DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

October 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

32 CFR SELF-INSPECTION HANDBOOK UPDATE

DCSA has updated the Self-Inspection Handbook for National Industrial Security Program (NISP) Contractors to address user reports of technical issues. If you have previously downloaded the Self-Inspection Handbook and run into any problems, please download the file again, save it to your local system, and verify you have the most recent version by ensuring the footer of the title page includes "v4."

The new Self-Inspection Handbook can be found in NISS on the Knowledge Base and posted to the dashboard, and is also available on the Resources tab on DCSA's Critical Technology Protection 32 CFR Part 117 NISPOM Rule page as well as on the Self-Inspections page of the Center for Development of Security Excellence (CDSE) FSO Toolkit.

Please direct any questions regarding the Self-Inspection Handbook to the new Self-Inspection Handbook Support Mailbox.

DCSA CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI IMPLEMENTATION PHASE 1 PRODUCTS

The DCSA CUI Program Office has developed and released the following three products for Industry use:

- CUI Frequently Asked Questions – This document provides answers to the questions most frequently asked during Industry engagements related to CUI.
- CUI Quick Start Guide for Industry – This guide provides basic facts for Industry, answers frequently asked questions, and provides sources for more detailed information and tools on safeguarding CUI.
- CUI Marking Job Aid – This job aid provides different methods for marking CUI. It contains information on marking methods for storing CUI, systems marking and identifying CUI in databases, shipping and mailing CUI marking, as well as instructions for mandatory CUI banner markings, portion marking, and CUI marking in spreadsheets, forms and emails.

These three products are posted on the DCSA CUI Webpage.

Several other resources are under development with releases to follow before the end of the calendar year:

- CUI Glossary
- CUI Baseline Requirements
- Self-Inspection Appendix for CUI
- Sample CUI Standard Practice and Procedure Template
- Compliance and Information Systems Controls Cheat-Sheets
- Training and Resource Job Aid

CUI resources are offered to support Industry's development, management, and sustainment of CUI programs resident at their locations. As resources are finalized and approved for release, they will continue to be posted on the DCSA CUI Webpage. Government and Industry partners are strongly encouraged to bookmark that page and visit it frequently.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

REPORTING MENTAL HEALTH ISSUES ON YOUR E-QIP

Contrary to a common myth, reporting mental health issues on Section 21 of the SF-86 is not a "career-killer." In fact, a DCSA CAF analysis of denial and revocation statistics shows that only a fraction of one percent of adjudicative actions are denials or revocations solely based on psychological conditions.

There are at least two main reasons for this. Section 21 now has a greater focus on potential security-relevant concerns such as findings of mental incompetence, court-ordered care, psychiatric inpatient care, and certain conditions that may indicate judgment or reliability issues. Second, security professionals understand that when individuals candidly report their conditions and seek mental health care in accordance with their practitioner's recommendations, psychological conditions are not security concerns in the vast majority of cases.

That said, curiosity about how adjudicators resolve affirmative answers to Section 21 is understandable and the following offers some insight:

- After obtaining consent, a Background Investigator will conduct a brief interview with the applicant's treating health care practitioner focusing on whether the applicant's condition may impact his/her ability to perform sensitive national security duties.
- Depending upon the nature of the symptoms, more details may be obtained regarding treatment and prognosis.
- Psychologists that work with adjudicative teams may also request a review of pertinent medical records.
- If security concerns remain after these inquiries, the security professional may ask for the applicant to participate in an evaluation with a psychologist or psychiatrist who will consider possible security risks associated with the condition. Keep in mind that these security evaluations are quite rare. For NISP contractors, usually fewer than 300 evaluations a year are requested, and a majority of those determine the applicant's psychological condition does not present security concerns.

For more information please contact the DoD CAF Call Center at dcsa.meade.caf.mbx.call-center@mail.mil.

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)

HOW TO NAVIGATE NISS V2.6 LIKE A PRO

In order to get the full functionality of NISS Version 2.6, please use Microsoft Edge or Mozilla Firefox to access the system. NISS v2.6 is NOT compatible with Internet Explorer, Google Chrome, or any other browser. Using non-compatible browsers will result in error messages and loss of functionality.

NISS V2.6 eLEARNING VIDEOS

- Having issues using NISS v2.6?
- Curious about all the updates?
- Not sure how to navigate through a sponsorship submission?
- There's an eLearning Video for that!

You will find four new eLearning videos In the NISS Knowledge Base under the "Training Videos" tab. The new eLearning videos are:

- Using and Navigating NISS – External
- Using and Navigating NISS – GCA
- Navigating a Sponsorship Submission
- Overview of the Facility Clearance Verification (FCV) Process

Note: eLearning Videos are uploaded as a zip file. Scroll to the bottom of the instructions to learn how to view the eLearning videos and to access the zip file.

More eLearning videos are coming soon!

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. Below are updates you will find on the NAESOC Web Page this month:

NAESOC Latest Tab – You can 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.

Insider Threat Tab – What's fresh this month? New resources, including a link to the recording of the 2021 Insider Threat Virtual Conference and "Organizational Culture and Countering Insider Threat" developed by the USMC Insider Threat Program.

Reporting Tab – Along with key information on reporting Cyber Intrusions, Facility Security Clearance Changed Conditions, updating your Facility Profile, and the latest on NISS, this month you'll find a new tri-fold addressing Threat Awareness in Academia.

FAQ Tab – Questions about Controlled Unclassified Information and your requirements? You'll find a FAQ for that here.

VETTING RISK OPERATIONS (VRO)

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 towards full implementation of Trusted Workforce (TW) 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 the Defense Information System for Security (DISS). Vetting Risk Operations (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 the 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.

PERSONNEL SECURITY INVESTIGATION FOR INDUSTRY BUDGET

Industry should disregard any memorandums received from 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 Customer Service 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)

OCTOBER 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 October newsletter focused on Cybersecurity 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!

CDSE WEBSITE MIGRATION

The CDSE website has recently migrated to a new server 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.

NEW CASE STUDIES

CDSE added five new Case Studies to the case study library:

- Glen Omar Viau – A case of an insider's unauthorized use of Government property and falsifying facts
- Wei Sun – A case of an insider's export violations
- Azzam Mohamed Rahim – A case study of an insider's attempt to provide material support to a foreign terrorist organization
- William Jarret Smith – A case study of an insider aiding a terrorist group
- Jesus Encarnacion – A case study of an insider aiding a terrorist group

Visit our case study library to view our all of our products.

NEW CYBERSECURITY WEBINAR

CDSE recently released a Cybersecurity webcast titled "Cybersecurity and Telework: Concerns, Challenges, and Practical Solutions Part 3 (Collaboration Tools)." Access the new webcast from our webinar archive under Cybersecurity.

NEW CYBERSECURITY COURSE

CDSE has a new instructor-led cybersecurity course, "Assessing Risk and Applying Security Controls to NISP Systems CS301." This course provides students with guidance on applying policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the Risk Management Framework (RMF) process. It also provides a comprehensive understanding of contractor requirements under the NISP. Learn more about the course and register by visiting the course page.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE