DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

December 2021

Dear FSO (sent on behalf of your ISR),

This monthly newsletter contains recent information, policy guidance, and 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

FIELD OPERATIONS

SECURITY REVIEW IMPLEMENTATION UPDATE

Over the past several months, DCSA personnel have successfully rolled out the implementation of an updated security review process. We ask that you continue to visit our DCSA Security Review and Rating Process page on the DCSA website, located at: https://www.dcsa.mil/mc/ctp/srrp/. This page provides an overview of the process, access to resources to better understand and apply the process, as well as links to recent security review briefings. This page will continue to be updated as additional resources are created and webinars are conducted.

The last several years have been a period of many challenges and changes for everyone, but especially so for DCSA and our NISP partners. We look forward to working with you to raise standards for success as we begin a new year. We also want to thank everyone in Industry for their patience and support in creating and fielding an updated security review and rating process.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC: UPDATES, LINKS, AND MORE – CHECK OUT OUR WEB PAGE

Your one-stop-shop for NAESOC Facility Oversite and requirements is the NAESOC Web Page. Below are updates you will find in January:

FAQ Tab – Check out the latest resources to help you as a New FSO. Read about the "Getting Started Seminar" and CDSE's Security Short for new FSOs. Also, you will find links to data to assist with your management of your DISS account, as well as a downloadable Critical Nuclear Weapons Design Information (CNWDI) briefing.

NAESOC Latest Tab – Ready to be ready? Help make sure your company's oversight requirements are being met more accurately and efficiently by ensuring your profile is up-to-date. Find out more here.

Reporting and Insider Threat Tabs – Be sure to review and make sure you are familiar with the processes and actions here before you need them. Forewarned is Forearmed.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NEW YEAR, NEW DD254s

Start the New Year off right by ensuring all active DD254s are uploaded to your facility NISS profile. To do so, navigate to your NISS facility profile then click on "Business Information." From the dropdown menu select "Customers and Programs." Review all listed contracts, be sure to remove any expired contracts, and upload any missing active contracts. Doing so will prepare you for any future engagements with DCSA.

NOTE: To delete a contract, click the "delete" link from the actions column by the contract you want to delete. To upload a contract, click the "+ Add New Program" link on the top right side of the center screen.

The NISS team would like to wish you and your loved ones a safe and happy holiday season!

NISP AUTHORIZATION OFFICE (NAO)

COMMON CONTROL PROVIDER SYSTEM SECURITY PLAN SUBMISSION

Within the Risk Management Framework (RMF), inheritable controls are referred to as "common controls," while organizations offering up common controls for inheritance are called Common Control Providers (CCPs). This arrangement is unique in the National Industrial Security Program (NISP) as cleared companies and facilities are restricted to inheriting controls only within their company structure not across a broader enterprise.

The Common Control Provider System Security Plan

A CCP System Security Plan (SSP) enables cleared industry to document their common controls, ensure consistency, and streamline the assessment and authorization process. The CCP plan identifies the common controls and all associated procedures and artifacts. The requirements for the CCP plan are the same as other SSPs. A CCP plan must be complete, including a digitally signed document detailing the Commercial and Government Entity (CAGE) Codes and locations of the facilities authorized to inherit from the CCP, before an authorization decision can be made. The plan is required to address System Details, Control Information (Implementation Plan, System Level Continuous Monitoring (SLCM)), Test Results (Control Correlation Identifiers (CCI)/Assessment Procedures (AP)), and include all supporting artifacts.

How Many Security Controls to Include?

A well-crafted CCP plan should include only the security controls that provide the required protection fully or in a hybrid fashion and not include all 388 security controls of the DCSA Moderate-Low-Low (M-L-L) Baseline. For a security control to be considered "common," the entire implementation of the security control is provided by the CCP. The systems inheriting the common control do not need to implement any system-specific infrastructure protections. If additional system-specific infrastructure protections are required, the security control is hybrid. System specific security controls should NOT be included in the CCP plan. Security controls not addressed in the CCP plan, should be marked as Not Applicable.

How to Get Started?

Guidance for cleared industry is located in the DCSA Assessment and Authorization Process Manual (DAAPM), the NISP Enterprise Mission Assurance Support Service (eMASS) Industry Operation Guide, and Section 13.0 of the DISA RMF Functionality Guide. To repeat, a complete CCP SSP should be submitted to ensure the best path to an authorization decision. CCPs are responsible for the development, implementation, assessment, and monitoring of common controls (e.g., security controls inherited by systems). Since CCPs are responsible for the inheritable security controls, it is imperative that the test results in the CCP plan fully address the CCIs. The test results must show how/why the security control is compliant. Addition, policy documents and/or procedures used to support test results must be referenced (e.g., page number, section, and paragraph) and associated with the security control.

Final Steps

Once the CCP plan is developed, cleared industry must submit the CCP plan and request authorization to allow systems to inherit the common controls. The security controls cannot be inherited on any authorized system until authorization is granted by the Authorizing Official (AO). If a system with an inherited control is found to be Non-Compliant, it will impact the CCP plan as well as ALL systems inheriting the security control.

The CCP plan will require reauthorization when security controls are modified or added. Using NISP eMASS, companies and facilities should select the applicable DCSA Field Office Group for the Security Control Assessor (SCA) and Team Lead (TL) roles and the Region Group for the AO. The CCP plan will be assessed by the DCSA Field Office assigned to the CCP's CAGE Code.

CCP plans should be submitted to NAO only when meeting ALL of the following criteria:

1. The submitted security controls are all fully inheritable (i.e., common);
2. An on-site assessment is not required at the providing and receiving system(s) sites to complete the assessment of the CCP plan submission; and
3. The CCP plan covers all DCSA Regions.

Guidance on CCPs, security control designations, submission requirements, and navigating NISP eMASS can be found here:

- NISP eMASS Industry Operation Guide
- DCSA Assessment and Authorization Process Manual (DAAPM)
- DISA RMF Functionality Guide (Located on the NISP eMASS [Help] page)

Contact your assigned Information System Security Professional (ISSP) for additional information.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS)

The DISS Training team would like to make you aware of the following DISS resources and training materials that were recently created or updated.

DISS resources and training are now accessible from the DCSA DISS Page. From there, we encourage you to explore and use supporting materials located under:

- DISS Resources
- DISS FAQs
- DISS Webinars

DISS now has 12 E-Learning Modules that can be accessed through the DISS Resources tab on the DCSA DISS Page. The modules provide step-by-step processes for variety of functions. The 12 modules include:

- **Welcome to DISS:** An introduction while providing the main components of the DISS framework.
- **Getting Started and Account Access:** Learn about the system requirements, user role determination, and how to set up an account.
- **Navigation:** Understand how to navigate the control panel features within the Joint Verification System (JVS).
- **Subject Management:** Learn the detailed process of how to search, create, and maintain a subject's record.
- **Clearance Eligibility and Granting Access:** Learn how to identify a subject's eligibility and determine how and when to grant access.
- **Investigation Request:** Master how to submit and manage investigation requests.

- **Suitability Determination and Homeland Security Presidential Directive 12 (HSPD12) for Non-Sensitive Positions:** Understand how to define suitability and HSPD-12, describe the three tiers of investigations required for non-sensitive positions, and follow suitability determination procedures.
- **Visit Requests:** Learn how to create, change, send, receive, and accept visit requests.
- **JVS System Reports:** Be able to describe the distinct types of JVS reports and explain how to generate and read reports.
- **Incident Management:** Learn how to receive and submit Incident Reports (IRs) along with how and when to send documentation to the adjudicative facility.
- **Removing SMO Relationships and Debriefing Access:** Learn the process of debriefing and suspending access.
- **Customer Service Requests (CSR):** Gain a better understanding of the numerous CSR options and CSR submission processes, as well as the appropriate steps for troubleshooting.

Additionally, there are plenty of training aids on the DCSA website that dive deeper into specific topics. These job aids are located under the "DISS Resources → Training Aids" page, and include the topics:

- JVS Access
- JVS Initial Login
- Adding JVS to Firefox/Chrome
- DISS Troubleshooting Guide
- JVS Agency PSSAR Read Only Access
- JVS Create PCAP User
- Verification by SSN
- Consolidating SMOs

We also encourage you to stay up to date with all the new content updates by following DCSA on Twitter and Facebook.

If you have any questions, please reach out to the DISS training team at dcsa.quantico.nbis.mbx.training@mail.mil.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

ADJUDICATIONS INCIDENT REPORT GUIDE FOR SECURITY MANAGERS

In an effort to ensure the security of classified information or technology, security managers and FSOs are required to report any adverse information that comes to their attention concerning a cleared employee. Adverse information consists of any information that negatively reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of National Security. In reporting the incidents, it is imperative that security managers and FSOs provide all information that is available so that DoD CAF is able to make a well-informed decision.

Provide the Five W's

Security managers and FSOs can create, submit, and update IRs in DISS on cleared personnel reporting events that may affect the individual's eligibility to access classified information. When creating a new incident, be as thorough as possible in the Incident Notes, and, at a minimum, provide the five W's (Who, What, When, Where, and Why). The five W's help explain the 'Who was involved,' 'What happened,' 'When it happened,' 'Where it happened,' and 'Why it happened.' For example, instead of "John Doe was driving under the influence (DUI)," the following is preferred: "Mr. John Doe had a DUI on Friday, October 15, 2021, while driving home from a party; he was arrested by the Localville Police Department and released with a court date not yet determined. Local access was not suspended."

Provide Supporting Documentation

When providing reportable information, submit all available supporting documentation. For example, if the individual had a security violation, provide letters to the individual from security and the commander or director, etc., as well as any related training completed (both before and after the incident). If the subject tested positive for an illegal drug, provide test results, letters to the individual from security and the commander or director, etc., and results of any investigation conducted. Security managers and FSOs play an important role in providing information and supporting documentation that assists adjudicators in making timely adjudicative decisions.

Valid and Responsive Points of Contact (POCs)

Communication is vital to the personnel security vetting process. Security managers and FSOs are the keystone to its success and play a critical role in communicating with DCSA, as they interact with cleared individuals on a frequent basis. All of these steps are important.

Finally, when submitting IRs or CSRs, it can't be overstated how important it is that a valid and responsive POC be provided for DoD CAF communication regarding submissions. While it is good that general POCs are identified in DISS, identifying yourself and how we may contact you about your request/submission (such as phone number and email address) can often help expedite the processing of the request/ submission. With valid and responsive POC information, DoD CAF can call or email for additional information if needed. Providing appropriate details with supporting information and specific POCs is very important and enhances the ability to provide a timely decision.

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. 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.

VETTING RISK OPERATIONS (VRO)

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-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.

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.

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 Requests 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)

DECEMBER 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 December newsletter focused on Security Awareness. 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!

REGISTER NOW FOR UPCOMING WEBINARS

CDSE invites you to participate in all our upcoming Speaker Series:

- SPēD Certification Program Overview
  Friday, January 21, 2022
  1:00 – 2:00 p.m. ET
- Classification of Information Released to the Public
  Wednesday, February 23, 2022
  1:00 – 2:00 p.m. ET
- Mental Health and Your Security Clearance Eligibility
  Thursday, January 20, 2022
  1:00 – 2:30 p.m. ET

Visit CDSE Webinars to sign up for all three events and join the discussion!

REGISTER NEW SAP COURSE NOW AVAILABLE

CDSE retired the Special Access Program (SAP) Nominations Process short and has launched the new Special Access Program Personnel Security Official (SPO) eLearning course. The course provides DoD military, civilian, and contractors who perform the duties of a SPO with the knowledge required to engage in the SAP Nomination process as outlined in DODM 5205.07 Volume 2, Personnel Security. To learn more information and register for the course, visit SPO Training.

For additional information on SAP Nominations in general, please check out our job aids Special Access Programs Job Aids

NEW SHORTS AVAILABLE

CDSE recently released the following three Shorts:

- Protecting Microelectronics (New)
- Counterintelligence Concerns for Adjudicators (Updated)
- Academic Solicitation (New)

Visit Counterintelligence Shorts to view the new and updated products.

NEW INSIDER THREAT VIGILANCE CAMPAIGN

The 2022 Insider Threat Vigilance Campaign job aid is now available. A vigilance campaign helps implement Insider Threat Awareness training. Vigilance campaigns are loaded with awareness resources to share within an organization. Use this new tool to jump-start your annual campaign. Access the job aid here.

CDSE.EDU – A FIX IS ON THE WAY

When the cdse.edu website migrated to a new platform in September 2021, some users experienced certificate errors trying to reach the site. After investigating this issue, the root cause appears to be related to a web content filter put in place to protect DoD users from inappropriate or unsafe content.

CDSE is working with numerous entities to remedy this issue and hope to have it fixed soon. In the meantime, https:\\www.cdse.edu is accessible from your personal computer or non-DOD system.

Stay tuned to the CDSE Pulse and other CDSE communications for updates.

SAVE THE DATE – 2022 VIRTUAL SECURITY CONFERENCE FOR INDUSTRY

Mark your calendars for the 2022 Virtual DCSA Security Conference for Industry on February 16, 2022! This year's conference theme is "Inform & Transform: Enhancing the Security Landscape." The conference is open to cleared industry under the NISP. Stay tuned for more details.

NEW CASE STUDIES

CDSE added new Case Studies to the case study library:

- Mostafa Ahmed – A case study of an insider's attempted espionage
- John Beliveau – A case study of an insider leaking information

Visit our Case Study Library to view our 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).

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE