DSS Monthly Newsletter

October 2014

(Sent on behalf of ISR)

Dear FSO,

This is the monthly email 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.

INFORMATION

FOURTH ANNUAL VOICE OF INDUSTRY SURVEY

From October 6th to the 31ST, Defense Security Service (DSS) will conduct the fourth annual DSS Voice of Industry Survey. This survey of all Facility Security Officers (FSOs) provides an opportunity for feedback on DSS' performance with respect to the administration and implementation of the National Industrial Security Program. While participation in this survey is voluntary, DSS is requesting a 100 percent response rate in order to maintain and improve the quality of our relationship with cleared industry. This survey will be sent directly by email to all FSOs from DSSVOISurvey@dss.mil with a unique https://www.securitysurveys.net link to your facility's survey. Please send any questions regarding the survey to DSSVOISurvey@dss.mil.

FSO ROLE IN COMBATTING CYBER THREATS THROUGH THE COLLABORATION

Cross-functional collaboration is a primary key to the cleared facilities successfully confronting cyber-attacks against a company's unclassified networks. These attacks threaten company profits, products, performance and survival, and the security and wellbeing of its personnel. They endanger the government and proprietary information that the company's unclassified information networks hold or process and the classified contracts they support. The attacks come relentlessly and continuously from nation-states, criminal actors, and others. They have such persistence, sophistication and stealth that many companies may not know an attack has occurred or may not realize it until long after the fact.

NISPOM 1-301 and 302.b, along with ISL 2013-05 address the cleared company's responsibility in reporting such attacks on the classified and unclassified networks. Under the NISPOM the FSO would not have purview of the security and management of the unclassified information systems (except as required under certain FOCI provisions). However, the FSO still has the responsibility to share threat information and assure the company meets NISPOM reporting obligation.

A sound practice increasingly noted among cleared companies is for the FSO to establish continuing security collaboration with the company's information network security management. In that collaboration, they share releasable cyber threat information the FSO receives from DSS and elsewhere, help identify reportable incidents and resolve common challenges, obtain more timely initial and follow-on reports on cyber events meeting the NISPOM criteria, and accomplish early detection and denial of the cyber threat. This is a win-win situation for the FSO, the network security management team, the company, DSS and the company's government customers. A teamed effort gives us an added edge against our cyber adversaries.

RATING MATRIX UPDATE- CI ENHANCEMENT

Effective 1 October 2014, the CI enhancement update to the Rating Matrix was deployed. Last fall, DSS implemented an update to the Security Vulnerability Assessment Rating Matrix, a tool that enables our representatives to consistently and systematically account for vulnerabilities and enhancements during assessments. As a result of your feedback, DSS is updated the Counterintelligence (CI) enhancement (presently Category 7) by splitting it into two separate categories. One enhancement will focus on "process" (Category 7a) and the other on "performance" (Category 7b):

For more information, please go to www.DSS.mil.

MANAGING PERSONNEL SECURITY RECORDS IN THE JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)

The number one finding on Vulnerability Assessments continues to be failure to properly manage JPAS records. As a reminder, NISPOM 2-200b requires the contractors to annotate and maintain the accuracy of their employees' access records.

NOMINATING AND VALIDATING OFFICIALS FOR JPAS/SWFT ACCESS REQUESTS

When completing a Personnel Security System Access Requests (PSSARs) for JPAS or SWFT access, the Nominating Official (Part 5 of the PSSAR) must be an individual who is listed on the Key Management Personnel (KMP) list as required to be cleared in connection with the facility clearance (FCL). Excluded KMP or KMP who are not required to be cleared in connection with the FCL but are cleared for contract performance are not authorized to sign these documents. PSSARs signed by these individuals will be rejected. For companies with only one (1) KMP required to be cleared in connection with the FCL, the KMP must sign his or her own PSSAR as Nomination Official. The Validating Official section (Part 6 of the PSSAR) can be completed by anyone who is not the subject and can validate the person's clearance in JPAS. If the company does not have the ability to complete this section, the entire section (item nos. 33-40) must be left completely blank. In this case, DMDC will serve as Validating Official upon receipt of a complete access request.

POLICY NEWS AND POSTINGS

September 4, 2014: DSS provides information regarding the use of Legacy Operating Systems, such as Windows XP. Link to posting - http://www.dss.mil/isp/policy_faqs.html

ATTENTION JPAS/SWFT/ISFD SYSTEM ACCESS APPLICANTS - SYSTEM ACCESS REQUEST (SAR) PROCESS

Please see http://www.dss.mil/about_dss/news/20110818.html for important information pertaining to the JPAS/SWFT/ISFD system access request processes.

REVISION TO THE LETTER FOR FCL SPONSORSHIP
Please see the below link for the latest version of the FCL sponsorship letter.
-Link to posting - http://www.dss.mil/isp/fac_clear/fac_clear_check.html
-Sample letter – http://www.dss.mil/documents/facility-clearances/fcl_sponsorship_request_letter.pdf

SECURITY EDUCATION AND TRAINING

GETTING STARTED WITH THE SECURITY PROFESSIONAL EDUCATION DEVELOPMENT (SPĒD) PROGRAM
The SPēD Certification Program offers the Security Fundamentals Professional Certification (SFPC) and Security Asset Protection Professional Certification SAPPC) assessments to all security professionals. The SFPC and SAPPC are training-agnostic, meaning they are high-stakes certification assessment and do not have training requirements before testing. Access is easy as CDSE uses Pearson VUE to deliver these tests at over 1,000 test centers worldwide. If you wish to participate in this program and sign up for an account, go to http://www.cdse.edu/certification/index.html and follow the easy steps.

CDSE LEARN@LUNCH WEBINARS
Make plans today to attend our Cybersecurity Learn@Lunch webinar *Trusted Download* on Thursday, October 9, 2014. This webinar provides contractors with specific guidelines for trusted download requirements and explains how to maintain an acceptable level of risk during the creation of lower-than system-level output. These requirements are based on NISPOM requirements for newly accredited and/or reaccredited Information Systems.

Additional information can be found at http://www.cdse.edu/catalog/webinars/cyber-security/trusted-download.html.

NEW CDSE JOB AIDS
CDSE has recently released two new job aids that can provide assistance when using the Electronic Facility Clearance System (e-FCL) or Industrial Security Facilities Database (ISFD) databases. Take a minute to review them today!

DSS Electronic Facility User Guide, September 2014.
This guide provides instructions on how to use the e-FCL Submission Site. The e-FCL Submission Site was developed for contractors to submit required facility clearance information to DSS in an electronic format.

Industrial Security Facilities Database (ISFD), July 2014.
This job aid provides instructions on the use of the ISFD Facility Clearance Verification and Notification features which were enhanced during the most recent update to the database.

NEW CDSE eLEARNING COURSE RELEASED
On Friday, September 19, 2014, CDSE released a new eLearning course: *Security Support to International Industrial Operations*. This course provides basic training on the array of international security requirements applicable to cleared defense contractors who participate in international programs.

CDSE TWITTER FEED

Subscribe to CDSE News (http://www.cdse.edu/news/index.html) and follow CDSE on Twitter @TheCDSE for the latest in security training, education and professionalization.