DSS Monthly Newsletter
September 2016

(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.

INSIDER THREAT IMPLEMENTATION

With the National Industrial Security Program Operating Manual (NISPOM) Change 2 updates promulgated on May 18, 2016, all cleared contractors under the National Industrial Security Program (NISP) must begin establishing the baseline requirements for an insider threat program. Your insider threat programs must be able to gather, integrate, and report relevant and available information indicative of a potential or an actual insider threat in accordance with NISPOM requirements. Additional resources and guidance on establishing your program may be found on DSS's Industry Insider Threat Information and Resources page and through the Center for Development of Security Excellence's (CDSE's) Insider Threat Toolkit. The Industry Insider Threat Information and Resources page also includes the balance of Change 2 requirements.

By November 30, 2016, you must accomplish the following:

- Establish your program;
- Appoint an Insider Threat Program Senior Official (ITPSO) who will finish ITPSO-specific training by November 30, 2016;
- Implement workforce training requirements related to insider threat; and
- Self-certify to DSS that your program can fulfill insider threat requirements.

NISPOM CHANGE 2, INSIDER THREAT WORKSHOPS

To further support the implementation of NISPOM Change 2, Insider Threat Program requirements, DSS will present a series of online workshops to continue discussions regarding program implementation and to provide information on NISPOM Change 2, Insider Threat Program requirements. For more information on the workshops, go to the DSS Industry Insider Threat Information and Resources webpage. Starting September 20, 2016, DSS will present a series of online workshops to further support industry in their implementation of NISPOM Change 2 requirements. During the workshops, DSS will answer questions and discuss establishment and maintenance of contractor insider threat programs. The first workshop was

conducted via Adobe Connect on September 20, 2016, and additional workshops will run through November 15, 2016. Register here.

Please contact dss.quantico.dss-hq.mbx.policyhq@mail.mil, if you have any registration difficulties.

The workshops will be held on Tuesdays from 1:00-2:30 p.m. The 2016 dates are as follows: September 20, 27; October 4, 11, 25; and November 1, 8, 15.

RESTARTING CHANGE IN REP NOTICES

In the second half of 2015, Industrial Security Field Operations (IO) lost its capability to distribute the Change In Rep Notice and VOI Newsletter through automated means. We were able to develop a manual solution for the VOI Newsletter; however, a solution for the Change In Rep Notices was far more difficult to develop, so the product was placed in a hold status until a viable solution could be developed. Starting the end of September 2016, IO will resume the distribution of the Change In Rep Notice through this temporary solution until the capability to automate the process has been restored. The Change In Rep Notice will be delivered through the same email address as the VOI Newsletter, so no adjustments to your spam filters will be required.

We thank you for your patience.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) AND NISP CONTRACT CLASSIFICATION SYSTEM (NCCS) EXTERNAL WEBSITES ARE LIVE

NISS is DSS's future information system architecture and will replace the Industrial Security Facilities Database (ISFD) and the Electronic Facilities Clearance System (e-FCL). It will provide capabilities to develop an on-demand, data-driven environment with automated workflows accessible to Industry and Government partners. NISS will also provide Industry and Government partners with a portal to interact and exchange data with DSS.

For more information, visit our NISS webpage.

The NCCS is an enterprise federal information system supporting government agencies and cleared companies in the NISP by facilitating the processing and distribution of the contract security classification specifications for contracts requiring access to classified information. NCCS establishes a centralized repository for the collection of this data while automating the DD Form 254 (DoD Contract Security Classification Specification) processes and workflows.

For more information, visit our NCCS webpage.

INTERNATIONAL WEBSITE UPDATED

The International Website has been updated. Please refresh your browser history to view the changes. Updates include new visit request forms, visit submission instructions, and security

assurance updates. The visit request forms have all been updated to include a new section requiring the security office to acknowledge whether the travelers will be hand carrying classified information. We will only accept the visit request forms located on our website. All other versions of the visit request form will be rejected.

For questions or concerns please email our office at dss.rfv@mail.mil.

REMINDER ABOUT UPCOMING ELECTRONIC FINGERPRINT DEADLINE

Effective October 1, 2016, all fingerprints associated with SON 346W must be submitted electronically to the Office of Personnel Management (OPM), or the fingerprint will be rejected. OPM will also reject any investigation request if an electronic fingerprint is not received within 14 days of request submission. Click here to view the electronic fingerprint capture options for Industry.

TIER 5 IMPLEMENTATION OF FEDERAL INVESTIGATIVE STANDARDS

In December 2012, the Office of the Director of National Intelligence (ODNI) and OPM jointly issued revised federal investigative standards for the conduct of background investigations for individuals that work for, or on behalf of, the federal government in order to bring consistency to investigative quality expectations. Effective Oct. 1, 2016, the Tier 5 investigation is being implemented as part of the phased approach for implementing the federal investigative standards. As a result, the Single Scope Background Investigation (SSBI) is being replaced with the Tier 5 investigation when Top Secret and SCI access to classified information are required.

Effective October 1, 2016, users may notice the Tier 5 investigations versus SSBI when reviewing investigative information in JPAS. For example, an investigation line may appear as "T5 From OPM, . . ." vice "SSBI From OPM, . . ."

Periodic Reinvestigation will be designated as "T5R" to represent Tier 5 Reinvestigation, instead of “SBPR.”

RESEARCH-RECERTIFY-UPGRADE (RRU) REQUESTS

The Personnel Security Management Office for Industry (PSMO-I) is overhauling the RRU process and is now only accepting RRU submissions via JPAS under the following three classifications:

- RESEARCH - Reciprocity Requests. PSMO-I will attempt to verify the eligibility via Scattered Castles/Central Verification System (CVS) prior to contacting the agency directly. If the eligibility is not verified in the available databases, a hardcopy reciprocity request will be submitted to the appropriate agency. Timeframes will vary depending on the action needed or agency response.
- RECERTIFY - Official government requests for information from DoD CAF, DOHA or DSS such as requests for information such as name changes, marriage to foreign nationals, follow-ups to Incident Reports, etc.

- UPGRADE - The FSO has reason to believe the eligibility line in JPAS is incorrect. For example: eligibility states Secret, but should be Top Secret, or it has a Loss of Jurisdiction (LOJ), but should be an eligibility, etc.

All other personnel security related questions and concerns should be directed to the DSS Knowledge Center at (888) 282-7682.

SECURITY EDUCATION AND TRAINING

NEW E-FCL JOB AID

CDSE has created the "Understanding Your e-FCL Submission Requirements" job aid. This job aid explains the various business documents and forms required for the NISP Facility Security Clearance (FCL) process using the e-FCL system. Access the job aid here.

NEW INSIDER THREAT JOB AID

CDSE has added the "Sample Insider Threat Program Plan" to its Insider Threat resources page. This job aid provides a sample plan to help the ITPSO draft a facility's Insider Threat Plan. The ITPSO may use this job aid to tailor their program to suit the size of their facility. Access the job aid here.

CDSE SECURITY SPEAKER SERIES TO FEATURE DSS COUNTERINTELLIGENCE (CI) DIRECTOR

On November 10th, CDSE will host a CDSE Security Speaker Series webinar featuring DSS Counterintelligence Director William Stephens. The webinar is intended for an audience of DoD enterprise and industry partner security personnel. Sign up today!

UPCOMING COUNTERINTELLIGENCE WEBINAR

Join DSS and CDSE for the "DSS 2016 Targeting U.S. Technologies – A Trend Analysis" Webinar on Thursday, October 13, 2016 as we discuss the latest trends in foreign targeting of U.S. defense technologies. Efforts to compromise or exploit cleared personnel, or to obtain unauthorized access to sensitive or classified information have been documented throughout the year. This unclassified format will provide analysis of methods of operation and targeted technology. Sign up today!

NEW DEFENSE INSIDER THREAT MANAGEMENT ANALYSIS CENTER (DITMAC) SHORT AVAILABLE

CDSE recently posted the "DITMAC" short. This product was developed in conjunction with the DITMAC to introduce DoD personnel to the DITMAC's role in the DoD Insider Threat Program. View the short here.

CDSE POSTS TWO NEW INSIDER THREAT CASE STUDIES

CDSE has released two new insider threat case studies to its collection of Insider Threat job aids.

- Hannah Robert pled guilty to violating Arms Export Control Act. She had transmitted sensitive military data to foreign contacts through a church website where she volunteered as a web administrator.
- Kun Shan Chun was a Federal Bureau of Investigation electronic technician who acted as a Chinese agent, and in multiple instances delivered classified information to Chinese contacts.

CDSE releases these job aids regularly to provide accessible, easy-to-follow training materials of recent cases that stress the impact of economic espionage, traditional espionage, and other national security crimes. Access the new and previously issued job aids here.

NEW SPECIAL ACCESS PROGRAM (SAP) SECURITY INCIDENT VIDEOS

Two new SAP related videos are now available: "SAP Security Incidents - Transportation" and "SAP Security Incidents - The Email." The intended audience for these scenario-based videos is civilian, military, and contractor personnel who work within the SAP environment. The videos highlight errors common to the SAP environment, and should be incorporated into SAP security training programs so that viewers can prevent these recurrent issues. Students are encouraged to apply critical thinking to the videos so they are aware of the importance of protecting SAP information. Access the videos here.

NATIONAL CYBER SECURITY AWARENESS MONTH 2016

National Cyber Security Awareness Month 2016 is just around the corner! Having recognized the importance of cybersecurity to our nation, President Obama has designated October as National Cyber Security Awareness Month. For more information, see our updates here.

SOCIAL MEDIA

Connect with CDSE on Twitter (@The CDSE) and on Facebook.
Thanks,
ISR
Defense Security Service