DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

September 2022

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

INDUSTRIAL SECURITY OPERATIONS UPDATES

OPEN STORAGE APPROVAL CHECKLIST GUIDE

DCSA approves safeguarding under the National Industrial Security Program (NISP) for contracts upon which the DoD maintains security cognizance. The implementation of 32 CFR, Part 117 (the NISPOM Rule), codified requirements for open storage areas and replaced “closed areas” as an entity for protecting classified holdings within Industry.

Open storage areas are approved by DCSA. DCSA Form 147 was created to aid facilities in documenting the characteristics of measures to protect classified information in their open storage areas, and to document DCSA’s approval for the use of those areas.

The form was approved in April 2022 by the Office of Management and Budget (OMB) for use by Industry to collect the information. Upon DCSA approval of the area for use, the form becomes a living record that stays with the area, to be updated for approval by DCSA as changes occur to the area. OMB estimates that this form should take no more than an hour to complete.

The open storage area process is new and does not place additional requirements on Industry, but rather replaces obsolete requirements. This form should be filled out by the FSO for each open storage area in their facility. FSOs for larger safeguarding facilities should develop a plan with their ISR to transition remaining closed areas approved under the old DSS Form 147 to the new DCSA Form 147.

To aid FSOs in completing DCSA Form 147, DCSA has created the Open Storage Approval Checklist Guide, which will be posted shortly to NISP Resources under the "FSO Guides" tab.

SECURITY REVIEW AND RATING PROCESS (SRRP) PROGRESS UPDATE

On September 1, 2021, DCSA began Year 1 of implementation for the refined SRRP with cleared industry. The process is firmly grounded in policy and will not be changing as we progress into Year 2. That being said, we will continue to examine both the review process and the rating evaluation process, and will issue iterative guidance to enable consistency and efficiency.

Since then, DCSA field personnel have conducted over 2,600 security reviews that found over 98% of the contractors were in general conformity with the basic terms of the NISPOM. This is a huge win for both DCSA and Industry! Of those security reviews, approximately 79% resulted in satisfactory ratings, and 20% resulted in commendable or superior ratings. These security ratings are consistent with historical norms under previous security ratings.

In June 2022, DCSA established an internal working group to examine SRRP results and feedback since implementation. The results of this working group were briefed to DCSA field personnel during internal sessions on September 7 and 8. These sessions also included refresher training related to common SRRP concepts and new job aids applicable to field personnel. DCSA is in the process of determining if any of these new job aids would also benefit Industry security personnel. In the interim, we recommend cleared contractors continue to reference the current job aids available on the DCSA SRRP website.

Looking ahead, DCSA personnel will begin implementing Year 2 of the SRRP on October 1. During Year 2, field personnel will increase the number of security reviews conducted across the NISP. We expect to see both DCSA field personnel and Industry become more comfortable with the SRRP, resulting in increased consistency and improved quality. DCSA will continue to identify gaps and will refine processes and job aids as necessary.

CONSOLIDATED ADJUDICATION SERVICES (CAS)

PROPER SUBMISSION OF INCIDENT REPORTS

To facilitate quicker processing, incident reports must include basic information covering:

- How - how did you receive the derogatory information?
- Who - who was involved?
- What - what is/was the incident?
- Where - where did the incident happen?
- When - when did the incident occur and who else is aware?

Steps to take after receiving an incident report:

1. The FSO should submit the Incident Report in the Defense Information System for Security (DISS), entering as much information and documentation as possible while also ensuring to select the appropriate dates and guidelines.

2. Be on the lookout and "claim" any and all Supplemental Information Requests (SIR) sent via Requests for Action (RFA) in DISS in response to the Incident Report.

3. Read the SIR carefully and either respond directly, or have the Subject respond to the SIR, in its entirety. Ensure the response addresses each of the bulletins of request. SIRs are a part of our fact-finding mission and the information requested is required by DCSA CAS in order to make an adjudicative determination.

4. If an extension is needed, make DCSA CAS aware of the extension request and the reasoning behind it in a timely fashion.

5. Lastly, if the Subject fails to or refuses to respond to the SIR, inform DCSA CAS rather than letting the RFA expire without a response.

Note: Refer to Security Executive Agent Directive (SEAD) 3 & 4, and DoD Manual 5200.02 regarding self-reporting incidents and life events. For assistance, please contact the Call Center at 301-833-3850.

RENAMING OF THE DOD CAF

On June 13, DCSA renamed the Department of Defense (DoD) Consolidated Adjudications Facility (CAF) to better reflect personnel vetting into the future. DoD CAF is now DoD Consolidated Adjudication Services (CAS). The renaming to DCSA CAS does not change any internal or external organizational reporting relationships, missions, resources, or support functions. DCSA, through the CAS, will continue to deliver informed and timely adjudicative decisions for the Federal Government to enable operational readiness in keeping with risk management principles.

CAS (ADJUDICATIONS) FY21 YEAR IN REVIEW ANNUAL REPORT

Please take a moment to read our FY21 Annual Report here.

CAS CALL CENTER

The CAS Call Center is available by telephone or email for inquiries. For more information, please call 301-833-3850 or email the CAS Call Center. We look forward to hearing from you.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

Check out the latest offerings from the NAESOC:

- What exactly do I need to do to have a compliant and effective Insider Threat Program? Check out the updates on the Insider Threat Tab at NAESOC website for a “How To” that can help you ensure your program is both complete and it supports your efforts.

- While you are there, download the latest NAESOC One-Pager too as a quick-reference for the resources and support it provides.

- In addition, National Background Investigation Services is coming for NAESOC facilities in December. Get ahead of the game with advice and resources on the NAESOC Latest Tab.

More questions? We have answers - You can talk to a Live Agent at the NAESOC Help Desk Mondays through Thursdays (9:00 to 11:00 am and 1:00 to 3:00 pm) and Fridays (9:00 am to 1:00 pm) by calling the DCSA Knowledge Center (1-888-282-7682; Option #7).

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

The NISS Team has been hard at work fixing issues regarding the submission and resubmission of packages based on feedback received from our industry partners.

On September 7, NISS Version 2.6.1.6 was released. This included updated functionality when completing Sponsorship Packages. The system now requires a Compelling Need Letter to be uploaded if access to classified information is not required in the performance of the contract. This release also resolved an issue with industry user's inability to select the "Save" and "Submit" buttons when attempting to resubmit Change Condition Packages and Facility Security Clearance Packages.

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 am to 6:00 pm ET.

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

DISS TO NBIS ORGANIZATIONAL HIERARCHY DATA MIGRATION UPDATE

Thanks to our industry partners for taking action based on the request to consolidate DISS for Security Management Offices as appropriate in March. Since that review and consolidation, DCSA has created business transformation rules and worked through quality assurance reviews to ensure Industry hierarchical data from DISS was migrated to the NBIS system.

Due to this joint effort, Industry hierarchy data has successfully transitioned from DISS to NBIS. Over 14,500 parent and 2,500+ child-type organizations have been moved into NBIS. As building organizational hierarchy is a primary step for Industry onboarding to NBIS, the migration effort has reduced the need for manual data entry, allowing for a more seamless onboarding experience.

This accomplishment represents a major step forward in moving towards the NBIS Industry Onboarding Regional Strategy discussed in the July Voice of Industry. Once onboarded to NBIS, industry users will need to ensure their hierarchies match in DISS and NBIS and keep them maintained.

For additional information and updates, please visit the NBIS Industry Onboarding website.

NISP CONTRACTS CLASSIFICATION SYSTEM (NCCS)

On August 10, Federal Acquisitions Regulation Section 4.402, was updated on August 10 to reflect the new DCSA-hosted NCCS 2.0 system. The Initial Onboarding Test Phase (IOTP) is well underway and we will be transitioning into Phase 1 of deployment for Government users starting in October. As we continue this phased onboarding approach, we are poised to begin Industry testing starting in mid-October. Industry testers will work closely with NCCS administrators to work through test cases and business flows to identify issues.

For more information, please visit the NCCS website.

VETTING RISK OPERATIONS (VRO)

REMINDER ON TIMING ON ELECTRONIC FINGERPRINT TRANSMISSION

As we move closer to full implementation of Trusted Workforce 2.0, VRO continues to work diligently to collaborate with Industry to get cleared people into the workforce faster and more efficiently all while effectively managing risk. To maintain our interim determination timeliness goals, we ask that electronic fingerprints be submitted with or just before an investigation request is released to DCSA in DISS.

Fingerprint results are valid for 120 days, the same amount of time for which Electronic Questionnaires for Investigations Processing (e-QIP) signature pages are valid. Therefore, submitting electronic fingerprints at the same time or just before you complete your review for adequacy and completeness should prevent an investigation request from being rejected for missing fingerprints.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

SEPTEMBER 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. In addition, we share upcoming courses, webinars, and conferences. The September newsletter focused on "National Insider Threat Awareness Month." 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!

NATIONAL INSIDER THREAT AWARENESS MONTH WRAP UP

As September ends, the fourth annual National Insider Threat Awareness Month (NITAM) comes to a close. This month-long campaign brought together thousands of U.S. security professionals and policy makers from Government and Industry, located in 25 countries around the globe, to educate and learn about the risks posed by insider threats and the role of insider threat programs. This year's theme was "Critical Thinking in Digital Spaces." Although NITAM is ending, insider threat awareness information should continue to be shared throughout the year. Access the following resources to continue educating yourself and your organizations:

- NITAM
- Insider Threat Training
- Insider Threat Toolkit

2022 INSIDER THREAT VIRTUAL SECURITY CONFERENCE ARCHIVED MATERIALS

The Insider Threat Virtual Security conference, jointly hosted by CDSE and Office of the Under Secretary of Defense for Intelligence and Security, was held on September 1. It brought together security professionals and policy makers from across the U.S. Government and Industry to kick off the National Insider Threat Awareness Month campaign. If you missed the conference or would like to revisit the presentations, visit the Conference Archive on the CDSE website.

NEW INSIDER THREAT ELEARNING GAME

CDSE recently released a new security awareness eLearning game, "The Adventures of Earl Lee Indicator: Mission One." Use your knowledge of the counter-insider threat mission to escape locked rooms before time runs out! Share the game with your workforce for a variety of fun ways to test insider threat knowledge and encourage security awareness within your organization. Play the game here!

DECEMBER CYBERSECURITY INSTRUCTOR-LED COURSE

The next "Assessing Risk and Applying Security Controls to NISP Systems CS301.01" instructor-led course is scheduled to start December 5. This 5-day 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 process. This course will also provide a comprehensive understanding of contractor requirements under the NISP. The target audience for this training includes information system security managers (ISSMs), information system security officers (ISSOs), and FSOs involved in the planning, management, and execution of security programs for cleared industry. To learn more, register, and view the required prerequisites, visit here.

NEW INDUSTRIAL SECURITY VIDEO NOW AVAILABLE

CDSE has a new video to improve your industrial security knowledge! This video provides an overview of the SEAD 3 reporting requirements for cleared contractors. Access the video here.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE