DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

# VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

**June 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

# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

DCSA continues to finalize its plan to manage CUI responsibilities, with details expected to be communicated to Industry this summer. At this time, DCSA is not conducting any oversight of CUI associated with classified contracts or cleared contractors.

DCSA has fielded several CUI-related questions in recent months and is currently developing a Frequently Asked Questions (FAQ) resource for Industry to be posted within the next 60 days. One common question concerns CUI training, and this message intends to provide clarity on that topic.

## WHAT TRAINING IS REQUIRED FOR INDUSTRY?

- Training is required when requested by the Government Contracting Activity (GCA) for contracts with CUI requirements. Any questions regarding training should be directed to your GCA.
- Per CUI Notice 2016-01: Implementation Guidance for the Controlled Unclassified Information Program (September 14, 2016), at a minimum, training must:
  - Convey individual responsibilities related to protecting CUI
  - Identify the categories or subcategories routinely handled by agency personnel and any special handling requirements (i.e., for CUI Specified)
  - Describe the CUI Registry, its purpose, structure, and location (i.e., http://www.archives.gov/cui/)
  - Describe the differences between CUI Basic and CUI Specified
  - Identify the offices or organizations with oversight responsibility for the CUI Program
  - Address CUI marking requirements, as described by agency policy
  - Address the required physical safeguards and methods for protecting CUI, as described by agency policy
  - Address the destruction requirements and methods, as described by agency policy
  - Address the incident reporting procedures, as described by agency policy
  - Address the methods and practices for properly sharing or disseminating CUI within the agency and with external entities inside and outside the Executive branch; and
  - Address the methods and practices for properly decontrolling CUI, as described by agency policy.
- Industry organizations may develop their own CUI training, so long as the training includes these eleven requirements.

## ARE THERE CUI COURSES CREATED FOR INDUSTRY?

- Yes, the Center for Development of Security Excellence (CDSE) has developed an eLearning course titled “DoD Controlled Unclassified Information (CUI) Training for Contractors” (IF141.06.FY21.CTR).
- The course conveys the 11 training requirements for accessing, marking, safeguarding, decontrolling and destroying CUI, along with procedures for identifying and reporting security incidents.
- The course fulfills CUI training requirements for Industry when required by GCAs for contracts with CUI requirements.
- CDSE also offers a CUI Toolkit with training, policy documents, resources, and a FAQ video.

# 32 CFR PART 117 NISPOM RULE WEBPAGE UPDATE

DCSA Critical Technology Protection Policy has updated the webpage for 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM) Rule with Key Changes, FAQs, and Resources, including a new series of recordings on the Rule and a list of upcoming events. Please check The NISPOM Rule Webpage often for new updates and additional information on the Rule.

# DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

## ASSISTANCE FOR SUPPLEMENTAL INFORMATION REQUESTS (SIRs)

DoD CAF recently published guidance on responding to Supplemental Information Requests. 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 Acknowledge the Date, and complete. Once you click Complete, the task will move into the 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.

## NEW DOD CAF PRODUCTS NOW AVAILABLE

DoD CAF launched two noteworthy products for your resource library: the Suitability, Fitness, and Credentialing Factsheet, and a one-pager on DCSA Adjudication Services. Each of these documents is easily downloadable so you can share. To locate these informational documents and more, please refer to DoD CAF Resources.

## REMINDER: REINSTATED RESPONSE REQUIREMENTS

DoD CAF is no longer issuing indefinite automatic extensions related to the COVID-19 pandemic non-responses. DoD CAF will send a Request for Action for a single extension related to COVID-19 via DISS. Commands, Security Management Offices, Security Managers, National Industrial Security Program FSOs, and other authorized security professionals will have 30 days from receipt to comply with the official Supplemental Information Request as received before DoD CAF continues the adjudicative decision process.

If the requested action is not completed in the allotted timeframe, the DoD CAF may be unable to continue processing the adjudication until there is compliance with the official request.

Questions regarding DoD CAF requests should be communicated via the DISS Portal or via email to the DoD CAF Customer Call Center.

## DOD CAF CALL CENTER

The DoD CAF Call Center resumed telephone services and can be contacted at 301-833-3850. You may also continue to send your inquiries via email at dcsa.meade.caf.mbx.call-center@mail.mil. We look forward to hearing from you.

# DISS WEBINARS PAGE

A new DISS Webinars page has been created, where you can find all things webinar-related for the DISS Joint Verification System including upcoming training, training materials, and Q&As.

The one-hour webinar sessions are geared toward industry users and will focus on high-level user functions such as Subject Management, NDA Submission Process, Access Management, Visit Requests, and Investigation Requests. A Q&A session will be included at the end of each session. Please note: no pre-registration is required but attendance will be capped at 250 attendees.

The next session is scheduled for July 1 at from 4:00 pm - 5:00 p.m. ET. Click on the DCS Link to attend.

Please refer to the rolling schedule of Industry webinars at DSS Webinars for future dates and times.

To join via phone, dial 410-874-6300 or DSN: 312-874-6300 and use the PIN: 974 650 249. To follow along, the Industry slides are posted on the DISS Resources page (select the DISS Webinars button.)

# NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC provided Help Desk support during the National Classification Management Society (NCMS) 57th Annual Virtual Training Seminar in June. Thank you to all the NAESOC facilities that participated and offered us the opportunity to address your issues.

NAESOC will continue processing the new batch of over a thousand additional facilities to our ranks through early July. Be sure to look for the "Welcome" email and reach out to us for any questions you may have.

We look forward to opportunities to meet with or offer presentations at your local industry events. Please contact us using the form found here to schedule your event.

The NAESOC Web Page has been significantly updated to address your needs:

Frequently Asked Questions (Check Here First) – webinars, handouts, and FAQs for your use

Insider Threat – new and updated resources and links added to assist in developing and supporting your Insider Threat Program

NAESOC Latest – Links and feedback highlighting how the NAESOC resources can be used for your individual security programs

Reporting (New Tab) – Changed Condition reporting guidelines; and how to process Security Violations and Administrative Inquiries

NISS Tips – Links, resources, and Best Practices for Common NISS Questions.

# NISP AUTHORIZATION OFFICE (NAO)

## COMMON CONTROL PROVIDER SYSTEM SECURITY PLAN SUBMISSIONS

Within the Risk Management Framework (RMF), inheritable controls are referred to as "common controls," and organizations offering up common controls for inheritance are called Common Control Providers (CCPs). This arrangement is unique in the 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, and, just like other SSPs, they must be complete and include 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 given. The CCP SSP is required to address System Details, Control Information (Implementation Plan, System Level Continuous Monitoring), Test Results (Control Correlation Identifiers (CCI)/Assessment Procedures), and include all supporting artifacts.

How Many Security Controls to Include?

A well-crafted CCP plan should include only the security controls that provide 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. In 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 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 and ALL systems inheriting the control.

The CCP plan will require reauthorization when security controls are modified or added. Using the 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 the 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.

# NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

## NEW NISS FEATURES COMING SOON!

The NISS team is working hard to bring some exciting new features to NISS this fall. The enhancements will provide the user base with a more streamlined, modern, and efficient system. A few key features include:

- A new look and feel, with simplified access to key functions
- More interactive and dynamic layouts, menus, and buttons
- Performance improvements with shorter "time-on-task" due to faster loading and processing times
- New features, including a "Bookmarks" tab
- A Streamlined Sponsorship Submission Package process.

The team is also working on enhancements to the in-system messaging feature, which will be upgraded in the near future. These enhancements will focus on improving usability and enhancing the ability to search and manage message content within the system. Please submit suggestions and ideas on this feature or any other functionality to the Industry Requirements mailbox.

Reminder: For any technical questions with NISS, please contact the DCSA Knowledge Center at 888-282-7682 and select Option 2, then Option 2. The DCSA Knowledge Center hours of operation are Monday through Friday from 8:00 a.m. to 6:00 p.m. ET.

# VETTING RISK OPERATIONS CENTER (VROC)

## 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 until further notice. We will continue to provide status updates via DISS Customer Service Request and VROC email.

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

- Industry PIN Resets, e-QIP PIN Resets, and 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 (TW) 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. VROC 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.

# CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

## JUNE 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 June newsletter focused on Controlled Unclassified Information. Check out all the newsletters in the CDSE 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 webinars:

- NATO Control Point
  Thursday, July 8, 2021
  1:00 – 2:00 p.m. ET
- Overview of Personnel Vetting Methodology
  Wednesday, July 21, 2021
  12:00 – 1:00 p.m. ET
- The Modernized Self-Inspection Handbook
  Thursday, July 22, 2021
  1:00 – 2:00 p.m. ET
- Organizational Culture and Countering Insider Threats: Best Practice Examples from the U.S. Marine Corps
  Thursday, July 29, 2021
  12:00 – 1:00 p.m. ET
- Overview of the National Background Investigation Services (NBIS)
  Thursday, August 26, 2021
  12:00 – 1:00 p.m. ET

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

## NEW CDSE CASE STUDY

CDSE Insider Threat recently released a new case study:

- Jean Patrice Delia and Miguel Sernas. This theft of trade secrets case study outlines Delia and Serna's crimes, Serna's sentence (Delia's sentence is pending), the impact, and the potential risk indicators that, if identified, could have mitigated harm.

All of CDSE's case studies can easily be included in an organization's security education, training, and awareness programs. They are suitable for printing or easy placement in a company or command newsletter, email, or training bulletin. Access our Newest Case Study today!

## 2021 INSIDER THREAT VIRTUAL CONFERENCE

Save the date for the upcoming Insider Threat Virtual Conference:

September 2, 2021
10:00 a.m. - 3:00 p.m. ET
Open to security professionals in Government and Industry.

The 2021 Insider Threat Virtual Conference, hosted jointly by DCSA and the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S), will bring together security professionals and policy makers from across the U.S. Government and Industry to kick off the National Insider Threat Awareness Month (NITAM) campaign. The theme for this year's conference and campaign is Cultural Awareness and Insider Threat.

Registration opens August 2.

## NITAM CULTURAL AWARENESS VIDEO COMPETITION

DCSA and its partners in the Counter-Insider Threat community would like to hear about your organization's daily actions to create a positive workplace culture. To participate, create an original video clip (between 30 - 45 seconds long) relevant to Cultural Awareness or any of the sub-themes: Toxic Workplaces, Leadership and Top-Down Culture, Microaggressions in the Workplace, and Work-Life Stressors. Competition winners will receive recognition during the Annual Virtual Insider Threat Conference. The submission deadline is July 31, 2021, at 11:59 p.m. ET. Learn more about the competition at NITAM Cultural Awareness Video Competition!

# SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE