DSS Monthly Newsletter

February 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

IMPORTANT REMINDER NOTICE
2014 Annual Personnel Security Investigations (PSI) Survey Deployment Timelines

Annual NISP PSI Requirements Projection Survey-Two stages:
STAGE ONE-February 10-24, 2014: Contact Validation Survey to determine if a facility will be included under a consolidated response.

This survey will precede the annual web-based Personnel Security Investigations requirements survey to determine if your projection will be consolidated under a parent cage code. Your response should include your cage code and that of the parent! The survey is scheduled to remain open for a two week period beginning February 10, 2014 and closing February 24, 2014.

STAGE TWO-March 2014: Deployment of the annual web-based survey to identify Facility Personnel Security Investigation requirements for FY15-17. The Survey will be fielded on or about March 10, 2014 and will remain open for four weeks.

Facility participation in the Survey is critical to DoD program planning and budgeting for NISP security clearances and forecasting workload requirements by the Office of Personnel Management.
Survey invitations will contain a securitysurveys.net survey link. As in years past, verification of the legitimacy of the Survey URL can be obtained through your Cognizant Security Office. If you have any questions, please send them to our mailbox: DSSPSISurvey2014@dss.mil.

BEWARE OF RANSOMWARE
Ransomware is a class of malware that restricts access to infected systems and demands the targets pay the creator of the ransomware in order for the restriction to be removed. Ransomware is also called "FBI MoneyPak" or the "FBI Virus" due to the perpetrators' propensity to use the FBI logo in

messages to the target in order to add legitimacy to the extortion attempt. Similar messages have used the USCYBERCOM logo.

There are two types of ransomware: lock-screen ransomware and encryption ransomware. Lock-screen ransomware will employ a full screen image to block the target from accessing anything on their computer. Encryption ransomware will lock the target's computer and/or files with a password.

In fourth quarter fiscal year 2013, DSS received several reports from cleared contractors infected with Crypto-Locker, a variant of encryption ransomware. Crypto-Locker first surfaced in September 2013 and is disseminated via spear-phishing. Crypto-Locker is more sophisticated and aggressive in demands than most ransomware, demanding up to $300 to unlock files, typically payable through MoneyPak, Ukash, or Bitcoin.

While DSS determined that each reported event was criminal in nature, ransomware such as Crypto-Locker, can have a devastating effect on a company's computer network. To help prevent a ransomware attack, carefully examine received emails, do not click links from unknown or suspicious senders, update antivirus definitions, and frequently backup and encrypt sensitive or critical files.

DERIVATIVE CLASSIFICATION TRAINING JOB AID
Notice: The Derivative Classification Training job aid listed as a training resource in ISL 2013-06 has been revised. Click here to read notice (add link) to text.
http://www.dss.mil/about_dss/news/20140106_2.html

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 changes affecting JPAS/SWFT/ISFD system access applicants; changes were implemented on June 1, 2013, in conjunction with the transfer of various DSS Call Center customer support services to the DMDC Contact Center. Thank you!

SECURITY EDUCATION AND TRAINING

ONLINE COUNTERINTELLIGENCE AND THREAT AWARENESS TRAINING
The DSS Center for Development of Security Excellence, in collaboration with the Counterintelligence (CI) Directorate, offers a web-based counterintelligence awareness course for employees working at cleared contractor facilities. The intent of the web-based training is to increase awareness of the potential threats directed against U.S. technology and explain common suspicious activities that cleared employees should report to their facility security personnel. This training is available for personnel working at cleared facilities, and is a convenient tool for Facility Security Officers to enhance their security awareness training. The scenario-based training takes approximately 30 minutes to complete. *Thwarting the Enemy: Providing Counterintelligence and Threat Awareness to the Defense Industrial Base* (CI 111.16) is directly available at: http://cdsetrain.dtic.mil/thwarting.

This course and other counterintelligence training materials are available at DSS CI: http://www.dss.mil/isp/count_intell/count_train_mat.html as well as CDSE at: http://www.cdse.edu/catalog/counterintelligence.html

CDSE WEBINARS

Our next Industrial Security Learn@Lunch webinar, *Technology Control Plans (TCP) Under the NISPOM*, is scheduled for Thursday, February 13, 2014 at 11:30 a.m. and 2:30 p.m. EST. This webinar will not only explain what a TCP is, it will identify the NISPOM TCP requirements as well as the elements that should be incorporated into a TCP.

Go to: http://www.cdse.edu/catalog/webinars/industrial-security/technology-control-plan.html to sign up for this webinar.

Don't forget that CDSE offers other webinars that might also be beneficial to you and your security program. You can check out all of the CDSE upcoming webinars at: http://www.cdse.edu/catalog/webinars/index.html.

Thanks,
ISR
Defense Security Service