DSS Monthly Newsletter
March 2018

(Sent on behalf of your ISR.)

Dear FSO,

This is the monthly newsletter containing recent information, policy guidance, and security education and training updates. If you have any questions or recommendations for information to be included, please feel free to let us know.

WHERE TO FIND BACK ISSUES OF THE VOI NEWSLETTER

Missing a few back issues of the Voice of Industry (VOI) Newsletter? The Defense Security Service (DSS) Public Affairs Office maintains a library of the VOI Newsletter (and other important forms and guides) on its Industry Tools page.

DSS IN TRANSITION (DiT)

In 2017, DSS launched an enterprise-wide change initiative called, "DSS in Transition". The goal of DiT is to move the Agency from being focused strictly on schedule-driven NISPOM (National Industrial Security Program Operating Manual) compliance to an intelligence-led, asset-focused, and threat-driven approach to industrial security oversight.

The new DiT methodology is based on knowing the relevant assets at each facility, establishing tailored security plans, and applying appropriate countermeasures based on threat. DSS is implementing the new process in an incremental way that educates both DSS personnel and participating industry partners as the process is continuously evaluated and improved. Comprehensive training of the new DiT methodology for DSS field personnel is scheduled to occur at DSS Operational Training Events in April 2018. DSS is also in the process of conducting a training needs analysis that will help inform the long-term training developed for industry, Government partners, and DSS personnel.

As part of a phased implementation, four facilities were selected by DSS to participate in the first phase of implementation of DiT. These four industry partners were the first to be reviewed under the entire DiT process outside of the direct supervision of the Change Management Office. The assessments are now concluding and DSS will soon pause to assess the process and incorporate lessons learned. DSS will use expertise and insights gained to improve the process and begin incrementally expanding the number of facilities assessed under this new methodology. DSS Field Offices are currently validating the list of facilities associated with the DSS Director's top priority technology and determining eight facilities to be reviewed during the second phase of implementation. If your facility is selected to be reviewed for the second phase of implementation, your ISR will notify you in the coming weeks.

By the end of the year, DSS anticipates a majority of personnel will be trained on the new approach, facilities assessed will have developed a tailored security plan, and the process will be refined along the way. DSS will continue to assess and rate facilities not involved in DiT implementation in 2018 under the traditional security vulnerability assessment model. During these assessments, DSS will introduce facility security personnel to the concepts of asset identification and documenting business processes associated with the protection of assets. DSS will also introduce facility security officials to a new threat assessment tool known as the "12x13" matrix.

For more information on the DiT methodology, click here.

INDUSTRY REAUTHORIZATION SUBMISSIONS

Industry reauthorization submissions should be submitted 60 - 90 days before the current Authorization to Operate (ATO) expires. This will give DSS time to review the System Security Plan (SSP), conduct an assessment, and interact with Industry regarding potential corrections or updates.

It is incumbent on Industry to submit a timely and complete reauthorization package. Communication between the Information System Security Manager (ISSM) and Information Systems Security Professional (ISSP) is the key to successfully achieving an ATO reauthorization. If Industry waits until the day before an ATO expires to engage, the process will fail.

The DSS goal is to make authorization decisions within 30 days.

If you have questions or concerns, please contact your assigned ISSP or visit the DSS RMF Website.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) MARCH UPDATE

Over the past several months, DSS has been researching and resolving NISS application issues and helping NISS reach full operational capability. DSS has prioritized efforts to resolve account registration/access issues. We appreciate your patience as we continue to keep NISS a top agency priority and deliver its capability as quickly as possible.

The NISS continues to remain in a soft launch, test state. Users can log in and explore the system by conducting functions that they would during their day-to-day job. However, all official business should be conducted in the Industrial Security Facilities Database (ISFD) and the Electronic Facility Clearance System (e-FCL), as they remain the official systems of record until NISS is operationally deployed.

Once it is determined that all critical issues have been resolved, DSS will notify the user community to prepare for the full transition to NISS. We expect to provide at least 30 days notice. Please note, the NISS soft launch period allows end-users to report bugs and issues to DSS. Every issue reported helps DSS test and fix the system prior to full operational capability.

Update regarding Account Registration/Access Issues:

1) If you are unable to submit your NISS account request and receive "An error occurred while determining the approver for the Commercial and Government Entity (CAGE) Code specified," please send your name, email address, and CAGE Code to DSS.NISS@mail.mil. This is a system bug that the team is actively working. While this bug has been resolved for many CAGE codes, there are still some outstanding issues. We will notify the user base, including affected users, when it is resolved. Please clearly state the issue and attach screen shots of any error messages. *If you have already provided your information for this error and received a response from DSS, you do not need to resubmit your information.*

2) If your account was approved but you still cannot log into NISS (either the NISS link does not appear or the NISS application does not load properly), please send your name, email address, and CAGE Code to DSS.NISS@mail.mil. Please clearly state the issue and attach screen shots of any error messages. *If you have already provided your information for this error and received a response from DSS, you do not need to resubmit your information.*

Reminder - you must log into your NISS account every 30 days to avoid account lockout. If your account becomes locked, call the Knowledge Center (888) 282-7682 and choose Option 1, then Option 2. Accounts are locked after 30 days of inactivity and are deactivated after 45 days.

Please Note – merely logging into the National Industrial Security Program (NISP) Central Access Information Security System (NCAISS) does NOT log you into NISS. You must click the NISS Application link within NCAISS followed by the "I Accept" button on the consent page to keep your NISS account active.

The NISS training course for Industry and External Government users is available here.

Thank you for your patience during this transition!

SF-312 GUIDANCE

In May 2018, the Personnel Security Management Office for Industry (PSMO-I) is slated to transition to the Defense Information System for Security (DISS). With the advent of the new system of record for Personnel Security Clearance (PCL) processing, there will be changes to existing processes for Industry. One of the primary changes affect the handling and processing of Classified Information Nondisclosure Agreements (SF-312). More information and guidance may be found here.

REMINDER ON TIMING FOR ELECTRONIC FINGERPRINT TRANSMISSION

Electronic fingerprints should be submitted at the same time or just before an investigation request is released to DSS in Joint Personnel Adjudication System (JPAS).

You can confirm that the National Background Investigations Bureau (NBIB) has processed the fingerprints by checking SII in JPAS which indicates an "SAC" closed.

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 fingerprint 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.

A high level process flow outlining this and other PCL activities associated with obtaining a security clearance for industry is provided here for your ease of reference, and Step #2 outlines the submission activities.

TIER 5 REINVESTIGATIONS

Effectively immediately, Industry should continue to submit all Tier 5 Reinvestigations (T5Rs) whose investigation close date is 6 years or older. Caveat T5Rs should continue to be submitted at the 5-year mark.

SECURITY EDUCATION AND TRAINING

NEW INSIDER THREAT INDICATORS IN UAM JOB AID

This job aid discusses Insider Threat policies and procedures for User Activity Monitoring (UAM) on classified networks in support of Insider Threat Programs. Logging, monitoring, and auditing of information system activities can lead to early discovery and mitigation of behavior indicative of insider threat. UAM also plays a key role in prevention, assistance, and response (PAR) capabilities to insider kinetic violence threats. The job aid may be viewed here.

COUNTERINTELLIGENCE AWARENESS VIGILANCE CAMPAIGN

Check the Vigilance button of the Insider Threat Toolkit for customizable Vigilance Campaign posters, guidance, job aids, and other resources.

UNAUTHORIZED DISCLOSURE VIDEO

Improper handling of classified documents can happen. As a cleared individual, you have an obligation to protect classified information. Failure to do so can result in damage to national security and the warfighter. There are approved channels to report fraud, waste, or other abuse through existing whistleblower or inspector general channels. There are also approved channels for the release and review of DoD information. Knowing how to handle these situations is crucial to protecting our Nation's secrets. See the video here to learn more.

NEW CYBERSECURITY CURRICULUM RELEASED

The Center for Development of Security Excellence (CDSE) recently launched a new Cybersecurity curriculum, "NISP Assessment and Authorization (A&A) Curriculum." This curriculum provides students with a thorough understanding of the security requirements for safeguarding classified information being processed and stored in information systems at cleared contractor facilities through an in-depth review of the NISP A&A process. Access the new curriculum here.

NEW CYBERSECURITY COURSE RELEASED

CDSE recently launched a new Cybersecurity course, "Technical Implementation of Assessment and Authorization in the NISP." This course is the third in a series of three courses comprising the NISP A&A Curriculum. It focuses more on technical aspects of the A&A process and guides students on assessing the system using the Security Content Automation Protocol (SCAP) Compliance Checker, Security Technical Implementation Guides (STIGs), and the STIG Viewer. The new Cybersecurity course may be accessed here.

UPCOMING WEBINARS

CDSE invites you to participate in our upcoming webinars:

- **Key Management Personnel and Personnel Security Clearance**
  Thursday, April 19, 2018
  11:30 a.m. ET & 2:30 p.m. ET

  This webinar will identify the Key Management Personnel (KMP) required to be cleared for granting or maintaining a Facility Security Clearance (FCL). Discussions will include Essential KMP, Non-Essential KMP, Exclusion Resolutions, and Common List of KMP.

- **Transmitting or Transporting of Classified Material by Industry**
  Thursday, May 17, 2018
  11:30 p.m. ET & 2:30 p.m. ET

  This webinar will present an overview of NISPOM requirements for the transmission or transportation of classified material by Industry.

Register and be part of the conversation! Sign up today at CDSE Webinars.

ARCHIVED INDUSTRIAL SECURITY WEBINAR NOW AVAILABLE

Did you miss last month's "Visits and Meetings in the NISP: What's New?" webinar? This webinar discussed why it was necessary to make changes to the course, "Visits and Meetings in the National Industrial Security Program (NISP)." It also addressed the definitions of visits and meetings in accordance with the NISPOM. If so, you can now access the archived webinar.

Access the archived webinar (no certificate provided) at CDSE Previously Recorded Webinars or register for the on-demand webinar (certificate provided) at CDSE On Demand Webinars.

UPCOMING SPEAKER SERIES

Join CDSE for our April/May Speaker Series:

- **Let's Talk About FOCI**
  Thursday, April 12, 2018
  12:00 p.m. ET

This is the first of a series of topics from the Industrial Security discipline that will focus on various missions within DSS. Our guest will be speaking with us regarding Foreign Ownership, Control, or Influence (FOCI) and some main concerns for DSS, as well as the problems that occur when one doesn't report FOCI. The speaker will also delve into ways in which we can change things.

- **Kicking off an Insider Threat Vigilance Campaign**
  Thursday, May 10, 2018
  12:00 p.m. ET

  This webinar will discuss the goals of the Insider Threat Vigilance Campaign, which is built on the foundation of required annual training in Insider Threat Awareness as mandated by executive order and DoD policy.

Register and be part of the conversation! Sign up today at CDSE Webinars.

GETTING STARTED SEMINAR FOR NEW FSOs FY18 SCHEDULE

Getting Started Seminar for New FSOs (GSS) gives new FSOs the opportunity to discuss, practice, and apply fundamental NISP requirements in a collaborative classroom environment and develop a network of professional associates. This course is appropriate for any FSO, new or old, who is looking to enhance their security program.

Take a look at our FY18 schedule to see if we will be presenting this course in your neighborhood:

June 4, 2018, Dallas, TX (a 1-day course in conjunction with NCMS), go here

Aug. 14-15, 2018, Pasadena, CA, go here.

We will also be offering this class at CDSE in Linthicum, MD on June 12-13, 2018. This course will be given in the hybrid format (instructor-led and Adobe Connect). Please see the website here for additional details regarding the hybrid course.

Seats are limited, so make sure you have successfully completed the current version of the prerequisite course, "Facility Security Officer (FSO) Role in the NISP" (IS023.16) and exam (IS023.06). Once completed, register for the course you would like to attend. We look forward to seeing you soon!

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.

Thanks,
ISR
Defense Security Service