DSS Monthly Newsletter
April 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. DSS field personnel were provided with comprehensive training of the new DiT methodology at DSS Operational Training Events in April.

Also in April, the DSS Industrial Security Field Operations Program Management Office established the Implementation Program Review Board (IPRB). The IPRB is responsible for overseeing DiT project areas to ensure new processes are clearly documented, supported by technology, trained, and implemented while ensuring stakeholders are proactively informed and engaged. 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 concluded in early April and DSS completed several after action reviews, the final of which was conducted on April 18. DSS is now in the process of incorporating lessons learned

from the first phase into future phases and will continue to use expertise and insights gained to improve the process throughout the year.

In April, DSS Field Offices validated the list of cleared facilities associated with the Department's top priority technologies and determined 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 Industrial Security Representative 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 for 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.

GUIDANCE FOR SECURITY EXECUTIVE AGENT DIRECTIVE 4 (SEAD 4)

DSS provides updated guidance for cleared contractors on the implementation of SEAD 4 in relation to the disposition of foreign passports belonging to cleared employees.

On December 10, 2016, the Director of National Intelligence signed SEAD 4, "National Security Adjudicative Guidelines," which became effective on June 8, 2017. SEAD 4 establishes the single common adjudicative criteria for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. The guidelines reflected in the SEAD 4 supersede all previously issued national security adjudicative criteria or guidelines. The SEAD 4 guidelines may be found here.

This guidance provides for Industry implementation of the SEAD 4 Adjudicative Guidelines related to the disposition of foreign passports belonging to cleared employees that have been retained by contractors in accordance with prior DoD directions or decisions under the former Adjudicative Guidelines. In accordance with SEAD 4, cleared contractors will not be asked by the DoD Consolidated Adjudications Facility (CAF) to routinely retain or destroy foreign passports and/or identity cards as a means of mitigating security concerns for individuals who maintain dual citizenship with other countries.

In order to implement SEAD 4, cleared contractors who have retained a cleared employee's foreign passport or identity card based on prior DoD directions or personnel security adjudicative decisions should return the foreign passport or identity card to the cleared employee.

Upon returning the foreign passport or identity card to the cleared employee, the facility security officer, or designated JPAS user acting on behalf of the contractor, will remind the cleared employee of their responsibility to enter and exit the United States using a U.S. passport.

The cleared contractor will submit incident reports if any cleared employees report use of a foreign passport to enter or exit the United States.

NEW DD FORM 254

A new DD Form 254, "Department of Defense Contract Security Classification Specification," has been published. On April 19, 2018, Washington Headquarters Services posted the new DD Form 254 and supporting instructions to the "DoD Forms Management Program" website. The new form is more user friendly and some new features include:

- Lengthening of classification text fields
- After entering a classification, the remainder of the classification fields automatically fill
- Capability for users to have certain items expand (instead of having to select "add page")
- Digital signature capability for internal reviewers in item 13
- Ability to add attachments before the final approver signs in item 17h
- Date automatically fills in item 17i when final approver digitally signs in item 17h
- Instructions have been updated to provide guidance on how to expand certain text fields as well as how to print the completed form.

The form can be found at DD Form 254 and the instructions can be found at DD 254 Instructions.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

DSS has been working diligently to deploy a fully-operational NISS, including efforts to resolve account registration and access issues. We appreciate your patience as we complete this top agency priority and deliver its capability as quickly as possible.

Currently, NISS remains in a soft launch, test state to allow users to log in and become familiar with NISS functions for their day-to-day jobs. The NISS soft launch period also allows end-users to report bugs and issues to DSS. Every issue reported helps DSS test and fix the system prior to full operational release. Once it is determined that all critical issues have been resolved, DSS will provide 30 days' notice to the user community to prepare for the full transition to NISS.

We intend to make NISS the system of record in mid-June, but the exact date has not yet been determined. In the coming weeks, DSS will make a decision on the exact cutover date and provide additional instructions to the user community about this transition. Until then, official business will still be conducted in the Industrial Security Facilities Database (ISFD) and the Electronic Facility Clearance System (e-FCL), which remain the official systems of record.

For the following Account Registration/Access Issues, please send your name, email address, and CAGE Code to DSS.NISS@mail.mil. Clearly state the issue and attach screen shots of any error messages. If you have already provided your information for either error and received a response from DSS, you do not need to resubmit the information.

1) 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".
2) 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).

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

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

Thank you for your patience during this transition!

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 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 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.

FOR THOSE REQUESTING INVESTIGATION/ADJUDICATIVE RECORDS FROM DSS

Freedom of Information Act/Privacy Act (FOIA/PA) requests for investigative or adjudicative records maintained in the Investigative Records Repository (IRR), Defense Central Index of Investigation (DCII), Secure Web Fingerprint Transmission (SWFT), or Joint Personnel Adjudication System (JPAS) IT systems should be submitted to the DMDC Office of Privacy at:

Defense Manpower Data Center
ATTN: Privacy Act Branch
P.O. Box 168
Boyers, PA 16020-0168

DSS no longer maintains any personnel security investigative records, to include clearance adjudicative records, JPAS, and SF-86s (e-QIP) on DoD employees or DoD contractor personnel. For further information, please visit the DSS FOIA website here.

PREPARE FOR DISS

In preparation for accessing the Defense Information System for Security (DISS) portal, the Personnel Security Management Office for Industry (PSMO-I) offers Preparing for DISS - Clean Up Your SMO.

SECURITY EDUCATION AND TRAINING

VOICE OF THE CUSTOMER SURVEY

The Center for Development of Security Excellence (CDSE) strives to create the most up-to-date and relevant security products and services. Your feedback is extremely important and will help us enhance our offerings and remain current, accurate, and relevant in this dynamic security environment.

Please take a few minutes to fill out this survey to provide feedback.

UPCOMING SFPC AND SAPPC REVISIONS

An innovative pilot to test assessment items for Security Fundamentals Professional Certification (SFPC) and Security Asset Protection Professional Certification (SAPPC) concluded on Mar 2. A total of 213 certified and non-certified candidates participated in the pilot. These items will be filtered into the SFPC and SAPPC assessments for publication in September. Learn more about the SFPC and SAPPC Certifications at the About SPeD Certification website.

COUNTERINTELLIGENCE CASE STUDIES AVAILABLE AT CDSE

Take a look at CDSE's CI case study - Attempted Acquisition of Technology Radiation Hardened Integrated Circuits. Our adversaries have significantly closed the gap in space platform technology with the U.S. through their aggressive and successful attempts in obtaining U.S. technology. One of the hottest targets in the past few years has been Radiation Hardened Integrated Circuits (RHIC). In this study, a Texas company owner was sentenced to 46 months in prison and fined $50,000 for a conspiracy to smuggle and illegally export RHICs to foreign entities. Read the rest of the case study here.

UPDATED INDUSTRIAL SECURITY COURSES

CDSE will be relaunching three updated Industrial Security courses. Check out NISP Reporting Requirements, Introduction to Industrial Security, and Visits and Meetings in the NISP. The courses were updated to incorporate new policy, remove out-of-date material, and to give the courses an updated look. All three courses will be available May 1.

Access each course through STEPP.

SUPPLY CHAIN RISK MANAGEMENT (SCRM) FOUNDATION/FRAMEWORK

April was Supply Chain Integrity Month. Increased risk to supply chains are due to evolving dependence on globally-sourced commercial information and communication technologies (ICT) and other components of mission critical systems and services. Resultant residual risks are passed to end-user enterprises in the form of products and services that may contain defective, counterfeit, or otherwise tainted components with malware, exploitable weaknesses, and vulnerabilities from sources with unknown trust.

SCRM is a systematic process for managing this risk by identifying vulnerabilities and threats throughout the "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the distribution chain. You can learn more about the Supply Chain Risk Management Framework with the links in our SCRM toolkit.

NEW KINETIC VIOLENCE TAB

CDSE developed a new tab on the Insider Threat Toolkit! The tab provides resources on training, policy, and best practices regarding Kinetic Violence. Check it out here.

UPCOMING WEBINARS

CDSE invites you to participate in our upcoming webinars:

- **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.

UPCOMING SPEAKER SERIES

Join CDSE for our May Speaker Series:

- **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.

ARCHIVED WEBINARS AND SPEAKER SERIES NOW AVAILABLE

Did you miss last month's Speaker Series "DoD Unauthorized Disclosure Program Manager" or "Applied Research on Social Media"? If you missed the Industrial Security discipline's first of a series of Speaker sessions regarding various DSS missions, don't worry. You can catch the "Let's talk about FOCI" Speaker Series, March sessions, and the "Key Management Personnel Security Clearances" webinar, in our archives.

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