DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

November 2021

Dear FSO (sent on behalf of your ISR),

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 CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) 2.0

In September 2020, the DoD published an interim rule to the Defense Federal Acquisition Regulation Supplement (DFARS) in the Federal Register (DFARS Case 2019-D041), which implemented the DoD's initial vision for the CMMC program and outlined the basic features of the framework (tiered model, required assessments, and implemented through contracts). The interim rule became effective on November 30, 2020, establishing a 5-year phase-in period.

In March, the DoD initiated an internal review of CMMC's implementation, informed by more than 850 public comments in response to the interim DFARS rule. This comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

In November, the Department announced CMMC 2.0, with an updated program structure and requirements designed to achieve the primary goals of the internal review:

- Safeguard sensitive information to enable and protect the warfighter
- Dynamically enhance Defense Industrial Base cybersecurity to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

The announcement marked the completion of an internal program assessment led by senior leaders across the DoD. These updates were initiated to focus on the need to enhance CMMC by (1) reducing costs, particularly for small businesses; (2) increasing trust in the CMMC assessment ecosystem; and (3) clarifying and aligning cybersecurity requirements to other federal requirements and commonly accepted standards. CMMC 2.0 was designed to meet these goals, which also contribute toward enhancing the cybersecurity of the Defense Industrial Base.

One of the key changes was to streamline the CMMC compliance levels from five to three and align them with National Institute of Standards and Technology (NIST) cybersecurity standards. CMMC Level 1 is foundational, based on 17 practices, and requires an annual self-assessment. Level 2 is based on the 110 security controls of NIST SP 800-171 and requires triennial third-party assessments for critical national security information and annual self-assessments for select programs. Level 3 is based on 110+ security controls of NIST SP 800-172 and requires triennial Government-led assessments.

The Department does not intend to approve inclusion of a CMMC requirement in any contract prior to completion of the CMMC 2.0 rulemaking process. The rulemaking process and timelines can take 9 to 24 months. CMMC 2.0 will become a contract requirement once rulemaking is completed.

It is highly recommended that Industry review the Securing the Defense Industrial Base CMMC 2.0 website.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS)

ELIGIBILITY REMOVAL FOR UNANSWERED REQUESTS FOR INFORMATION

Facilities are reminded to regularly monitor their DISS accounts for Requests for Information (RFIs) and any other changes that could influence the Personnel Security Clearance (PCL) eligibility of individuals under their responsibility. Under most circumstances, DCSA will provide facilities 60 days to answer RFIs, however, unanswered RFIs lasting over 90 days will result in DCSA removing the subject's PCL eligibility in DISS and replacing it with a "No Determination Made" status. Facilities that have any subjects with a "No Determination Made" status must immediately remove them from access to classified information in DISS to avoid the possibility of a security violation. To restore eligibility status after removal from the system, facilities must answer the RFI and submit a Customer Service Request (CSR).

NEW DISS JVS TRAINING MATERIALS

If you haven't done so already, check out the new DISS Joint Verification System (JVS) training materials on the DISS website! For updated training aids and e-learning courses, simply visit DISS Resources.

Under the Trainings Aids subtab, you will find aids on:

- JVS Access
- JVS initial Login
- Adding JVS to Firefox/Chrome
- DISS Troubleshooting Guide
- JVS Agency PSSAR_ReadOnly Access
- JVS Create PCAP User
- Verification by SSN
- Consolidating SMOs

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 to access modules on:

- Welcome to DISS
- Getting Started and Account Access
- Navigation
- Subject Management
- Clearance Eligibility and Granting Accesses
- Investigation Request
- Suitability Determination and Homeland Security Presidential Directive 12 (HSPD12) for Non-sensitive Positions
- Visit Requests

We encourage you to periodically check out DISS Resources content updates, as well as **DCSA Twitter:** @DCSAgov and **DCSA Facebook:** @DCSAgov for upcoming events!

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

ASSISTANCE WITH SUPPLEMENTAL INFORMATION REQUESTS

DoD CAF has published guidance on responding to Supplemental Information Requests (SIRs). The Supplemental Information Request Instruction is a guide for our customers to respond to DoD CAF requests and to navigate the process to completion. The instructions guide you to "Claim the Task," use the calendar to enter the Acknowledgement Date, and complete. Once you click "Complete," the task will be moved to Task-In-Process, and you will need to access the task from your task inbox to work the SIR. Once you have completed the request by following the guidance instructions, you will click "Complete" with any required attachments included in the response. The full Supplemental Information Request Instruction is located here.

DOD CAF CALL CENTER

The DoD CAF Call Center is available by telephone or email for inquiries. Please contact us at 301-833-3850 or via email at DoD CAF Call Center. We look forward to hearing from you.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

SECURITY REVIEWS FOR NAESOC FACILITIES

NAESOC welcomes facilities that are currently participating or will be participating in Security Reviews conducted by NAESOC! NAESOC has officially resumed Security Reviews and will contact you when it is time for your security review.

NAESOC RESOURCES

You might have asked, but even if you didn't, NAESOC has resources for you to help ensure your facility maintains its compliance for standard operations. Check out our NAESOC Web Page to find tabs and links that will assist you in maintaining that solid compliance standard, such as:

Updating your NISS Profile – You'll find instructions on how to do this on our page. Ensuring that your NISS profile is accurate provides a baseline for any Security Review. Make sure your facility is set for success! Also, you will find details on how and when to submit Changed Conditions.

Conducting a Self-Inspection – Don't allow yourself to be surprised. You can find instructions on accessing and using the Self-Inspection Handbook on our website to ensure you have the best security program possible for your facility.

Contacting the NAESOC Regarding Your Facility's Security Requirements – Have a question or concern? Check out the website for Self-Help Resources and for the many ways you can contact us to help address issues you may have.

Scheduling a Presentation – NAESOC has a "Best Practices for NAESOC FSOs" presentation it can provide for your Industrial Security Awareness Councils or National Classification Management Society meetings. Download and submit a request for this training.

NISP AUTHORIZATION OFFICE (NAO)

ENTERPRISE WIDE AREA NETWORK (eWAN) PROGRAM PAUSE

NAO announces that the National Industrial Security Program (NISP) eWAN Program has paused on accepting new Industry participants to work towards enhancing existing program requirements. NAO has struggled to sustain and strengthen the Program due to its unexpected growth and popularity. Over the past 6 months, NAO has started shifting eWAN operations to DCSA regional operations and field offices for assessment and continuous monitoring actions. Updates to the DCSA Assessment and Authorization Process Manual and eWAN Program Job Aid are anticipated in 2022 to formally codify realignment and the oversight process.

Additionally, last September, NAO conducted the inaugural NISP eWAN Industry Conference. At this half-day event, Industry participants, representing the largest and most complex information systems in the NISP, shared lessons learned and best practices with one another in an open forum. The NAO and eWAN Program Manager provided insight and recommendations for increasing the security and efficiency for these large classified contractor networks.

Questions and comments regarding the eWAN Program should be addressed to the NAO eWAN Mailbox.

NISS AND NCCS

WE ARE THANKFUL FOR AN UP-TO-DATE FACILITY PROFILE

Please verify that all information on your facility profile in NISS is up to date. Pay special attention to the “Contacts” subcategory under “Facility Overview.” In case of an emergency, a DCSA team member will use this information to contact your facility. This contact information is also used to send important updates to your Key Management Personnel.

Ensure that the FSO, Senior Management Official, and the Insider Threat Program Senior Official have the correct name, phone number, and email listed. In order to update the contact information, you must submit a Facility Profile Update Request.

For more information on how to submit a Facility Profile Update Request, reference the “Facility Profile Update Request – Full Operational Capability (Jun. 2021) User Guide,” in the NISS Knowledge Base.

NCCS IMPLEMENTATION

The NISP Contract Classification System (NCCS) 2.0 development is underway and is scheduled to be released in the third quarter of FY22. Updated schedules and implementation planning materials will be provided during NCCS Operational Requirements Committee meetings.

Reminders: During the system transition, please email DD Form 254(s) 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 CTP Field Locations.

VETTING RISK OPERATIONS (VRO)

PERSONNEL SECURITY INVESTIGATION FOR INDUSTRY BUDGET

Industry should disregard any messages received about limitations to the FY22 Personnel Security Investigation for Industry (PSI-I) budget. DCSA is not experiencing any issues with the PSI-I budget. FSOs should continue to submit PSI requests to VRO for processing.

INVESTIGATION SUBMISSIONS TO INDUSTRY SON/SOI IDENTIFIERS

The Submitting Office Number (SON) is required to process investigative requests. The SON is a unique four-character alphanumeric code assigned by DCSA to each office that requests an investigation from DCSA. The SON identifies which office initiated the investigation and is recorded in the appropriate Agency Use Block (AUB) of the Standard Form.

The Security Office Identifier (SOI) is also required for all investigative requests. Each security office is issued a unique alphanumeric four-character identifier by DCSA to identify the appropriate agency official who will receive case results, data, or other information from DCSA.

For Industry, the required SON is 346W and the correct SOI is DD03, which pre-populate in DISS when an investigation request is initiated. In order for investigation requests to be processed accurately and in a timely manner, FSOs should ensure the correct SON and SOI are used prior to submitting the investigation request to VRO for processing.

RETENTION OF COMPLETED SF-86 FORM

The 32 CFR Part 117 NISPOM Rule no longer has the requirement to retain completed SF-86 forms (Questionnaires for National Security Positions). Users can access a copy of the SF-86 in JVS by viewing the Subject Details screen and selecting the CSR/RFA tab. Subjects have the option to save an archival copy of the SF-86 prior to submitting the request to the FSO. If you have additional questions, contact the VRO at the Ask VRO Mailbox.

SF-312 FORM, CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

When the System of Record (SOR) reflects a fully executed SF-312 form, or an NDA/NDS date is in the SOR, there is no requirement to initiate and submit an updated SF-312, as the SF-312 is a lifetime binding agreement between the individual and the U.S. Government. If you have additional questions, email the VRO at the Ask VRO Mailbox.

BREAK-IN-ACCESS

If an individual was previously enrolled in CV and their CV enrollment history displays "deferred investigation," 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 eligibilities do not expire, but it is necessary for the FSO to maintain cognizance of their subject’s eligibility and access statuses. Ultimately, an FSO can grant the access in DISS if the subject has an active eligibility.

BREAK-IN-SERVICE

A break-in-service occurs when a cleared contractor terminates the employment of an employee with eligibility for access to classified information regardless of the reason for the termination. Upon termination, the employee is debriefed from access and separated. As we move toward full implementation of Trusted Workforce 1.25 reform efforts, additional procedural changes will likely occur.

As it stands, FSOs are required to submit an initial investigation request if there is no eligibility on the subject's record in DISS. VRO will conduct an interim eligibility determination and release for an initial investigation.

If the subject has current eligibility and is not enrolled in Continuous Vetting (CV), an updated SF-86 must be submitted to the VRO. VRO will review the SF-86 using a risk-based approach for deferment into CV or release for investigation.

PRIME CONTRACT NUMBER REQUIREMENT

When submitting requests for 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 Request 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.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NOVEMBER 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 November newsletter focused on Critical Infrastructure Security and Resilience. Check out all the newsletters in CDSE's Electronic Library, 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

The CDSE website has recently migrated to a new platform and is working to resolve some issues users are experiencing when accessing the site. These may be resolved by entering in the full site URL, https://www.cdse.edu, in your browser, but some of the issues may be related to site certificates. Additional updates to follow.

2021 INSIDER THREAT VIRTUAL CONFERENCE PRESENTATIONS

The 2021 Insider Threat Virtual Security Conference was held on September 2, 2021. The conference was open to security professionals in Government and Industry and was jointly hosted by DCSA and the Office of the Under Secretary of Defense for Intelligence and Security. The event brought together security professionals and policy makers from across the U.S. Government and Industry to kick off the National Insider Threat Awareness Month campaign. The theme for this year's conference and campaign was "Workplace Culture and Insider Threat." If you missed the conference or would like to revisit the presentations, the recordings are now available in our Webinar Archive under Insider Threat.

NEW CASE STUDIES

CDSE added new Case Studies to the Case Study Library:

- Izaak Kemp – A case study of an insider's mishandling classified information
- Randall Hughes – A case study of an insider's kinetic violence
- Richard Liriano – A case study of an insider's hacking

Visit our Case Study Library to view all our products.

REGISTRATION NOW OPEN FOR THE GETTING STARTED SEMINAR

The next Getting Started Seminar for FSOs is scheduled to start February 8, 2022! This virtual course is not only a great way to get started as a new FSO, but also a way for experienced FSOs to stay informed about policy changes, procedural changes, emerging trends, threats, concerns, etc. Students work in collaboration with other security professionals, exploring security topics through practical exercises. To learn more and register today visit Getting Started Seminar for New Facility Security Officers (FSOs) (IS121.10).

NEW INDUSTRIAL SECURITY TRAINING VIDEOS

CDSE developed two new Industrial Security Videos that focus on maintaining an effective security program and Insider Threat:

- Maintaining an Effective Industrial Security Program – This video discusses how to maintain an effective industrial security program at your facility.
- Insider Threat Overview for FSOs – This video provides a high-level overview of the Insider Threat Program and describes how the FSO is an important part of protecting national security against the Insider Threat.

Visit Industrial Security Training Videos to see CDSE's most recent training videos.

UPDATED INDUSTRIAL SECURITY eLEARNING COURSES AND SHORTS

- Visits and Meetings in the NISP (IS105.16) is an updated interactive Industrial Security eLearning course that covers the rules and procedures for classified visits and meetings for NISP facilities. Course lessons deal with requirements and procedures that must be completed before sending visitors to contractor facilities, hosting classified visits and meetings at contractor facilities, and hosting incoming and outgoing foreign visits and North Atlantic Treaty Organization visits.
- Preparing the DD Form 254 (IS128.16) is an updated Industrial Security eLearning course that provides an overview of the DD Form 254, Contract Security Classification Specification, and assists the user with the form's purpose and preparation in accordance with applicable Federal Acquisition Regulation clauses and DD Form 254 instructions. Strategies for gathering DD 254 required information are also provided.
- You're a new FSO: Now What? is an updated Industrial Security Short that introduces the CDSE FSO Program (minimum of 13 eLearning courses required for all FSOs). This short also provides newly appointed FSOs with a high-level overview of their responsibilities, and guides them to essential resources. Find "You're a new FSO: Now What?" at Industrial Security Shorts.
- Industrial Security for Senior Management is an updated Industrial Security Short that provides senior management at cleared contractor facilities with a basic understanding of the important role they play in the success of their security program. The short takes a brief look at the Facility Security Clearance process, the importance of the FSO position, and the role of the Senior Manager. Find "Industrial Security for Senior Management" at Industrial Security Shorts.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE