DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

September 2021

(Sent on behalf of your ISR)

Dear FSO,

This monthly newsletter contains recent information, policy guidance, security education, and training updates. Please let us know if you have any questions or recommendations for information to be included.

WHERE TO FIND THE "VOICE OF INDUSTRY" (VOI) NEWSLETTER

VOI Newsletters are posted for Facility Security Officers (FSOs) in the National Industrial Security System (NISS) Knowledge Base. Look for a monthly announcement on your NISS dashboard for each new VOI. VOI Newsletters are also found with important forms and guides on the Defense Counterintelligence and Security Agency (DCSA) website Industry Tools Page (VOIs are at the bottom). For more information on personnel vetting, industrial security, and other topics in the VOI, visit www.dcsa.mil.

TABLE OF CONTENTS

DCSA'S NEW FIELD STRUCTURE

DCSA is establishing a new regional field structure on October 1. The new structure merges existing field mission areas into a four-region structure that includes Western, Central, Eastern, and Mid-Atlantic jurisdictions. With this new structure in place, for some stakeholders, DCSA points of contact (POCs) may change. If your DCSA POC is changing, your current Counterintelligence Special Agent (CISA), Industrial Security Representative (ISR), or Information Systems Security Professional (ISSP) will notify you and ensure there is no break in support. Address any questions about changes to your current CISA/ISR/ISSP. More information can be found here.

SECURITY REVIEW AND RATING PROCESS UPDATE

Effective September 1, DCSA began conducting security reviews based upon the refined security review approach, which is aligned to current national and DoD policies. DCSA personnel are scheduling and visiting on-site contractor personnel to verify the security program is protecting classified information and implementing the provisions of "the NISPOM Rule."

At the conclusion of the security review, DCSA personnel are rating the facility's security posture using the security rating process. This process is a compliance-first model that eliminates enhancements. It then utilizes a whole company approach based on analysis of the corporate culture, management support from the top, employee awareness, and cooperation within the security community.

DCSA held a Security Rating Process webinar on September 16. To view a recording of this webinar or to review the webinar questions and answers, please visit the DCSA Security Review and Rating webpage.

REGISTER NOW FOR THE SEAD 3 Q&A WEBINAR

Register now for the Security Executive Agent Directive 3 (SEAD 3), "Reporting Requirements for Personnel Who Access Classified Information or Those Who Hold a Sensitive Position," Question and Answer Webinar. DCSA Critical Technology Protection (CTP) Directorate will host a joint DCSA and cleared industry panel to address industry questions associated with the implementation of SEAD 3 as outlined in Part 117 of Title 32 CFR, the NISPOM Rule, and the SEAD 3 Industrial Security Letter. Cleared industry under DOD cognizance should email questions to dcsa.quantico.dcsa-hq.mbx.policyhq@mail.mil. Questions must be submitted by October 4 to allow time for coordination. The webinar, as well as the questions and answers, will be recorded and posted to the DCSA NISPOM Rule webpage after the event.

Register now for the SEAD 3 Q&A Webinar:

- Reporting Requirements for Personnel Who Access Classified Information or Those Who Hold a Sensitive Position
  October, 12, 2021
  1:00 p.m. – 2:00 p.m. EDT

DCSA CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI IMPLEMENTATION PHASE 1

On October 1, DCSA will begin operationalizing its eight CUI responsibilities using a phased approach and will be in an initial operating capability throughout fiscal year 2022. Phase 1 starts with the standup of a centralized program administration office (hereafter referred to as the DCSA CUI Program Office), which will begin executing several administrative functions, including developing processes and procedures, engaging Government and Industry stakeholders, and producing tools, training, and resources to support Industry's development, management, and sustainment of CUI programs within their contractor facilities.

DCSA will also develop unauthorized disclosure and threat notification processes in accordance with two of its eight responsibilities. As processes are developed, information will be provided to Government and Industry partners on how to report both unauthorized disclosures of, and threats to, CUI. Effective October 1, and until formalized processes are in place, Government and Industry partners should notify the DCSA CUI Program Office mailbox at dcsa.quantico.ctp.mbx.eso-cui@mail.mil of any instances involving unauthorized disclosures of, or threats to, CUI.

DCSA will not assess contractor compliance with contractually established CUI system requirements in DoD classified contracts associated with the National Industrial Security Program (NISP) during Phase 1. Instead, the DCSA CUI Program Office will develop and disseminate a number of tools and resources to support Industry's self-management and attestation of CUI programs resident at their locations. Several resources are already being developed with initial releases scheduled for October 2021 and other releases to follow before the end of the calendar year. Resources under development include:

- CUI Frequently Asked Questions
- CUI Quick Start Guide
- CUI Glossary
- CUI Baseline Requirements
- Self-Inspection Appendix for CUI
- Sample CUI Standard Practice and Procedure Template
- Compliance and Information Systems Controls Cheat-Sheets
- Marking Job Aid
- Training and Resource Job Aid

As these resources are finalized and approved for release, they will be posted to the DCSA Controlled Unclassified Information webpage. Government and Industry partners are strongly encouraged to bookmark that page and visit it frequently.

WHAT CAN INDUSTRY DO NOW?

- Review the DoD CUI Registry at https://www.dodcui.mil to become familiar with CUI organizational index groupings and CUI categories.
- Continue to review existing contracts and engage with Government customers to determine which, if any, CUI requirements are applicable to current contracts.

- Discuss the results of these engagements with your DCSA ISR.
- Review CUI resources and training available on the Center for Development of Security Excellence (CDSE) website.
- For contractors with contracts that have CUI requirements, consider adding a CUI-specific addendum to your facility's Standard Practice Procedures.
- Routinely monitor the DCSA CUI website for updates and new resources.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

RECIPROCITY GUIDE: DETERMINING SECURITY CLEARANCE OR SUITABILITY

This guide assists security managers and FSOs in determining if an individual has an existing security clearance or suitability determination, prior to sending in a Defense Information System for Security (DISS) Customer Service Request (CSR) for Reciprocity. The Request Reciprocity CSR is used to request eligibility for a subject who has a previous eligibility or investigation with another trusted Government agency to be transferred to DISS.

Prior to submitting a Request Reciprocity CSR, ensure you have an owning relationship with the Subject.

- If the Subject record does not exist, then you must create one prior to initiating the CSR. Conduct a review for the individual's eligibility in one of the following systems of record:
  - Scattered Castles
  - Central Verification System (CVS) within OPM
  - DISS Joint Verification System (JVS) (Here you should be able to verify the Investigation History and Adjudication History)
- If you determine the Subject has eligibility, generate a Request Reciprocity CSR with the following:
  - Request Reciprocity
  - Name of Former Agency (if unclassified)
  - Level of Clearance Eligibility
  - Type of Investigation
  - Agency which Conducted the Investigation
  - Date of Investigation
  - POC in your office (name, phone, and email)

  Example: Request Reciprocity with [former agency]'s clearance eligibility of [level - TS/SCI, TS, Secret] granted on [type of investigation- T5, T3, SSBI, etc.] conducted by [agency] dated [date of investigation].
- If you have verified the Subject's eligibility directly from the prior agency, please attach the supporting documentation (Inter-Agency Clearance Verification form, official emails, etc.) to the CSR.
- If there is no record of eligibility and no history of an investigation, initiate a new investigation for the Subject.
- If there is no record of eligibility and there is a history of an investigation, submit a CSR Supplemental Information for adjudication of the existing investigation.

DOD CAF CALL CENTER

The DoD CAF Call Center has resumed telephone services. Please contact us at 301-833-3850, or continue sending inquiries via email at dcsa.meade.caf.mbx.call-center@mail.mil. We look forward to hearing from you.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS VERSION 2.6 RELEASE

NISS Version 2.6 was released on September 27. Updated user guides and NEW eLearning videos have been posted to the NISS Knowledge Base to walk users through the new system.

The update includes:

- A modern look and feel
- Application performance improvements including faster loading and processing times, and shortened time-on-task
- Utilization of the "Back" button
- The capability to open multiple tabs and windows
- The "Search" bar is always visible within the system
- The "+Create" task button is always visible within the system
- Revised Quick Links

NCCS UPDATE

Due to community feedback relating to system challenges for implementing the NISP Contracts Classification System (NCCS), DCSA has decided to sunset the current NCCS application effective October 1. DCSA will be coordinating with the Office of the Under Secretary of Defense for Acquisition & Sustainment and the Office of the Under Secretary for Intelligence and Security (OUSD(I&S) to update the Federal Acquisition Regulation. Over the next few months, DCSA will develop NCCS 2.0, which has a tentative release date of Q2 FY22.

Until then, please email DD Form 254s to your respective Cognizant Security Office (CSO) located in Block 8, Part C, and copy to the NCCS mailbox.

- CSO email addresses can be found at https://www.dcsa.mil/mc/ctp/locations/
- The NCCS Mailbox address is dcsa.quantico.dcsa-hq.mbx.nccs@mail.mil

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

CONTINUED SUPPORT FOR THE ACCESS ELSEWHERE COMMUNITY

October marks the beginning of the NAESOC's third year supporting the NISP. Operational since 2019 with over 4,500 facilities assigned, it continues to administer the oversight mission for access-elsewhere companies and prepares for the intake of additional companies. There are significant and important updates on the NAESOC website this month:

NAESOC Latest Tab – Did you notice a change to the address on emails coming to you from the NAESOC General mailbox? Find out more here.

Reporting Tab – NAESOC facilities were provided additional updates to our enhanced counterintelligence support in September; more can be found here, along with details on reporting Cyber Intrusions, Facility Security Clearance Changed Conditions, updating your Facility Profile, and the latest on NISS.

Insider Threat Tab – You'll find information here on additional CDSE resources for your Insider Threat Program, Best Practices, and Common Insider Threat Vulnerabilities.

NISS Tips Tab – Here you can find links, resources, and Best Practices for Common NISS Questions.

VETTING RISK OPERATIONS (VRO)

PERSONNEL SECURITY INVESTIGATION FOR INDUSTRY BUDGET

Industry should disregard any memorandums received by Government Contracting Activities (GCAs) about suspension of submission of Personnel Security Investigation Requests. DCSA is not suspending the submission of Industry Personnel Security Investigation Requests. FSOs should continue to submit Personnel Security Investigation Requests to VRO for processing.

PRIME CONTRACT NUMBER REQUIREMENT

When submitting requests for Personnel Security Clearance (PCL) investigations in DISS, the prime contract number is a required field. DCSA may reject investigation submissions that do not include the prime contract number. This information is essential to validate contractor Personal Security Investigation submissions against their sponsoring GCAs.

PCL KNOWLEDGE CENTER INQUIRIES

In an effort to protect our workforce during the COVID-19 pandemic, Personnel Security Inquiries (Option 1/Option 2) of the DCSA Knowledge Center have been suspended. We will continue to provide status updates via DISS CSR and VRO email.

When calling (888) 282-7682, customers will have the following menu options:

- Industry Pin Resets, e-QIP Pin Resets, Golden Questions: HANG UP and call the Applicant Knowledge Center at 724-738-5090 or email DCSA Applicant Support
- Assistance Requests: Submit an Assistance Request via DISS
- All other PCL-related inquiries: Email the PCL Questions Mailbox.

APPLICANT KNOWLEDGE CENTER GUIDANCE

In order to improve the customer experience when initiating investigation requests in DISS and to provide the opportunity for DCSA to reduce call volume, please review Applicant Knowledge Center Guidance on the DCSA website prior to contacting the Applicant Knowledge Center and DISS Contact Center. For non-Industry customers, please contact your agency representative for assistance.

BREAK-IN-SERVICE

A break-in-service occurs when a cleared contractor ceases employment of an employee with eligibility for access to classified information whether initiated by the company (termination), by the employee (resignation), or by mutual agreement between the two. At such time, the employee is debriefed from access and is separated. As we move towards full implementation of Trusted Workforce 1.25 reform efforts, many changes will likely occur; however, at this time, processes and procedures have not changed as they relate to how a break-in-service is handled.

As it stands, FSOs are still required to submit a new SF-86 if there is a break-in-service of more than 24 months and the subject is not enrolled in Continuous Vetting (CV) or if the subject has an out-of-scope investigation. VRO will review the new SF-86 using a risk-based approach to determine whether the individual is eligible for automatic enrollment into CV via the deferred investigation method versus conducting a traditional Initial Investigation.

To that end, if the individual was previously enrolled in CV and their CV enrollment history displays "deferred investigation," then they are considered in-scope for their investigation and will not need a new SF-86 or subsequent investigation. While a break-in-access does not typically necessitate a new SF-86, it may be requested in some instances. It is important to note that clearances do not expire, and an FSO retains cognizance of their subject's eligibility and access status. Ultimately, an FSO can grant access in DISS.

NEW DISS JVS TRAINING MATERIALS

New DISS JVS training materials are now available on the DISS website! Simply go to DISS Resources for updated training aids and e-learning courses. Under the Trainings Aids subtab, you will find aids on how to do a verification by SSN, how to consolidate SMOs, and more. Do you have questions on how to create and manage visit requests or investigation requests? Want to know how to grant access and determine eligibility, and gain a thorough understanding of suitability determination? The E-Learning subtab has a link to DISS Training at USA Learning where new e-learning modules can be found. We invite you to click DISS Training for modules on Clearance Eligibility and Granting Accesses, Investigation Request, Suitability Determination and Homeland Security Presidential Directive 12 (HSPD12) for Non-sensitive Positions, Visit Requests, and others. Start your new course today to learn more!

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

SEPTEMBER PULSE: CDSE SECURITY AWARENESS NEWSLETTER

We recently released the CDSE Pulse, a monthly security awareness newsletter that features topics of interest to the security community. The September newsletter focused on Insider Threat. Check out all the newsletters in the DCSA Electronic Reading Room or subscribe/update your current subscription to get the newsletter sent directly to your inbox by submitting your email address to CDSE News!

CDSE WEBSITE MIGRATION

Our website recently migrated to a new web-hosting platform. While our homepage URL (www.cdse.edu) is the same, the rest of the website URLs have changed. This may impact your "Favorites" or "Bookmarks" pages. We apologize for any inconvenience this causes and thank you for your understanding.

2021 INSIDER THREAT VIRTUAL CONFERENCE

The 2021 Insider Threat Virtual Conference was held on September 2. The conference was open to security professionals in Government and Industry and was jointly hosted by DCSA and OUSD(I&S). The event brought together security professionals and policy makers from across the U.S. Government and Industry to kick of the National Insider Threat Awareness Month (NITAM) campaign. The theme for this year's conference and campaign was "Workplace Culture and Insider Threat." If you missed the conference, or would like revisit the presentations, the recordings will be available in the next few weeks.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE