DSS Monthly Newsletter
December 2017

(Sent on behalf of your ISR.)

Dear FSO,

This is the monthly newsletter containing recent information, policy guidance, 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)

DSS is changing. Where the Agency once concentrated on schedule-driven NISPOM (National Industrial Security Program Operating Manual) compliance, DSS is now moving to an intelligence-led, asset-focused, and threat-driven approach to industrial security oversight.

To achieve this, the Agency started the second of two planned Practical Exercises in November 2017 to operationally test the integrated Concept of Operations (CONOP) for DiT methodology. The Methodology Development Team (MDT) met with personnel in the Huntsville, AL, Field Office and with the cleared contractor facility selected to participate in the second exercise.

As we conclude the Practical Exercises, we will look to expand the new methodology to a larger audience and encourage Industry to identify both the assets at their facilities as well as the security controls they have implemented to establish a Security Baseline. This will set the foundation for developing a Tailored Security Plan in collaboration with DSS. Starting Asset Identification will help DSS to provide more timely, relevant threat information to contractors.

Both Practical Exercises are expected to conclude in February 2018.

Following the completion of the Practical Exercises, we will begin conducting the first phase of implementation at selected facilities in each region to further refine and document the process. Following each implementation phase, we will take a pause to capture lessons learned and make modifications as we continue to expand both Industry and DSS understanding of the process while implementing the new end-to-end process.

For more information on the DiT methodology, click here.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) EXTERNAL TRAINING COURSE AVAILABLE & REGISTRATION UPDATE

DSS has launched the "NISS External User Training Course" in STEPP (Course ID: IS127.16). This course is currently optional but will become a required part of the FSO Curricula (replacing Industrial Security Facilities Database (ISFD) and Electronic Facility Clearance System (e-FCL) training) when NISS becomes the system of record. For more information about the course, click here.

Industry members may continue to register for NISS accounts. To date, over 800 Industry roles have been approved. We have received feedback that some Industry members are unable to register for the NISS Application. DSS is actively working to resolve this issue and will notify the impacted users when the issue is resolved.

If an Industry member encounters an error in the National Industrial Security Program (NISP) Central Access Information Security System (NCAISS) when registering for their NISS account ("An error occurred while determining the approver for the CAGE Code specified."), please send an email to DSS.NISS@mail.mil with the CAGE Code and the assigned DSS Industrial Security Representative. We will remedy this issue and provide a direct notification when fixed. All other questions should be directed to the DSS Knowledge Center (888-282-7682).

For more information about NISS, please visit the NISS Website. Thank you for your continued support and patience during the transition!

SUBMITTING SELF-INSPECTION CERTIFICATIONS IN E-FCL FOR CY 2018

On Jan. 1, 2018, Industry members will be able to submit self-inspection certifications in e-FCL for calendar year (CY) 2018. Beginning in the New Year, Industry members should only submit self-inspection certifications if they occurred after Jan. 1, 2018. Additionally, after the New Year, Industry members will not be able to use e-FCL to report self-inspection certifications for the prior year (CY 2017). If after the start of 2018 you need to submit a self-inspection certification for CY 2017, please contact your assigned DSS Industrial Security Representative (ISR). For any other questions, please contact your assigned DSS ISR.

NISP AUTHORIZING OFFICE (NAO)
REMINDER: PKI TOKENS ARE REQUIRED FOR SIPRNet CONNECTIONS

Effective Oct. 1, 2017:

a) All DoD sponsors of contractor-site SIPRNet connections must obtain SIPRNet PKI tokens for their cleared contractors. User names and passwords will no longer be used.

b) All DoD sponsors of contractor-site SIPRNet connections using Microsoft Active Directory (AD) must configure these connections to require user network crypto-logon with DoD SIPRNet PKI tokens.

c) All users of contractor-site SIPRNet connections must use PKI tokens to authenticate to websites and applications.

d) All Command Cyber Readiness Inspections will check for compliance with these requirements.

Non-compliance may result in the loss of SIPR connectivity.

For additional information on SIPRNet PKI, please see the Defense Information Systems Agency SIPRNet PKI webpage.

Please contact your assigned Information System Security Professional (ISSP) with any questions or concerns regarding the implementation of this requirement.

ANNUAL NATIONAL INDUSTRIAL SECURITY PROGRAM COST COLLECTION

As the Executive Agency for the National Industrial Security Program (NISP) under Executive Order 12829, the Department of Defense is required to provide the Information Security Oversight Office (ISOO) with an estimated annual cost to Industry of complying with NISP security requirements. We determine the costs by surveying contractors who possess classified information at their cleared facility. Results are forwarded to ISOO and incorporated in an annual report to the President.

To meet this requirement, DSS conducts a stratified random sample survey of contractor facilities using a web-based survey and Office of Management and Budget (OMB)-approved survey methodology. Since the sample of cleared facility participants is randomly selected, not all facilities will receive the survey. The survey will be fielded on Jan. 16, 2018 and remain open through COB Jan. 29, 2018. Participation is anonymous. The survey invitation will contain a foresee.net survey link. Verification of the legitimacy of the Survey URL can be obtained through your Cognizant Security Office. Please direct any questions to dss.ncr.dss.mbx.psiprogram@mail.mil.

We appreciate your cooperation and submission of the cost information by Jan. 29, 2018.

IMPACT OF REAL ID ON NISPOM CLEARED INDUSTRY CONTRACTORS

The REAL ID Act established minimum security standards for license issuance and production, and prohibits Federal agencies from accepting driver's licenses and identification cards from states not meeting minimum standards. The Act covers all U.S. states and territories (collectively referred to as "States" in the Act). As of the date of this VOI Newsletter, the Department of Homeland Security (DHS) REAL ID Website cites an implementation date of Jan. 22, 2018, however, information in the public domain indicates that this may change.

The Act may affect your ability to fly in the U.S. and enter Federal and Military facilities or sites. It does not influence or affect the verification of security clearances or employment status. It will impact anybody who will board a federally regulated aircraft.

A current U.S. Passport is the most universally accepted ID, followed by DOD military (active/ reserve/retired/dependent) and Federal Contractor CAC/ID cards (however, your CAC is only to be used for Government business, and recommend you check with your company program manager and Government COR to ensure appropriate use of your CAC under your contract).

Check the Department of Homeland Security (DHS) REAL ID Website to see if your state is compliant (or has an extension) and to ensure you follow the most current DHS approved guidance.

To Board a Federally Regulated Commercial Aircraft - If your state is compliant (or has an extension), then you can use your state ID. If your state is not compliant, then check the TSA list here to see acceptable alternative IDs.

NOTE – As of the implementation date (Jan. 22, 2018 as of press time), IDs issued by non-compliant states will not be accepted to board federally regulated aircraft. If you reside in a non-compliant state and do not possess an acceptable alternative ID, you are strongly encouraged to get a U.S. passport as soon as possible.

To Access a Federal Facility or Site - Ahead of your visit, contact the security office at the destination agency/site to determine what forms of ID are required and acceptable. Also recommend that you contact the security office to process or validate your visit clearance and security clearance passage instructions to ensure that you and they are prepared for your visit. (Some agencies and sites require more than one ID and have additional access restrictions (such as the Pentagon)). If your state is compliant with the REAL ID Act, then your state ID will be one acceptable form of ID. For official government business under your contract, your Federal Contractor CAC will serve as a second optional approved ID.

REMINDER: USE THE MALWARE RELATIONSHIP TRIAGE TOOL (MRETT) TO SUBMIT SUSPICIOUS FILES

Due to the recent malicious attachments sent to DSS Counterintelligence Special Agents (CISAs), cleared contractors are reminded to submit suspected malicious files only to MReTT.

Do not forward suspected malicious files anywhere because doing so only further spreads the problem and/or infects the networks of others.

NOTE – Prior to submitting files to MReTT, please coordinate with your FSO to review for potential classified or controlled technology information, recruitment attempts, illegal acquisition or elicitation.

Suspected malicious attachments should be sent to MReTT as follows:

1. Create a New Email message.
2. To Line: submit@dss.apiary.gtri.org.
3. Subject Line: ABC12 (Note: Subject Line must include a valid CAGE Code to be processed).
4. Copy the suspected malicious email message with attached file(s) to the new email message. The steps may vary depending on which email application you use.
5. Send the email message Unencrypted.

Once the suspected malicious attachment is sent to MReTT, the cleared contractor and local DSS CISA will receive an automatic email reply from MReTT indicating if the submission was either successfully ingested or rejected. If the submission was rejected, forward the rejection email (NOT the malicious email) to the local DSS CISA, who will work with the DSS Cyber Team to ensure that the submission issue is resolved.

Suspected malicious hyperlinks should be forwarded to your responsible DSS CISA to be submitted to MReTT on your behalf. (Submitting hyperlinks via email to MReTT will not work and will likely get rejected.)

MReTT can ingest and analyze the following file types: /bin/sh scripts, ace, android, bash script, cab, cdf, coff, elf, generic archive, generic script, gzip, html, image, mach-o, mpeg, ms-dos, msa, office, pdf, pe, perl script, posix script, python script, rar, riff, rtf, ruby script, url, and zip.

DISS DEPLOYMENT UPDATE

The Defense Information System for Security (DISS) will deploy to MILDEPS on Jan. 8, 2018.

The Jan. 8, 2018 deployment of DISS to the MILDEPS will begin Phase I of the deployment schedule and major activities in Phase I include migration to a single adjudicative system and interfaces with the Joint Personnel Adjudication System (JPAS), National Background Investigation Bureau (NBIB) systems, the Clearance Verification System (CVS), the Personnel Data Repository (PDR), and the Defense Central Index of Investigations (DCII). Beginning on January 8th, completed investigations will be adjudicated in DISS, while investigations completed prior to Phase I deployment will continue to be worked in legacy systems. The DISS deployment phases may be viewed 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

TIER 5 REINVESTIGATIONS (T5Rs) UPDATE

This is a DSS update to 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 signed a memorandum on Dec. 7, 2016, which reminded DoD Components that personnel security clearances do not expire, remains in effect. Individuals with current eligibility in 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 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 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.

SECURITY EDUCATION AND TRAINING

NEW INSIDER THREAT CURRICULA

The Center for Development of Security Excellence (CDSE) is proud to announce the release of two new Insider Threat Curricula. These Curricula combine Insider Threat courseware with Counterintelligence and Security Fundamentals training to meet National Minimum Standards for Insider Threat Hub personnel. Register today to complete this suite of training and a comprehensive final exam to earn your certificate of completion.

- The Insider Threat Program Operations Personnel Curriculum, INT301.CU, is found here
- The Insider Threat Program Management Personnel Curriculum, INT302.CU, is found here.

UPCOMING INSIDER THREAT SPEAKER SERIES

Join CDSE on Thursday, Jan. 11, 2018 at 12:00 p.m. ET for the “Insider Threat Programs: Engaging Management and Supervisors” webinar. Insider Threat Programs must engage management and first line supervisors to ensure recognition of and appropriate response to concerning behaviors. Join special guest Keith Dixon, Department of Transportation Insider Threat Program Office, for a discussion on methods and techniques for working with this group to mitigate insider risk. Sign up today at CDSE Webinars.

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

ARCHIVED CI AND INSIDER THREAT WEBINAR NOW AVAILABLE

Did you miss our recent webinar, "Counterintelligence and Insider Threat Training Products?" If so, the webinar recording is now available in our archive here. Watch and learn about the many different Counterintelligence and Insider Threat training products available at CDSE. New products added to our library of materials over the past year include our popular eLearning courses and numerous job aids, videos, posters, micro videos, case studies, and other items. Take a few minutes to see what we have to offer and how to find it on our website.

SPēD CERTIFICATION MAINTENANCE REMINDER

Don't forget to submit your form! Please visit the CDSE website to complete and submit your Certification Renewal Form to extend your certification. Failure to submit will cause your certification to expire. For more information, login here.

SAPPC PILOT IS LIVE

Pilot testing for SPēD assessment items has begun and volunteers are needed. SPēD certificants holding at least a Security Fundamentals Professional Certification (SFPC) & Security Assets Protection Professional Certification (SAPPC) are eligible to earn 12 Professional Development Units (PDUs) in one afternoon by reviewing and validating new SPēD assessment items. To register, please follow the instructions below:

1. Log in to My SPēD Certification (MSC) account
2. Select "Complete A Form Option"
3. Choose "SAPPC Pilot Request"
4. From the "New Forms" tab, select, complete, and submit your Assessment Request Form.
5. Schedule your test once you receive the email notifying you that your request has been approved.
6. After you have scheduled your appointment, you will receive a confirmation email with important information for test day, including directions to the test center.

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:

Apr. 17-18, 2018, Atlanta, GA, go here

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

We will also be offering this class at CDSE in Linthicum, MD on Feb. 13-14 and 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