DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

February 2023

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

FYI - AUSTRALIA REMOVING CHINESE-MADE CAMERAS

There has been a recent item in the news regarding the Australian government removing Chinese-made security cameras and equipment from their sensitive sites. This action follows an audit that found at least 913 Chinese-made cameras installed across more than 250 Australian government buildings, including the departments for defense, foreign affairs, and attorney general, according to official figures.

This action follows measures by the United States and the United Kingdom to ban Chinese-made cameras at their sensitive sites. The measures were taken out of an abundance of caution because Chinese companies are subject to China's National Intelligence Law which requires them to cooperate with Chinese intelligence agencies, and there is no way to ensure that sensitive information, images, and audio collected by these devices are not being provided to China.

Cleared Industry is reminded that Federal Acquisition Regulation 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, dated November 2021, contains language addressing the prohibition on contracting that uses services or equipment from specific Chinese companies. The Regulation may be viewed here.

SPONSORSHIP AND FCL PACKAGE SUBMISSION UPDATES

Effective March 1, 2023, DCSA is implementing updated procedures for facility clearance (FCL) sponsorship and FCL package submissions to reduce the cycle, or re-work, between government contracting activities (GCAs) or contractors and DCSA. These changes are one of a number of initiatives DCSA is undertaking, internally and externally, to streamline the FCL process, which will ensure the fullest degree of transparency practicable during the sponsorship and FCL package processes. DCSA encourages the full utilization of available resources from DCSA by sponsors or the sponsored contractors to ensure complete and accurate packages are submitted to facilitate DCSA's efficient and thorough evaluation of each case.

The reworking of packages submitted to DCSA adds significant time to case reviews and contributes to the aging of package submissions in queue. These increases in time across the FCL process severely impede the ability of GCAs to receive the goods or services required to execute their missions in a timely manner, the profitability of contractors, and the risk to national security. The cycle for sponsorship packages is, on average, 1.93 times per package with a 53% rejection rate. That number increases to 2.5 times for initial/upgrade FCL packages with a 70% rejection rate. DCSA is committed to reducing both rates, cycle and rejection, to or near 1.1 and 15%.

For more details regarding sponsorship and FCL submission procedures, see DCSA News.

NISP CONTRACTS CLASSIFICATION SYSTEM (NCCS)

The Industrial Security Systems Management Branch deployed NCCS version 2.1.1 this month. This version focused on improving the user search functionality for completed DD Form 254s and adjusting some of the administrator functions.

In the January NCCS Operational Requirements Committee (ORC) meeting, the NCCS team presented five requirements that were derived from an Industry testing event. All five requirements were approved by the ORC and passed to the development team for implementation into the system. These include allowing Industry to edit specific sections of the Subcontract DD Form 254 to include blocks 13, 18f, and 11m. Industry will also be able to enter up to 100 work locations in block 8.

The NCCS Team continues to work closely with the National Industrial Security Program Policy Advisory Committee (NISPPAC) to develop a phased onboarding approach for cleared Industry this spring. Stay informed by visiting the NCCS section on the DCSA external website and the monthly VOI newsletters.

For technical questions on NCCS, please contact the team via dcsa.quantico.dcsa-hq.mbx.nccs@mail.mil.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

Have you logged into NISS within the past 30 days?

If 30 days elapses without logging into your NISS account, your account will be locked and placed in an ‘Inactive’ status. At 45 days of inactivity, your NISS account will remain locked and all associated user roles will be removed. Inactive and locked accounts are not only inconvenient but also result in the following:

- An inability to utilize the NISS Messaging feature to contact your DCSA Oversight Team.
- An interruption in the ability to submit or resubmit Sponsorship Packages, FCL Packages, Industry Facility Profile Updates (IFPUs), and Changed Condition Packages.
- Loss of access to Facility Clearance Verification (FCV) Notifications.

To have an account reactivated and unlocked, contact the DCSA Knowledge Center. Once unlocked, new role requests can be submitted for review and approval.

Avoid losing access and the associated frustrations by staying active in NISS every 30 days!

For any technical questions with NISS, please contact the DCSA Knowledge Center at 888-282-7682 and select Option 2, then Option 2 again. The DCSA Knowledge Center hours of operation are Monday through Friday from 8:00 a.m. to 6:00 p.m. ET.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

"The NAESOC has contacted me and informed me that my facility is being scheduled for a remote security engagement. What does that mean and how can I prepare for it?"

NAESOC security engagements address specific security related items and information about your security program that the NAESOC has identified as a result of normal oversight and monitoring activities. The security engagement will focus on validating those issues and identifying mitigations that need to be applied. The security engagement may also assess the general security posture of the facility. Although these are not security reviews, these engagements focus on ensuring your facility remains in compliance with requirements in 32 CFR, Part 117, "National Industrial Security Program Operating Manual (NISPOM) Rule."

Best practices to support NISPOM Rule compliance:

- Complete a self-review using the self-inspection handbook (and submit the certified results letter through NISS
- Submit timely changed condition packages through NISS
- Complete facility profile updates as changes to the facility are identified
- Ensure that your facility is maintaining the accuracy of their Senior Management Official in the Defense Information System for Security (DISS)
- Maintain a current Security Standard Practices Procedures (to include your Insider Threat Program Plan) that includes NISPOM reporting requirements (32 CFR Part 117.8).

These actions will ensure you are ready to participate in a productive security engagement with your NAESOC ISR.

RENEWAL OF DD FORM 441 AND DD FORM 441-1

In December 2022, the DD Form 441, Department of Defense Security Agreement, and DD Form 441-1, Appendage to Department of Defense Security Agreement, were renewed. Previously executed versions of this form do not need to be re-signed, but the updated versions should be used going forward. The updated forms can be found here:

- DD Form 441
- DD Form 441-1

Questions can be directed to your assigned Industrial Security Representative.

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

INDUSTRY: HOLD ON SUBJECT MANAGEMENT ACTIONS IN NBIS

As Industry works through the onboarding and configuration processes in the NBIS system, the DCSA NBIS Industry Onboarding Team would like to remind users to refrain from taking any subject management actions in NBIS, to include creating a subject's profile or initiating cases, until notification is provided that these actions can begin.

DCSA is planning to migrate all subject information from the Defense Information System for Security (DISS) to NBIS at a later date (to be announced). Creating subjects prior to the migration effort could potentially create issues once migration from DISS to NBIS takes place, for instance, duplicate subject information. Until the migration takes place, organizations should concentrate their efforts on enrolling into NBIS and conducting the necessary validating and configuring actions to prepare for system functionality, the first of which will be case initiation.

At this time, organizations should continue to use DISS for Case Initiation, Investigation Status, Visit Management, Subject Management, Eligibility Determinations, Incident Reporting, Access Management, Foreign Travel, etc.

For other questions regarding the NBIS Industry Onboarding Process, please email the NBIS Industry Onboarding Team.

NOW AVAILABLE: RECENT NBIS WEBINARS SLIDES AND RECORDINGS

For any NBIS Industry Users that were not able to attend or would like to refresh or review, recordings and slide decks from the live Org and User Management and Assignment Management Configurations webinars that took place in December 2022 and January 2023 are now available on the NBIS Training Site.

Once logged into the site, navigate to the "Industry Onboarding Resources" section and click "View Materials" to access the aforementioned webinar resources as well as other available webinar recordings.

Be aware that the recordings and slides have not yet migrated to the Security Training, Education, and Professionalization Portal (STEPP) and ServiceNow. In the interim, Industry users will want to access these on the NBIS Training Site.

Note: Internal DoD users may not be able to access the Industry page on the NBIS Training Site due to firewall limitations.

If you have questions, please email the NBIS Industry Onboarding Team.

NBIS "QUICK LINK" NOW AVAILABLE

For Industry users that have already been granted access to NBIS, a "quick link" is now available on the DCSA NBIS Main Page. The quick link is available at the top of the page and is labeled "NBIS Agency (for SSOs/FSOs)." Once you click the link, it directs you to the NBIS portal in order to access the system.

In addition to the link on the NBIS main page, users are also encouraged to bookmark the NBIS portal page on their browser for fast and easy access.

For questions regarding the NBIS Onboarding Process, please email the NBIS Industry Onboarding Team.

COUNTERINTELLIGENCE AND INSIDER THREAT WEBINAR

DCSA invites cleared industry and academia personnel to participate in an unclassified webinar. On Thursday, March 16, Mr. Glenn Tiffert, Ph.D., Research Fellow, Hoover Institution, will present a "Chinese Malign Influence" webinar. This event is intended for industry personnel including but not limited to: executive officers, key management personnel, FSOs, engineers, business development personnel, industrial security personnel, and cyber security professionals. The webinar will be held virtually on March 16 from 1:00 to 2:30 PM ET. Please register using this eInvitation.

PSI INDUSTRY DATA COLLECTION IN NISS

DCSA is responsible for projecting Personnel Security Investigations (PSI) requirements each year. The data collection for PSI projection requirements will be conducted March 6 through March 31, 2023, through the NISS Submission Site. Annual projections acquired from Industry through this collection are the key components in DoD program planning and budgeting for NISP security clearances.

In preparation for this upcoming data collection, our Industry partners are highly encouraged to register for their NISS accounts before March 6 in order to participate in the survey. Registration instructions are found on DCSA's NISS website under the Registration tab. For all other NISS questions, please contact the DCSA Knowledge Center at 888-282-7682 and select Option 2, then Option 2 again.

We look forward to your participation. If you have any questions, please contact dcsa.ncr.dcsa.mbx.psiprogram@mail.mil.

DCSA CONSOLIDATED ADJUDICATION SERVICES (CAS)

CAS CALL CENTER

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

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

FEBRUARY PULSE: CDSE SECURITY AWARENESS NEWSLETTER

DCSA 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 February newsletter focused on "ACE Credit Recommendations." 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!

UPCOMING COUNTER-INSIDER THREAT WEBINAR

CDSE in collaboration with the DoD Insider Threat Management and Analysis Center (DITMAC) presents the counter-insider threat community training series. Join us on Thursday, March 2 to learn more about structured professional judgment (SPJ) tools in insider threat and be part of the conversation! Registration is now open here.

UPCOMING PERSONNEL VETTING TIMELY TOPICS WEBINAR

CDSE is hosting a live webinar with Vetting Risk Operations on March 14 from 1:00 p.m. to 2:30 p.m. This webinar will discuss Trusted Workforce 2.0 personnel vetting reforms, focusing on Continuous Vetting, which is applicable to DoD civilian employees, contractor personnel, and military members. Participation is limited to 1500 attendees, so sign up today!

For more information, and to register, visit our Webinars and Conferences webpage.

NEW PRODUCTS FROM THE THREAT LAB NOW AVAILABLE

The Defense Personnel and Security Research Center (PERSEREC) produces the Bottom Line Up Front (BLUF) products that highlight what The Threat Lab personnel are watching, listening to, reading, and thinking about. Issue 8 artifacts, which focus on Critical Thinking and Issue 9 artifacts, which focus on Bystander Effect, are now available Research Tab of the Insider Threat Toolkit. Scroll down to the Newsletters to check out the latest and previous issues of the BLUF.

CDSE LINKEDIN

CDSE is now on LinkedIn. Follow our profile for real-time information on professional development opportunities such as courses, webinars, and events!

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE