DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

December 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 December 2, the System Management Branch deployed NCCS Version 2.0.15. This release focused on organization hierarchy changes.

The NCCS team met with the Industry testers and captured additional requirements to be added to NCCS' capabilities. Those requirements have been codified and will be presented to the NCCS Operational Requirements Committee (ORC) in January for approval.

Be on the lookout for announcements on NCCS Industry onboarding coming in the New Year!

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

NSA UPDATED EVALUATED AND EXPIRED PRODUCTS LISTS

The National Security Agency (NSA) Central Security Service recently released (last October) updated an Evaluated Product List and an Expired Products List. These are available to the public at the NSA Evaluated Product Lists website. When visiting the site, you will see the link to the NSA Policy Manual 9-12, links to all the currently approved Evaluated Product Lists, as well as the updated Expired Products List. DCSA asks that you review the Expired Products List to ensure you do not continue to use any of these formerly-approved sanitizing devices.

It is important that you bookmark this page and review it regularly to ensure you have updated copies of the currently approved devices, as well as those with expired approvals. It is suggested that you review the approved Evaluated Product List and vendor information prior to purchasing and using any device for classified destruction.

DISS JVS TRAINING MATERIALS

Training materials for the Defense Information System for Security (DISS) Joint Verification System (JVS) are available! Simply go to DISS Resources here.

Under the Trainings Materials subtab, you will find job aids on Verification by SSN (social security number), Consolidating SMOs (security management offices), and more.

The E-Learning subtab has a link to DISS Training at USA Learning where you can access modules on:

- Subject Management
- Clearance Eligibility and Granting Accesses
- Investigation Request
- Suitability Determination and Homeland Security Presidential Directive 12 (HSPD12) for Non-Sensitive Positions, and many more!

These are great resources to assist you on your DISS JVS journey. Start a course today!

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

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

Self-Inspections:

- At the end of the calendar year, many FSOs are planning or executing their formal self-inspections, as described in 32 CFR Part 117.7(h)(2)(ii). If you are planning or executing yours, we want to recommend the best practice of using the "Self Inspection Handbook for Contractors" which can be found at Industry Tools under the FSO Guides subtab.
- In the Handbook you will find eight checklists that are common to ALL NAESOC companies:
    - Procedures [117.7]
    - Reporting Requirements [117.8]
    - Entity eligibility determination for access… [117.9]
    - (Contractor) eligibility for access to classified… [117.10]
    - Foreign Ownership, Control, or Influence (FOCI) [117.11]
    - Security training and briefings [117.12]
    - Classification [117.13]
    - Visits and meetings [117.16].
- Also, the NISS Knowledge Base has a NISS guide to assist in submitting the self-inspection. Instructions can be found on the NAESOC web page.

Facility Profile Updates:

- When conducting Self-Inspections, many FSOs have identified the need to provide Facility Profile Updates. Facility Profile Updates are information items that can be edited by Industry users, and include but are not limited to new contracts, program assets, and essential Key Management Personnel and security staff contacts. Ensure that you review your profile and submit timely updates. Please make sure all of your appropriate DD Form 254s are submitted via NISS and remember that FCL Change Conditions should not be submitted as Facility Profile Updates.

Insider Threat Programs:

- Self-Inspections have demonstrated the need for some facilities to ensure that their Insider Threat Programs are current and effective. Remember that your Insider Threat Program should include:
    - Endorsement by the Insider Threat Program Senior Official (ITPSO)
    - Formal appointment of an ITPSO who is a U.S. citizen employee and a company senior official
    - Contractor reviews, certified annually.
- Find more information and tips to enhance your Insider Threat Program on the NAESOC web page.

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

COMING IN JANUARY: NBIS ONBOARDING FOR ALL OF INDUSTRY

NBIS onboarding officially commenced in November 2022 for industry facilities in the DCSA Western Region. Starting January 9, all other Industry facilities in the remaining DCSA regions (Eastern, Central, Mid-Atlantic, as well as HQ) will be provided notification and instructions via email to DISS Account and Hierarchy Managers for organizations 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 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 organizational hierarchy migrated from DISS and configure organizational workflow and user assignments. Even after onboarding into NBIS, Industry organizations will continue using 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 Vetting Risk Operations (VRO) provides notification as to when this can begin.

In order to gain access to NBIS, all users are required to complete PII and Cybersecurity training within the last 12 months. To prepare, all potential NBIS users are encouraged to complete the required training, especially if their PII and/or Cybersecurity training is nearing the 12-month mark. 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 organizational changes.

For any questions, please email the NBIS Industry Onboarding Team. For additional information and updates on NBIS Industry Onboarding, please visit the NBIS Industry Onboarding website.

REGISTER NOW: NBIS INDUSTRY ONBOARDING LIVE WEBINARS

The DCSA NBIS Industry Onboarding Team invites Industry users to register for two upcoming live virtual webinars on the following NBIS topics:

- Org and User Management
  Tuesday, January 10, 2023
  1 p.m. – 3 p.m. ET

This webinar will provide basic NBIS navigation steps and organization management basics, show how to apply minimum configurations needed for investigation requests, describe and demonstrate form routing, and show how to manage users within your organization.

- Assignment Management Configurations
  Tuesday, January 17, 2023
  1 p.m. – 3 p.m. ET

This webinar will show how to create and apply optional configurations in NBIS to meet organizational needs, identify optional configurations based on organizational functionality, understand and apply assignment rules, and comprehend the use of both user assignment and order form templates.

Registration is now open now through January 5. For additional information and to register, please visit NBIS Onboarding Virtual Webinars. All participants MUST register to receive an invitation and further instructions.

Capacity for both sessions is limited. For those unable to attend, recorded sessions will be made available on the NBIS Training Site.

For questions, please email the NBIS Industry Onboarding Team at dcsa.meade.nbis.mbx.nbis-industry-onboarding-team@mail.mil.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

Start the New Year right by ensuring your NISS facility profile is up to date. Pay special attention to the "Contacts" subcategory under "Facility Overview." Verify that the correct phone number and email is listed for the FSO, the Senior Management Official, and the Insider Threat Program Senior Official.

In order to update the contact information, please submit a Facility Profile Update Request. For guidance on how to submit a Facility Profile Update Request, visit the Knowledge Base in NISS for associated training materials.

For any technical questions with NISS, 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.

DOD 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)

DECEMBER 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, it shares upcoming courses, webinars, and conferences. The December newsletter focused on ther SPēD Certification Program. 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!

REGISTER NOW FOR UPCOMING WEBINAR

CDSE invites you to participate in the following upcoming webinar:

- Overview of SPēD Certifications
  Thursday, January 26, 2023
  1:00 p.m. to 3:00 p.m. ET

This live webinar will feature SPēD PMO experts from CDSE who will discuss certifications and credentials available through the agency. This session will provide attendees with a general overview of available certifications, target audience identification, the general process to obtain and maintain certifications and a question and answer period.

Visit CDSE Webinars and Conferences to sign up for this event and join the discussion!

NEW 2023 INSIDER THREAT VIGILANCE CAMPAIGN

CDSE recently released the 2023 Insider Threat Vigilance Campaign job aid. The job aid promotes a different vigilance theme each month. CDSE will provide awareness materials relevant to each monthly theme to be shared with your workforce. Use the job aid to jump-start your 2023 annual vigilance campaign or tailor it to your organization using resources from our Insider Threat Toolkit Vigilance Tab.

CDSE LINKEDIN

Did you know that CDSE is now on LinkedIn? Follow the profile for real-time information on professional development opportunities such as courses, webinars, and events!

NEW WEBCAST NOW AVAILABLE

CDSE has a new recorded webinar "Tips for Setting Up Your Access Elsewhere Security Program Webcast," featuring NAESOC helpdesk security researchers. In this webcast, researchers answer questions from FSOs, and identify training resources to help FSOs set up and manage their Industrial Security Programs. View the webcast at here.

NEW INSIDER THREAT CONTENT IS AVAILABLE

Each month, CDSE's Insider Threat Division will highlight current job aids and case studies for learning, professional development, and for use as teaching tools for your Insider Threat Program.

This month's feature is the "Potential Risk Indicators: Active Shooter and Pathway to Violence" job aid, and a case study on Yu Zhou and Li Chen.

The Potential Risk Indicators: Active Shooter and Pathway to Violence job aid is now available here. This job aid includes the traditional pathway models and features other concerning behaviors that remain relevant as potential risk indicators.

Yu Zhou and Li Chen's case study details the career of the former researchers who worked for different doctors in separate laboratories at the Research Institute for Nationwide Children's Hospital (RINCH) in Columbus, Ohio. Their research centered on exosomes, which play a key role in the research, identification, and treatment of a range of medical conditions. An investigation revealed that, over a number of years prior to their departure from RINCH, Zhou and Chen worked together to steal propriety information and then monetize trade secrets by creating and selling exosome isolation kits to China. The couple were arrested in California in 2019, plead guilty in federal court, and sentenced to prison for their roles in the scheme. To access this and other case studies, go to the CDSE Case Study Library.

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 other publications. Visit the 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