DSS Monthly Newsletter
November 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 in Transition is a multi-year and enterprise-wide initiative. It is designed to move the agency from a focus strictly on NISPOM (National Industrial Security Program Operating Manual) compliance to an intelligence-led, asset-focused, and threat-driven approach to industrial security oversight.

The DiT efforts have been branded under the tagline, "Partnering with Industry to Protect National Security." To help transform this sentiment into reality, DSS has coordinated with NISPPAC (National Industrial Security Program Policy Advisory Committee) and assembled a focus group of 40+ volunteers from Cleared Industry. Their objective is to provide ongoing feedback through a series of quarterly webinars on the development of the new DSS methodology and the effectiveness of DiT communication efforts.

The third webinar in this series was held on Nov. 2, 2017. Its purpose was to:

- present an overview of the Asset Identification component of the new DSS methodology
- outline current Asset Identification initiatives
- detail the way ahead to develop the Asset Identification component of the new DSS methodology
- solicit questions, thoughts, and comments about the specific subjects being discussed.

The complete webinar may be viewed here.

More information about DiT may be found here.

NISS DEPLOYMENT UPDATE, ISFD/E-FCL TRANSITION

The National Industrial Security System (NISS) is currently in a "soft launch" test state. We are pleased to announce that, following successful testing, Industry can begin registering for NISS accounts on Nov. 29, 2017. Industry account requests will be routed to the facility's assigned DSS Industrial Security Representative (ISR) for action. For more information about how to register for a NISS account, please visit the NISS Website and find the "Registration" section. NISS will remain in the soft launch TEST STATE ONLY until DSS resolves all critical application issues. Industrial Security Facilities Database (ISFD) and Electronic Facility Clearance System (e-FCL) remain the systems of record. Industry members are encouraged to begin registering for accounts on Nov. 29, 2017 in order to become familiar with the system and provide system feedback using the in-system "Submit System Feedback" functionality. For more information about this transition, visit the NISS Website or contact DSS.NISS@mail.mil.

DISS DEPLOYMENT UPDATE

The Defense Information System for Security (DISS) is a family of systems that will serve as the system of record for comprehensive personnel security, suitability, and credential management of all DoD military, civilian, and contractor personnel. Comprised of two components, the Case Adjudication Tracking System (CATS) and the Joint Verification System (JVS), DISS will replace the Joint Personnel Adjudication System (JPAS). DISS is currently undergoing a phased deployment. Industry deployment is currently on schedule for May 2018 and training will commence Mar. 2018. Additionally, user provisioning is on schedule for all components. All hierarchy and account managers will be provisioned NLT 30 days prior to deployment.

NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) AUTHORIZING OFFICE (NAO)

On Nov. 17, 2017, the DSS NAO released the DAAPM Version 1.2 with updated System Security Plans (SSPs). The updated documents are posted on the DSS Risk Management Framework (RMF) Information and Resources Website.

The early release is intended to provide Industry with time to review the manual prior to the effective date of Jan. 1, 2018. Starting then, all Information Systems (IS) requiring authorization or re-authorization must use the manual and the RMF process. DSS has previously allowed certain IS to operate without Formal SSPs (and UIDs), and these systems, which previously did not require formal accreditation, should now be submitted formally under RMF in 2018.

If you have questions or concerns, contact your assigned Information System Security Professional (ISSP). Specific questions about the format or content, or general comments, may be provided to dss.quantico.dss-hq.mbx.odaa@mail.mil.

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.

NEW DD FORM 254, "DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION"

The new DD Form 254, "Department of Defense Contract Security Classification Specification," has been published. On Nov. 1, 2017, Washington Headquarters Services posted the new DD Form 254 and supporting instructions to the "DoD Forms Management Program," website.

DSS will continue to accept DD Form 254s that were initiated using the old form for the next 90 days. After this time, all new DD Form 254s should be created using the new form.

The DD Form 254 is found here.

The DD Form 254 Instructions are found here.

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) and will be fully implemented Jan. 22, 2018.

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 and to see the most current DHS approved guidance. Further information may be found in the REAL ID Act of 2005 Implementation: An Interagency Security Committee Guide (August 2015/1st Edition) here.

To Board a Federally Regulated Commercial Aircraft - If your state is compliant, 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 Jan. 22, 2018, non-compliant IDs issued by 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.

REMINDER ON TIMING FOR ELECTRONIC FINGERPRINT TRANSMISSION

Reminder! 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 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.

SECURITY EDUCATION AND TRAINING

NEW CYBERSECURITY COURSES

The Center for Development of Security Excellence (CDSE) is pleased to announce the release of the four new eLearning courses:

- Information systems used by cleared contractor companies play a vital role in our nation's security and DSS must ensure that these systems operate at an acceptable level of risk. These two A&A courses were specifically developed in response to DSS's transition to RMF to provide guidance and assistance in assessing and authorizing those systems:
    - Introduction to NISP RMF A&A Process - CS150.16
    - Applying A&A in the NISP - CS250.16

- Cybersecurity for Security Personnel - CS160.16 provides security personnel with an understanding of their role in Cybersecurity and imparts a baseline understanding of the cybersecurity concepts as they particularly apply to security personnel.

- Protected Distribution System - CS140.16 describes the requirements and responsibilities for the approval, installation, inspection, and operation of a Protected Distribution System (PDS).

All four courses are available at CDSE Catalog Cybersecurity.

NEW INSIDER THREAT eLEARNING COURSES

CDSE recently released four new Insider Threat eLearning courses to equip Insider Threat Program Management and Operational personnel with the knowledge, skills, and abilities to manage an Insider Threat Program (ITP).

- Insider Threat Mitigation Responses - INT210.16 identifies viable response options to security violations or infractions, including administrative actions and referrals to Human Resources (HR), the Employee Assistance Program (EAP), law enforcement, and/or the appropriate supporting counterintelligence organization.

- Preserving Investigative and Operations Viability in Insider Threat – INT220.16 instructs personnel to appropriately manage incident responses and other ITP actions within the scope of their authority, to properly handle evidence and apply the chain of custody to properly identify and report exculpatory information, to appropriately report and refer insider threat information, and to understand the consequences of a poorly executed insider threat response.

- Developing Multidisciplinary Insider Threat Capability – INT201.16 covers how to assemble a multidisciplinary insider threat team of subject matter experts capable of monitoring, analyzing, reporting, and responding to insider threat incidents.

- Insider Threat Records Checks – INT230.16 teaches personnel to conduct their duties under the data collection requirement of DoD Directive 5205.16, Insider Threat Program.

Access the new courses at CDSE Catalog Cybersecurity.

NEW CI AND INSIDER THREAT SECURITY VIDEOS

CDSE has posted four new Counterintelligence (CI) and Insider Threat videos at CDSE Security Training Videos:

- Counterintelligence and Insider Threat Support to Security - Counterintelligence, Insider Threat, and Security work together to manage risk in support of national security. Learn how CI and Insider Threat awareness can support your security program and discover resources for training your organization.

- Know the Risk - Raise Your Shield: Supply Chain Risk Management - SCRM is a systematic process for identifying, assessing, selecting, and implementing risk management principles and mitigating controls throughout organizations to help manage supply chain risks. Watch the video, then follow the links to test your knowledge, and learn more

- Insider Threat Program for Senior Leaders - Federal and DoD policies establish minimum standards for ITPs in government agencies, DoD Components, and Cleared Industry. This video provides an executive-level summary of these requirements in under eight minutes.

- Insider Threats to Cybersecurity - The internal cyber threat is different from other insider threat challenges faced by your organization and requires specific strategies to prevent and address them. Watch the video, then follow the links to test your knowledge, and learn more.

UPCOMING CI AND INSIDER THREAT WEBINAR

Join CDSE on Thursday, Dec. 7, 2017 at 12 p.m. ET for the "Counterintelligence and Insider Threat Training Program" webinar. This webinar will cover the many different CI and Insider Threat training products available at CDSE. There have been several new products added to our library of materials over the past year. These include not just our popular eLearning courses but also numerous Job Aids, Videos, Posters, Micro Videos, and Case Studies, as well as others. We'll take a few minutes telling you what we have to offer and how to find it on our website. 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:

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!

INDUSTIAL SECURITY OVERSIGHT CERTIFICATION (ISOC) ACCREDITATION

The ISOC was accredited by the National Commission for Certifying Agencies (NCCA) in Nov. 2017, ensuring all security professionals who earn the credential meet the highest industry standards and have the knowledge and experience to carry out industrial security oversight tasks and successfully protect our nation's assets. ISOC is the fifth certification to achieve accreditation. Learn more about the ISOC here.

DOD SECURITY SKILLS STANDARDS (DS3) UPDATES

DS3 Version 9.1 was finalized in Nov. 2017. It included personnel security updates, insider threat changes, and policy link updates. The format was also changed to include a new numbering sequence to improve document handling flexibility. This is part of a new agile review process that is aimed to keep the DS3 up to date on policy and community practices.

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.

Thanks,
ISR
Defense Security Service