISS with established adjudicative guidance (79A), which will affect how determination statuses are displayed and interpreted by users in the field.

Security Management Officers (SMOs) must be aware of these new values to correctly understand the status of their personnel within DISS. While some values remain unchanged, several key legacy terms are being replaced with more descriptive and precise language.

To help you prepare for this transition, we've outlined the direct mapping from the old (Legacy) values to the new ones in the following table.

LEGACY DISS VALUES	NEW DISS VALUES BASED ON 79A
Favorable	(1) Favorable security clearance/eligibility determination under E.O. 12968
Loss of Jurisdiction	(4) Resigned, terminated, or withdrew application prior to determination
No Determination Made	(11) Other action taken
Revoked or Denied	(10) Letter of intent to deny or revoke eligibility for access per E.O. 12968
No Action	No Action
None	None

What This Means for You

When you review a case in DISS, you will begin to see these new determination values instead of the legacy terms you may be used to. It is crucial for all SMOs to familiarize themselves with this new terminology to prevent misinterpretation of an individual's security eligibility status.

We encourage you to share this information within your organizations to ensure a smooth transition for everyone interacting with the DISS platform.

NI2 FOCI RISK MITIGATION KICKOFF

STRENGTHENING READINESS FOR UPCOMING DFARS RELEASE

The NISS Increment II (NI2) Foreign Ownership, Control or Influence (FOCI) Evaluation Team officially launched its Risk Mitigation Kickoff and Registration Walkthrough this week, marking an important step toward preparing for the upcoming Defense Federal Acquisition Regulation Supplement (DFARS) updates expected by October 1, 2026.

This session was designed to ensure every team member has a clear understanding of the roles, responsibilities, activities, and timeline associated with the NI2 FOCI Assessment. A key focus of the kickoff was a guided walkthrough of the NI2 registration process, ensuring all participants can successfully register for the roles required to complete the assessment.

To support the team's readiness, a comprehensive set of resources has been made available, including detailed demonstrations that walk users through each stage of the FOCI process within NI2. These materials are intended to serve as a reference throughout the evaluation period.

As the assessment progresses, the team will document any enhancements or additional capabilities needed to strengthen NI2's functionality - particularly those that will support compliance with the forthcoming DFARS revisions. This proactive approach ensures NI2 will continue to evolve in alignment with regulatory expectations and mission needs.

The kickoff marks the beginning of a collaborative, forward-looking effort to ensure the NI2 platform is fully prepared to support FOCI assessments well into the future.

SECURITY TRAINING

2026 VIRTUAL DCSA SECURITY CONFERENCE

SAVE THE DATE: September 14 - 18

For the first time, this event unifies the Department of War and industry partners to collaborate, share critical policy updates, and protect our nation's technological edge. Registration and full agenda will be available later this summer.

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.

SETA PULSE

The June 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 Shorts - Learn about these insider threat topics in just 10 minutes or less: Human Resources, Cybersecurity, and Law Enforcement.
- Infamous Spies Posters - Two new products were published for the Infamous Spies poster series: Ana Montes and Peter Debbins.
- 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)

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)

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)

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)

WEBINARS

Malice, Mental Illness, and Mitigation: Understanding the Role of Mental Illness in Targeted Violence
July 15, 2026 | 1 - 2:30 p.m. ET

The Nexus Between Counterintelligence and Fraud
July 16, 2026 | Noon - 1:30 p.m. ET

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

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