DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY
DCSA MONTHLY NEWSLETTER

November 2022

Dear FSO (sent on behalf of your ISR),

Industrial Security (IS) Operations publishes this monthly newsletter to provide recent information, policy guidance, and security education and training updates for Facility Security Officers (FSOs) in the National Industrial Security Program (NISP). Please let us know if you have any questions or recommendations.

VOI Newsletters are posted 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 posted on the Defense Counterintelligence and Security Agency (DCSA) website on the Industrial Security Industry Tools Page (VOIs are at the bottom). For more information on personnel vetting, industrial security, training, and other topics from the VOI, visit www.dcsa.mil.

TABLE OF CONTENTS

NISP CONTRACTS CLASSIFICATION SYSTEM (NCCS)

On November 9, the Systems Management Branch concluded a 2-week NCCS 2.0 test event with Industry volunteers provided through the National Industrial Security Program Policy Advisory Committee (NISPPAC). The test team verified Industry functionality through the DD Form 254 automated workflows. During the test event, daily meetings were held to discuss any issues or questions. All feedback, comments, and recommended enhancements provided by our Industry testers was captured and documented. The NCCS Team would like to express our appreciation and gratitude to the participants in this test event for their time, effort, and expertise.

Stay tuned for updates and announcements on Industry Onboarding as well as guidance on how to register for a NCCS account.

For any technical questions with NCCS, please contact the team at dcsa.quantico.dcsa-hq.mbx.nccs@mail.mil.

DCSA SECURITY REVIEW AND RATING PROCESS WEBSITE

The DCSA Security Review and Rating Process (SRRP) public website, located here, has been updated with refined products and information. This update is part of our continued effort to provide current, relevant, and timely information to our Industry and Government partners. We encourage you to visit the website at your convenience.

The following resources have been refined as part of this refresh:

- DCSA Security Review and Rating Process Overview

- DCSA Security Rating Process Flow (Overview Tab)

- DCSA Security Rating Process Slick Sheet (Resource Tab)

- DCSA Terms and Definitions (Resource Tab)

- Identifying Vulnerabilities, Administrative Findings, and Serious Security Issues (Resource Tab)

In addition to the refined products, you will also find the following products:

- DCSA Superior Security Rating Reference Card (Resource Tab)

- DCSA Commendable Security Rating Reference Card (Resource Tab)

- DCSA Security Review Process Slick Sheet (Resource Tab)

- DCSA Compliance Review (Resource Tab)

DOD CONSOLIDATED ADJUDICATION SERVICES (CAS)

THE HOLIDAY SEASON AND YOUR FINANCES

As we enter the holiday season, many are preparing to spend time with family/friends and exchange gifts. It can be stressful for some to feel the pressure of gift-giving, especially when they may not have the means to do so. As cleared professionals, we are all held accountable for financial responsibility. Just a gentle reminder to not overextend yourself to the point where repaying holiday debt becomes an uncontrollable issue. Material things are nice, but being in the presence of loved ones oftentimes can be the best present!

If you find yourself in need of advice, you can refer to the Employee Assistance Program through your employer or credit counseling services. Do not hesitate to ask for help!

For more information on financial adjudicative guidelines, please refer to Security Executive Agent Directive 4 (SEAD-4), "Guideline F: Financial Considerations."

CAS CALL CENTER

CAS Call Center representatives are available to assist with your security clearance questions and concerns. Please call them at 301-833-3850 or email the CAS Call Center.

GAO NISP SURVEY

On Monday, November 7, you may have received an email from an analyst with the U. S. Government Accountability Office (GAO). The analyst indicated that GAO planned to send a survey as a part of a review on reciprocity in personnel vetting. The analyst sent the email to a sample of FSOs using information in NISS, which DCSA provided to GAO.

The GAO email is a legitimate request for your assistance.

As you may know, GAO is an independent, nonpartisan agency that reports to Congress on the efficiency and effectiveness of federal programs. In the email, the analyst stated that Congress requested that GAO analyze aspects of the reciprocity process. To enable the GAO team to conduct its review, we provided information to allow the team to draw a sample of companies to survey and the contact information for the FSOs in those companies.

GAO may have already sent you the survey, or will shortly, and we encourage you to complete it. Completing the survey will help GAO get fully informed about your experiences with the reciprocity process, enabling them to account for your experiences in their report and any recommendations they may make. The GAO team told us that they plan to aggregate the responses and report on trends they observe. GAO also said that they would not reveal the source of any particular survey response in their report.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

Be sure to keep up with NAESOC announcements on the NAESOC Web Page.

Whether you are a new or a very experienced Facility Security Officer, you can benefit from resources you can find on the NAESOC Web Page to get the most from the required annual review of your security program.

Remember to bookmark the web page for what we keep updated on the NAESOC Latest tab. Use these resources to better prepare for the NBIS rollout to NAESOC facilities in December.

More questions? We're here to help – Check out the web page for the latest information already at your fingertips or for the opportunity to submit your issues and queries to our Help Desk and even talk to Live Agents.

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

UPCOMING NBIS TRAINING WEBINARS

Please be aware that the NBIS Industry Onboarding Team will introduce the following training webinars sometime in December 2022/January 2023, which will include live and recorded sessions:

- Org and User Management

- Assignment Management Configuration

- Optional User Management Configuration: Notifications

- Optional User Management Configurations: Program Tags

Details about these sessions will be forthcoming. Industry users, especially those from organizations that have been notified to start the NBIS onboarding process, are highly encouraged to participate.

Should you have any questions about these upcoming webinars, please send your inquiry via email to the NBIS Industry Onboarding Team at dcsa.meade.nbis.mbx.nbis-industry-onboarding-team@mail.mil.

NBIS ONBOARDING STARTS IN THE WESTERN REGION

On November 22, NBIS onboarding officially commenced for facilities located in the DCSA Western Region. Notification and instructions were provided via email to those identified as Account and Hierarchy Managers for the Defense Information System for Security (DISS) in order to begin the onboarding process into NBIS.

Onboarding to NBIS is accomplished through the Industry Onboarding Portal (known as NBIS ServiceNow). One user (known as the 'Initial User') from each organization will onboard through the Industry portal. Once provisioned and enrolled into NBIS, the Initial User will be responsible for provisioning additional users within their organization.

Once onboarded, users will validate their org hierarchy migrated from DISS and configure org workflow and user assignments. Even after onboarding into NBIS, Industry organizations will continue utilizing DISS for all functions until further notice. The Initiate, Review, and Authorize process will be the first NBIS capability to be adopted by Industry, but only once DCSA VRO provides notification when this can begin.

In order to gain access to NBIS, all users are required complete PII and Cybersecurity training within the last 12 months. To prepare, all potential NBIS users are encouraged to complete the required training. Please refer to the "NBIS Industry Onboarding Readiness Checklist" available on the NBIS Industry Onboarding website for details on where to access these trainings and maintaining the certificates.

After onboarding, users are reminded to login into NBIS at least once every 30 days to avoid account deactivation and monitor DISS and NBIS hierarchies for org changes.

As always, for additional information and updates, please visit the NBIS Industry Onboarding website.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

On November 9, the Systems Management Branch deployed NISS Version 2.6.1.8, which included enhancements to the Facility Clearance Notification. Industry and External Government users with the Facility Clearance Verifier (FCV) role will be able to view the following additional Facility Profile information when verifying facility clearances:

- Cleared Off-Site Address

- Cleared Off-Site Safeguarding Level

- FOCI Mitigation

- FOCI Adjudication

- FOCI Mitigation/Acknowledgment Date

- FOCI Agreement Expiration Date

If the requested company's Facility Profile does not have any of the above information populated, those sections will be blank on the Notification.

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 (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 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 DISS. 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 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.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NOVEMBER 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 November newsletter focused on "Critical Infrastructure Security and Resilience." 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 NEWS

CDSE offers an email subscriber news service to get the latest CDSE news, updates, and information. Subscribe to the Flash (news/updates), the Pulse (monthly security awareness newsletter), the Quarterly Product Report, insider threat bulletins, or one of our other publications. Visit our news page and sign up or update your account today.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE