DSS Monthly Newsletter

November 2013

(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

The Personnel Security Management Office for Industry (PSMO-I)
PSMO-I has moved!
Our new contact information is as follows:
Defense Security Service
ATTN: PSMO-I
7556 Teague Road, Suite 500
Hanover, MD 21076

Phone: 443-661-1320

Fax: (571)305-6011 or psmo-i.fax@dss.mil (for submission of SF312s)
*When using the email option, encrypt the file in the first email and send the password in a separate email.

New Version of SF312
This is a reminder to FSOs that the new version of the SF312 is mandatory. The new SF312 can be downloaded at http://www.gsa.gov/portal/forms/download/116218

Electronic Fingerprints
Electronic Fingerprints will be mandatory by the end of December 2013. See the following document for options for submitting electronic fingerprints.
http://www.dss.mil/documents/psmo-i/eFP_Guide.pdf

Homeland Security Presidential Directive (HSPD)-12.
DoD has implemented HSPD-12 for the uncleared contractor population that requires a NACI background investigation for physical or logical access to government systems or installations. Government agencies are responsible for paying for, submitting, and adjudicating NACI investigations. OPM's CVS system will store HSPD-12 adjudicative determinations. FSOs should not be creating JPAS records for personnel who do

not require access to classified information. If a government activity is asking an FSO to enter data into JPAS for the uncleared contractor population, please contact AskPSMO-I@dss.mil and provide the government installation making the request.

ADVERSE INFORMATION REPORTING
This is a reminder that NISPOM 1-302a requires FSOs to report adverse information coming to their attention concerning any of their cleared employees. Adverse information is anything that may impact the status of an employee's PCL.

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

ISFD SYSTEM ACCESS APPLICANTS - MOST COMMON SAR REJECT REASONS
The current rejection/disapproval rate for ISFD System Access Requests (SAR) continues to exceed 40 percent. Please see http://www.dss.mil/about_dss/news/20130516.html for the most common reasons for DSS Call Center rejection/disapproval of ISFD SARs. Avoiding these pitfalls will enhance the processing/approval timeline of your ISFD SAR submission. Please contact the DSS Call Center at 888-282-7682, if you have any questions. Thank you!

ISL QUICK REFERENCE TOOL
DSS publishes the "Industrial Security Letter (ISL) Quick Reference Tool," which lists ISL articles in NISPOM paragraph order, subject, ISL number and article, status, and a direct link to the ISL. The quick reference guidecan be found at the following link http://www.dss.mil/about_dss/news/20131030C.html.

SECURITY EDUCATION AND TRAINING

CDSE HOSTS DISA COURSES
Have you found yourself hunting for information on how to better secure your smartphone, tablet, or information system? Then the newest Center for Development of Security Excellence (CDSE) security discipline, Cyber security, is a one-stop shop for you. Cyber security training expands CDSE's eLearning resources by hosting Defense Information System Agency (DISA) courses that are relevant to your training needs.

CDSE has recently released three DISA courses. DS-IA108.06, "Smartphones and Tablets," contains general user awareness, platform-specific guidance, and device administrator training. DS-IA300.06, "Windows Server 2003 Incident Preparation & Response (IP&R)," focuses on security policy, archiving, logs, and host-based and network-based intrusion detection. DS-IA107.06, "DoD Intrusion Detection System (IDS) Analysis Part II," takes the student through a series of lessons which range from a description of tools used in intrusion analysis, to reviewing techniques used in identifying malicious traffic.

For more information and to sign up for these courses go to:
http://www.cdse.edu/catalog/cybersecurity.html

CDSE INDUSTRIAL SECURITY LEARN@LUNCH WEBINARS
Our next Industrial Security Learn@Lunch webinar, *What's an SCR?*, is scheduled for Thursday, November 14, 2013 at 11:30 a.m. and 2:30 p.m. EST. This webinar explains the process that a suspicious contact report (SCR) follows once it is received from a cleared contractor.

For more Information and to sign up for the *What's an SCR?* webinar go to:
http://www.cdse.edu/catalog/webinars/industrial-security/whats-an-scr.html

Just a reminder, due to the Government shut down, the Industrial Security Learn@Lunch webinar, *Technology Control Plans (TCP) Under the NISP*, scheduled for Thursday, October 10, 2013 was cancelled and has been rescheduled for Thursday, February 13, 2014.

For more information and to sign up for the TCP under the NISP webinar go to:
http://www.cdse.edu/catalog/webinars/industrial-security/technology-control-plan.html

Thank you,

ISR
Defense Security Service