DSS Monthly Newsletter
February 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.

DSS is starting to train the field on DiT, which is based on knowing the assets at each facility, establishing tailored security plans, and applying appropriate countermeasures based on threat. DSS is now rolling out the new process in an incremental way that educates both DSS personnel and industry partners as the process is continuously evaluated and improved.

As part of a phased implementation, four facilities were selected by DSS to participate in the first phase of implementation of DiT and will be the first four industry partners to complete the entire DiT process outside of the direct supervision of the Change Management Office. Upon completion of these assessments, DSS will 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.

By the end of the year, DSS anticipates the majority of DSS personnel will be trained on the new approach, approximately 60 facilities will have had a comprehensive security review and resulting in a tailored security plan, and the process will have been significantly refined along the way. For those facilities not involved in the DiT implementation, we will prioritize our engagements in accordance with the Department's priorities, and then allocate our limited resource to assess and rate the facilities using the traditional security vulnerability assessment (SVA) model… with some enhancements. The enhancements include asking facilities to assist in

the identification and documentation of critical assets, collaborating on and documenting business processes and security measures around those assets, and educating facility security officials on a new threat assessment tool known as the "12x13" matrix. By implementing the enhanced SVAs, industry will have the tools and knowledge of the processes that will expedite the implementation of the DiT process when the rollout continues in FY19.

For more information on the DiT methodology, click here.

SECURITY EXECUTIVE AGENT DIRECTIVE 3 (SEAD 3) STATUS

On December 14, 2016, the Director, National Intelligence signed Security Executive Agent Directive 3, "Reporting Requirements for Personnel with Access to Classified Information or Those Who Hold a Sensitive Position," (SEAD 3), which establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position. This Directive applies to any executive branch agency including the military departments.

While the Directive has an effective date of June 12, 2017, these requirements will not apply to cleared industry under the National Industrial Security Program (NISP) until guidance is developed and implemented through NISP policy. The process of policy development is underway and cleared industry will be advised as information becomes available on implementation of SEAD 3 requirements once established by NISP policy.

NISP AUTHORIZIATION OFFICE (NAO) MEMORANDUM OF UNDERSTANDING (MOU) GUIDANCE

The NAO provides a template for MOUs to facilitate connections between government and contractor systems. This template has the appropriate signature block and references, and will be the most up-to-date approved version. The template can be found in the ODAA Bulletin Board within OBMS, under "Headquarters Bulletin Board." Industry is not required to use the DSS template; however, doing so may expedite the coordination and approval process.

MOUs should not be emailed directly to NAO as this will not result in faster approval and may significantly slow down the process.

All questions should be directed to your Information Systems Security Professional (ISSP).

DSS AUTHORIZED WARNING BANNER

Industry indicated that the DSS Authorized Warning Banner does not display as shown in the DSS Assessment and Authorization Process Manual (DAAPM). The issue is due to the use of the semi-colons. In order to resolve this matter, industry is authorized to use a comma in place of the semi-colon.

If you have questions or concerns, please contact your assigned ISSP or visit the DSS RMF Website. If you have specific questions about the format or content of the DSS Authorized Warning Banner, please provide comments and questions to dss.quantico.dss-hq.mbx.odaa@mail.mil**.**

AUTHORIZATION TO OPERATE (ATO) PACKAGE REMINDER

NAO reminds industry to get upcoming ATO packages into the process as far in advance as possible as it takes longer for the packages to get through the approval process utilizing the Risk Management Framework.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) FEBRUARY 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 ISFD and 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 no fewer than 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 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. 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.*

If you emailed the NISS Team Box (DSS.NISS@mail.mil) and have not received a response, we sincerely apologize for the delay. We are working through a backlog of emails and will respond as quickly as possible.

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 - logging into 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.

Thank you for your patience during this transition!

E-FCL NISP PSI DATA COLLECTION HAS BEEN EXTENDED

The DSS data collection of NISP Personnel Security Investigation (PSI) Projections is open and has been extended until March 2, 2018. It can be accessed through the DSS Electronic Facility Clearance (e-FCL) system. To submit your projections, please go to the e-FCL Submission Site. Each user has full access to the PSI area of the site for facilities for which they have active e-FCL accounts.

Upon logging-in, a list of facilities to which you have access within e-FCL is displayed, or you may click "Select an Organization" from the menu. Clicking on a facility's icon will display the Company Information page, which contains an icon for accessing the PSI area of the site.

For facilities new to e-FCL, the system requires the Tax ID number and business structure type to finalize the setup process; upon saving this information, the system will redirect the user to a page listing the five steps of an e-FCL Initial Package. As this is outside the scope of the PSI Data Collection, click “Select an Organization” from the menu and click your facility’s icon, which will display the PSI icon for submitting your projections.

Please note that submitting your PSI projections is independent of e-FCL package submissions; submitting information related to your facility clearance is not required as part of the PSI data collection.

If your e-FCL password has expired or you have forgotten it, enter your email address on the login page and click the "Reset Password" button.

Those using Internet Explorer to access e-FCL must use IE 11 and have Compatibility View turned OFF; click the instructions banner at the top of the e-FCL Submission Site page for directions to do this.

A 12-minute tutorial video can be found at Electronic Facility Clearance System (e-FCL) webpage (under "Alerts") to assist in completing the PSI projections. For the best viewing of this video, please save it to your computer (hover the cursor over the link on the web page, and right-click to "save target as ..."). It can be viewed using Windows Media Player, QuickTime, and VLC Player.

We look forward to your participation. If you have any questions, please contact the PSI team at: dss.ncr.dss.mbx.psiprogram@mail.mil.

TIER 5 REINVESTIGATIONS (T5Rs) REMINDERS

Effectively immediately, industry should submit all T5Rs whose investigation close date is 6 years or older. Caveat T5Rs should continue to be submitted at the five year mark.

This is a DSS reminder regarding the Jan. 6, 2017, "Notice of six year submission window for contractor periodic reinvestigations." The temporary change in periodicity from 5 to 6 years for T5Rs will remain in effect until notified otherwise. Facility security officers should continue to submit T5Rs at the 6-year periodicity mark. Previously established exceptions will remain in effect. This will result in T5Rs continuing to be within the 7-year reciprocity guidelines.

The Office of the Undersecretary of Defense for Intelligence (OUSD(I)) signed a memorandum on Dec. 7, 2016, which reminded DoD Components that personnel security clearances that do not expire, remain in effect. Individuals with current eligibility in the Joint Personnel Adjudication System (JPAS) should not be denied access based on an out-of-scope investigation. When the system of record shows current adverse information, but eligibility is still valid, access may continue. The memorandum is provided here for ease of reference.

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 JPAS.

You can confirm that the National Background Investigations Bureau (NBIB) has processed the fingerprints by checking SII in JPAS which indicates a "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 Personal Security Clearance (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.

THE DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) WILL DEPLOY TO MILDEPS ON JANUARY 8, 2018

The Jan. 8, 2018 deployment of DISS to the Military Departments began Phase I of the deployment schedule and major activities in Phase I include migration to a single adjudicative system and interfaces with the JPAS, NBIB systems, the Clearance Verification System (CVS), the Personnel Data Repository (PDR), and the Defense Central Index of Investigations (DCII). As of January 8, completed investigations will be adjudicated in DISS while investigations completed prior to Phase I deployment will be worked in legacy systems. You can view the DISS deployment phases here.

Deployment to industry is scheduled for May 2018. The DMDC Contact Center is available for DISS user support at 1-800-467-5526, option #1

CLARIFICATION ON REPORTING REQUIREMENTS FOR CRYPTOCURRENCIES

DSS has fielded a number of questions from industry as to whether ownership of cryptocurrencies, such as Bitcoin, should be reported by cleared persons or clearance applicants. There is no current DoD guidance related to the reporting of ownership of cryptocurrencies. DSS is working with DoD policy offices for further clarification and once such guidance is issued, DSS will ensure the widest dissemination to industry.

SECURITY EDUCATION AND TRAINING

NEW CI AWARENESS GAME NOW AVAILABLE

Looking for a fun way to encourage Counterintelligence awareness at your organization? Share CDSE's CI Trivia Twirl with your personnel. This popular game is a quick and easy way to remind the workforce of messaging associated with Counterintelligence awareness. Take it for a spin here.

MARCH CYBERSECURITY WEBINAR

CDSE invites you to participate in the live webinar "Top 10 Security Incidents of 2017" on Thursday, March 15, 2018, at 11:30 a.m. or 2:30 p.m. ET. This webinar will discuss the 10 most notable security incidents of 2017, and will explore the nature of the incident, its impact, and discuss ways that it could have been avoided.

Sign up today at CDSE Webinars.

INTELLIGENCE OVERSIGHT INFORMATION AVAILABLE IN CI TOOLKIT

Explore CDSE's New Intelligence Oversight tab that has been recently added to the Counterintelligence Awareness Toolkit. You will find direct links to policies and resources on Reporting Questionable Government Activities, which provides information on the Whistleblower Protection Act (PPD-19) that protects employees from direct retaliation for reporting protected disclosures. View the information under the new tab here.

ARCHIVED JANUARY INSIDER THREAT WEBINAR NOW AVAILABLE

Did you miss last month's "Insider Threat Programs: Engaging Management and Supervisors" webinar with special guest Mr. Keith Dixon, Department of Transportation Insider Threat Program Office? If so, you can now access the archived webinar. Insider Threat Programs must engage management and first line supervisors to ensure recognition of, and appropriate responses to, concerning behaviors. It was a great discussion on methods and techniques for working with this group to mitigate insider risks.

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.

SPECIAL ACCESS PROGRAM (SAP) SECURITY ANNUAL REFRESHER SA002.16

CDSE is pleased to introduce a new eLearning course, "The Special Access Program Security Awareness Refresher" course. This course assesses and refreshes the student's basic understanding on the fundamentals of SAP security as outlined in DoDM 5205.07 Volume 1-4.

Topics include:

- Personnel security
- Information security
- Physical security
- Transmission requirements
- Classified networks
- Document control
- Threats
- Operations Security

Access the new eLearning course here.

SAP VIDEO REFRESH

To keep security video learning fresh, the SAP Team posted two new e videos:

- SAP Security Incident – The Email: As a cleared employee or an FSO of a defense contractor, you could be the target of a request for information or direct request email. Watch the video to learn about a recent case involving illicit information collection by a foreign adversary. Then, follow the links to test your knowledge, and learn more.

- SAP Security Incident – Bad Start: Some days it seems like things start off bad and continue to go downhill from there. Take a look at this video and see if you can identify what went wrong. Stop and think about what could be done to help prevent scenarios like this from happening in your program.

The videos will be refreshed in June. Check out our latest offerings at Security Training Videos.

NEW CASE STUDIES AVAILABLE

CDSE recently released new Counterintelligence and Insider Threat Case Studies:

- Counterintelligence Case Study – Attempted Acquisition of Technology- Radiation Hardened Integrated Circuits

- Insider Threat Case Study – Gregory Justice

These case studies can easily be included in an organization's security education, training, and awareness programs. These case studies are suitable for printing or easy placement in a company or command newsletter, email, or training bulletin. Access the new case studies today!

UPCOMING SPEAKER SERIES

Join CDSE for our March Speaker Series:

- **DoD Unauthorized Disclosure Program Manager**
  Thursday, March 22, 2018
  12:00 p.m. ET

  The unauthorized disclosure (UD) of classified and CUI undermines the DoD mission, costs DoD resources, and erodes the public's confidence and trust. In 2012, DoD established a "top down" approach to the identification, investigation, and reporting of UDs. The UD Program Management Office (PMO) was established within OUSD(I). CDSE hosts a discussion with DoD UD PMO.

- **Applied Research on Social Media and Security**
  Thursday, March 29, 2018
  12:00 p.m. ET

  Since 2009, the Defense Personnel and Security Research Center has studied publicly available social media as a data source for personnel security background investigations. While pilot studies have demonstrated the utility of this information, there are a number of legal and privacy concerns, and procedural requirements that must be addressed before social media information can be integrated into the DoD personnel security program. CDSE hosts a discussion with Ms. Andree Rose of the Defense Personnel and Security Research Center.

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:

April 3-4, 2018, Atlanta, GA, go here

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