DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

August 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

THE NISPOM RULE IS IN EFFECT! 2
32 CFR SELF-INSPECTION HANDBOOK UPDATE 2
DCSA CUI IMPLEMENTATION 2
BACKGROUND 2
IMPLEMENTATION UPDATE 3
WHAT YOU NEED TO KNOW ABOUT PHASE 1 (FY22) 3
FOR MORE INFORMATION 3
DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF) 4
NEW DOD CAF PRODUCTS NOW AVAILABLE 4
ADJUDICATIONS INFORMATION AND RESOURCES 4
DOD CAF CALL CENTER 4
NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC) 4
NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) 5
NISS VERSION 2.6 RELEASE 5
VETTING RISK OPERATIONS (VRO) 5
VROC NAME CHANGE 5
PERSONNEL SECURITY INVESTIGATION FOR INDUSTRY BUDGET 5
PRIME CONTRACT NUMBER REQUIREMENT 5
PCL KNOWLEDGE CENTER INQUIRIES 5
APPLICANT KNOWLEDGE CENTER GUIDANCE 6
BREAK-IN-SERVICE 6
CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) 6
AUGUST PULSE: CDSE SECURITY AWARENESS NEWSLETTER 6
CDSE WEBSITE MIGRATION 6
NITAM 2021 WEBSITE NOW AVAILABLE 6
2021 INSIDER THREAT VIRTUAL CONFERENCE 7
PERSEREC COUNTER-INSIDER THREAT SUMMIT 7
SOCIAL MEDIA 7

THE NISPOM RULE IS IN EFFECT!

On February 24, 2021, Title 32 of the Code of Federal Regulations (CFR) Part 117, "National Industrial Security Program Operating Manual (NISPOM)," became effective as a federal rule. Referred to as "the NISPOM Rule," it replaces the NISPOM previously issued as a DoD policy (DoD 5220.22-M), which will be cancelled shortly. This action codified NISP cognizance under the DoD, and NISP oversight under DCSA.

When the NISPOM Rule became effective, it provided contractors with a 6-month window to comply with the requirements, making August 24, 2021 the effective date for compliance by NISP contractors.

On August 19, The NISPOM Rule was amended. This amendment only applies to those NISP contractors under DoD security cognizance, and extends the compliance solely for the reporting and pre-approval of unofficial foreign travel to no later than 18 months after the Rule became effective (i.e., August 24, 2022).

DCSA posted an Industrial Security Letter (ISL) providing Cognizant Security Agency clarification on SEAD 3 and adverse information reporting for NISP contractors under its oversight. The ISL, as well as NISPOM Rule Key Changes, Resources, and Frequently Asked Questions (FAQs), may be found here.

32 CFR SELF-INSPECTION HANDBOOK UPDATE

DCSA has updated the Self-Inspection Handbook for NISP contractors in accordance with the new 32 CFR Part 117 NISPOM Rule that took effect August 24. This Self-Inspection Handbook is an optional tool that provides checklists to act as starting points to establish and manage an effective self-inspection program tailored to the security needs of your cleared company. Cleared companies are required per NISPOM §117.7(g)(2) to "… review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles."

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 our Outreach Mailbox.

DCSA CUI IMPLEMENTATION

BACKGROUND

On March 6, 2020, DoD Instruction 5200.48, Controlled Unclassified Information (CUI) was released, establishing policy, assigning responsibilities, and prescribing procedures for CUI throughout the DoD in accordance with Executive Order 13556, 32 CFR Part 2002, and Sections 252.204-7008 and 252.204-7012 of the Defense Federal Acquisition Regulation System (DFARS). This instruction directed the Director, DCSA, with eight responsibilities with respect to CUI:

1. Administer the DoD CUI Program for contractually-established CUI requirements for contractors in classified contracts in accordance with the May 17, 2018 Under Secretary of Defense for Intelligence and Security (USD(I&S)) Memorandum.

2. Assess contractor compliance with contractually-established CUI system requirements in DoD classified contracts associated with the NISP in accordance with Part 2003 of Title 32, CFR, and National Institute of Standards and Technology Special Publication 800-171 guidelines.
3. Establish and maintain a process to notify the DoD CIO, USD(R&E), and USD(A&S) of threats related to CUI for further dissemination to DoD Components and contractors in accordance with the Section 252.204-7012 of the DFARS.
4. Provide, in coordination with the USD(I&S), security education, training, and awareness on the required topics identified in Section 2002.30 of Title 32, CFR, including protection and management of CUI, to DoD personnel and contractors through CDSE.
5. Provide security assistance and guidance to the DoD Components on the protection of CUI when DoD Components establish CUI requirements in DoD classified contracts for NISP contractors falling under DCSA security oversight.
6. Serve as the DoD lead to report Unauthorized Disclosures of CUI (except for cyber incidents per DFARS Section 252.204-7012), associated with contractually-established CUI system requirements in DoD classified contracts for NISP contractors falling under DCSA security oversight.
7. Coordinate with the DoD CIO to implement uniform security requirements when the IS or network security controls for unclassified and classified information are included in DoD classified contracts for NISP contractors falling under DCSA security oversight.
8. Consolidate DoD Component input on the oversight of CUI protection requirements in DoD classified contracts for NISP contractors under DCSA security oversight, as required by Information Security Oversight Office (ISOO) Notice 2016-01.

IMPLEMENTATION UPDATE

Over the next several years, DCSA will operationalize its eight CUI responsibilities using a phased approach. DCSA will achieve initial operating capability of its CUI program administration responsibilities on October 1, 2021 and complete Phase 1 of implementation throughout the duration of FY22.

WHAT YOU NEED TO KNOW ABOUT PHASE 1 (FY22)

During Phase 1, DCSA will not assess contractor compliance with contractually-established CUI system requirements in DoD classified contracts associated with the NISP. DCSA will instead focus on preparing and executing program administration activities, which includes developing processes and procedures, engaging with Government and Industry stakeholders, and producing tools, training, and resources to support Industry's development, management, and sustainment of CUI programs within their facilities.

DCSA will also develop unauthorized disclosure and threat notification processes in accordance with two of its eight responsibilities. DCSA's CUI Program Administration Office will incorporate best practices and lessons learned throughout Phase 1 to mature its processes over subsequent phases.

FOR MORE INFORMATION

Next month, DCSA will communicate to Industry and Government stakeholders via this VOI Newsletter, the DCSA CUI webpage, and other venues with further details regarding its phased implementation approach. DCSA is also developing helpful resources for release in October to include a FAQs document and a Quick Start Guide to enable Industry's success in developing a CUI program within their facilities. For more information, please visit the Controlled Unclassified Information page.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

NEW DOD CAF PRODUCTS NOW AVAILABLE

DoD CAF announces the latest products for our Reciprocity Program. The Reciprocity Program one-pager provides a program overview including applicable Director of National Intelligence Security Executive Agent Directive standards. The Reciprocity Guide provides information on how to identify and determine existing Security Clearance or Suitability Eligibility. These informational documents can be easily downloaded and printed at your convenience from DoD CAF Resources.

ADJUDICATIONS INFORMATION AND RESOURCES

Please check out DoD CAF Resources for the latest product updates located on DCSA's website. We offer a robust section of information on adjudications, requesting adjudication records, and FAQs from "What does SCI mean?" to "If I leave the DoD for another Federal agency, will I lose my eligibility, or will it transfer to my new agency?" located on our DoD CAF FAQs page.

DOD CAF CALL CENTER

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

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

There are significant and important updates on the NAESOC Web Page this month:

NAESOC Latest Tab – Check out the latest on the Defense Industrial Base Vulnerability Disclosure Program (DIB-VDP) and the three NAESOC presentations that can be provided for your industry association, then sign up for any one of those here.

Reporting Tab – NAESOC facilities were provided updates to our enhanced counterintelligence support in early August; more can be found here. Also find details on reporting Cyber Intrusions, Facility Clearance Change Conditions, updating your Facility Profile, and the latest on NISS.

Frequently Asked Questions – Links have been added to quickly get a NATO and COMSEC briefing.

Insider Threat Tab – Information about the 2021 Insider Threat Virtual Conference, Common Insider Threat Vulnerabilities, and the Counter-Insider Threat Social and Behavioral Science Summit.

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

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS VERSION 2.6 RELEASE

The NISS team is happy to announce NISS Version 2.6 is scheduled to be deployed on September 27. This deployment includes a more interactive and dynamic user interface, performance improvements, enhanced security controls, and streamlined process workflows. To support the NISS 2.6 release, the system will be taken offline on September 22 at 8 p.m. EDT, and is scheduled to be online again on September 27 at 6 a.m EDT. Release notes, updated job aids, and e-learnings will be provided for your reference. More information on these changes will be provided over the next few weeks.

VETTING RISK OPERATIONS (VRO)

VROC NAME CHANGE

We are pleased to share with you that effective immediately, the Vetting Risk Operations Center (VROC) has changed its name to 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 the Defense Information System for Security (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.

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.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

AUGUST 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 August newsletter focused on Antiterrorism. 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 will be migrating to a new web-hosting platform in mid-September. While our homepage URL (www.cdse.edu) will remain the same, the rest of the website URLs will change. This may impact your "Favorites" or "Bookmarks" pages. We apologize for any inconvenience this causes and thank you for your understanding during this transition.

NITAM 2021 WEBSITE NOW AVAILABLE

Are you ready to #BeTheChange and participate in this year's #NITAM event? Visit our updated National Insider Threat Awareness Month (NITAM) website to access this year's products, case studies, welcome messages, and more.

2021 INSIDER THREAT VIRTUAL CONFERENCE

Register now 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 NITAM campaign. The theme for this year's conference and campaign is Cultural Awareness and Insider Threat.

PERSEREC COUNTER-INSIDER THREAT SUMMIT

The Counter-Insider Threat (C-InT) Social & Behavioral Science (SBS) Summit 2021 is The Threat Lab's contribution to NITAM. This 30-day virtual C-InT SBS Summit is designed to deploy and share knowledge, strengthen relationships across the global C-InT Community of Practice, and integrate research into operations through delivery of relevant artifacts. This year's theme is Cultural Intelligence: why it matters to the counter-insider threat mission space, what it means, and how it can improve our efforts to detect, mitigate, and prevent concerning behavior. Learn more at the C-INT SBS Summit 2021 website.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE