DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

July 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

DCSA SECURITY REVIEW AND RATING PROCESS

During a recent Center for Development of Security Excellence (CDSE) webinar, DCSA Critical Technology Protection (CTP) National Operations announced updates to the security review and rating process. DCSA personnel will begin using these refined processes when conducting security reviews of cleared contractors, starting September 2021.

The refined security review approach incorporates best practices from previous security review models and functions within the DCSA charter to verify compliance with the National Industrial Security Program Operating Manual (NISPOM) while identifying risks posed throughout classified contract performance. DCSA personnel will review internal processes with contractor personnel throughout classified contract deliverable lifecycles to assess NISPOM compliance, determine measures in place to counter potential threats, identify vulnerabilities and administrative findings, and advise the contractor on how to achieve and maintain an effective security program. DCSA will continue to provide a formal security rating at the conclusion of the security review that reflects the contractor’s effectiveness in protecting classified information.

The refined security rating model is a criteria-based system that aligns processes, terms, definitions, and minimum requirements to DoD and National-level policy. The security rating process is a compliance-first model that eliminates the use of enhancements and uses a whole company approach based on a corporate culture of security to include management support, employee awareness, and cooperation within the security community. DCSA will provide the contractor with a final security rating of Superior, Commendable, Satisfactory, Marginal, or Unsatisfactory.

DCSA CTP National Operations will host a webinar in late August to introduce the criteria used during the security rating process. More information to follow.

SMO RESPONSIBILITIES IN THE NISP WEBINAR

Please join DCSA CTP staff on Adobe Connect in a discussion on the responsibilities of the Senior Management Official (SMO) as outlined in 32 CFR Part 117 (NISPOM Rule). The webinar will focus on SMO roles and responsibilities, provide a brief overview of the NISPOM Rule, and the importance of the SMO during annual self-inspections. The webinar is recommended for attendance by Senior Management Officials, Key Management Personnel, Facility Security Officers, and key security staff. The webinar will include a question and answer session at the end.

- Senior Management Official Responsibilities in the National Industrial Security Program
  Tuesday, August 10, 2021
  1:00 to 1:30 p.m. ET

Link will be available on the DCSA website prior to webinar.

DISS WEBINARS WEBSITE

We are happy to share that the DISS Webinars website is available! It is a great resource for all things webinar-related for the Defense Information System for Security (DISS) Joint Verification System including the upcoming training webinar schedule, both the Agency and Industry slide deck presentations, and Q&As from previous webinars. We would also like to thank those who participated in the webinar survey.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

RECIPROCITY PROCESS IMPROVEMENTS

Prior to January 2020, reciprocity determinations timeliness averaged 65 days end-to-end, well above the Director of National Intelligence Security Executive Agent Directive (SEAD) 7 requirement of 5 days. A Lean Six Sigma study, conducted from January 14 to May 30, 2020, examined the reciprocity process end-to-end crossing two DCSA mission areas – Vetting Risk Operations and Adjudications. The study identified opportunities for improvement to eliminate bottlenecks and reduce timelines ultimately to achieve SEAD 7 compliance.

DCSA Adjudications fully implemented the Lean Six Sigma process improvement opportunities in June 2021. We are now consistently meeting SEAD 7 timeliness for end-to-end reciprocity request processing. Specifically, in June 2021, DCSA Adjudications processed concluded reciprocity actions in an average of 2 days end-to-end – a 97% improvement over performance from January 2020.

DOD CAF CALL CENTER

The DCSA Adjudications 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)

We would like to extend a warm welcome to the 1,200 new facilities that joined the NAESOC community in July! Be sure to look for the “Welcome” email and reach out to us for any questions you may have.

In July, the San Diego Chapter of the National Classification Management Society (Chapter 45) hosted the NAESOC for a presentation of its capabilities and resources. 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 updated to provide you with the latest resources:

Frequently Asked Questions (Check Here First) – Check here to find support for incorporating the new Self-Inspection Handbook into your security program

Insider Threat – Information about the 2021 Insider Threat Virtual Conference

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

Reporting – Changed Condition reporting guidelines; how to process Security Violations and Admin Inquiries; and a special handout on Counterintelligence Awareness and Reporting

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

NISP AUTHORIZATION OFFICE (NAO)

REMINDER: FEDERAL INFORMATION SYSTEMS

Federal Information Systems (FISs) are owned and authorized by U.S. Federal Agencies providing the system and are not under the cognizance of DCSA. If a Component or Government Contracting Activity (GCA) needs to locate an FIS at a cleared contractor facility, the GCA must follow the provisions of DoD Manual 5220.22, Volume 2.

The GCA and DCSA personnel will work jointly to explore options and the process for an exception. Cleared contractors do not request exceptions to policy for an FIS or deviate from DoD Manual 5220.22, Volume 2. Should an exception be granted, it is only a temporary measure to get the system to full compliance.

Recently, cleared contractors have been inquiring about requests being made to personnel to take classified FIS assets home due to COVID-19. The use of these assets falls under the direction and security cognizance of the Government customer that provided them, not under DCSA. Questions about their use should be directed to the Government customer.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS VERSION 2.6 RELEASE

NISS Version 2.6 will feature a more interactive and dynamic User Interface (UI). The upgrade will also include application performance improvements, enhanced security controls, and streamlined process workflows. The NISS team began testing the NISS Version 2.6 iteration at the end of July with deployment scheduled for late September. Webinars, training materials, and communications will be sent out before and after deployment.

VETTING RISK OPERATIONS CENTER (VROC)

PERSONNEL SECURITY INVESTIGATION FOR INDUSTRY BUDGET

Industry should disregard any memorandums received by 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 VROC 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 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)

JULY 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 July newsletter focused on Personnel Vetting. 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!

NEW CDSE CASE STUDY

CDSE Insider Threat recently released a new case study:

- Christopher Grupe. This sabotage case study outlines Grupe's crime, sentence, 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!

REGISTER NOW FOR UPCOMING WEBINAR

CDSE invites you to participate in our next webinar:

- 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 this event and join the discussion!

NEW JOB AIDS

CDSE recently released several new job aids:

- Potential Risk in Informal Banking and Finance. This job aid focuses on the cultural practice of informal banking and how participation in the practice may increase an insider's potential risk of becoming an insider threat.
- Insider Risk Implementation Guide for Food and Agriculture. This job aid provides guidance for agriculture facilities and organizations. It supports the development and implementation of insider risk programs with these critical organizations.
- Marking Classified Information. This job aid provides the requirements and methods for marking classified documents and other classified materials.

Access all our new job aids today!

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

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

Registration opens August 2.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE