DSS Monthly Newsletter

December 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
A special thanks to all who participated in this year's Voice of Industry survey. We appreciate the constructive feedback provided, as this helps us to progress and maintain our current practices, but also improve the quality of our relationship with cleared defense industry. Data analysis is currently underway!

KMP DESIGNATIONS IN JPAS
Key Management Personnel (KMP) are required to be cleared in connection with a Facility Security Clearance (FCL), including the Facility Security Officer (FSO), who must be indoctrinated at the level of the FCL in JPAS. FSOs should confirm all KMP required to be cleared in connection with the FCL, are properly designated with a KMP person category in JPAS, and indoctrinated at the appropriate level. Excluded KMP and KMP cleared for contractual performance that are not required to be cleared in connection with the FCL, should only be indoctrinated at the level of access they require in performance of classified contracts if applicable, and should not be designated as a KMP in JPAS.

CREATING A JPAS ACCOUNT
Government agencies are responsible for submitting, paying for, and adjudicating investigations for "other than access to classified". OPM's CVS system will store the adjudicative determinations if a clearance is not required for access to classified information. FSOs should not create 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 Policy_HQ@dss.mil and provide the name for the government installation making the request.

OVERDUE PERIODIC REINVESTIGATIONS
The Director of National Intelligence issued a memo that mandates that all e-QIPS for overdue Secret PRs need to be submitted by December 1st, and all e-QIPS for overdue Top Secret PRs, must be submitted by December 31st. Failure to submit an e-QIP as required may result in an administrative withdrawal of eligibility.

Please reference the link here at https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS

NCMS 2015: HOW TO ACQUIRE AND MAINTAIN COMPLIANT CONNECTIONS WORKSHOP
During this year's annual NCMS conference in Las Vegas, Nevada, DSS will be hosting a one-day workshop. This workshop will be led by DSS certified ISSPs/ISRs and will benefit industry stakeholders who may have questions or concerns that can be readily addressed in this forum. The goal is to minimize stress associated with the policy/procedural implementation of our CCRI program, as well as share solutions with industry partners early enough to benefit their programs. This also is an opportunity to address common issues in an open forum before they become problem areas. Ultimately, our goal is to partner with industry to ensure information assurance compliance and reduce risk to DoD networks.

Areas of instruction will include:
1) The NISP Cleared Contractor SIPRNet Process Overview
2) CCRI Overview Process & Preparing for an Inspection

Technical sessions will focus on DoD IA compliance, STIGS deep dive, scans, windows, HBSS, and traditional/physical security. This is a closed session and pre-registration is required. Recommended audience of attendees: Cleared industry FSO, ISSM, ISSO, and network administrators.

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.

SECURITY EDUCATION AND TRAINING

SPēD CERTIFICATION MAINTENANCE
Certification holders must maintain their certification through one of two avenues: professional development or testing. The preferred option requires individuals to earn 100 professional development units (PDUs) through participating in various activities, such as completing a training course or participating in a workshop. (At least half of these activities must relate to security topic areas). Or, for those who are considering testing as an option, the Center for Development of Security Excellence (CDSE) provides online tools to help you attain the competencies the exam is established on or to assist you in deciding whether testing is the right choice for you.

Regardless of which option you choose, you will need to report your activities in the Certification and Renewal Form (CRF). The CRF was developed to help you keep track of the PDUs as you accrue them.

Industry numbers for certified individuals by certification.

Industrial Security Oversight Certification	6
Physical Security Certification	10
Security Asset Protection Professional Certification	24
Security Fundamentals Professional Certification	205
Security Program Integration Professional Certification	4
Total number of CRFs (Approved and In Process)	65

Learn more about maintaining your certification: http://www.cdse.edu/certification/maintain-sped.html

ODAA BUSINESS MANAGEMENT SYSTEM (OBMS) eLEARNING COURSE UPDATES

On November 07, CDSE updated the two OBMS eLearning courses available in STEPP:

-OBMS - External User (Contractor Submitter) CS120.16

-OBMS - External User (Government Submitter)

These updates provide enhanced audio for students and accommodate those who wish to complete the courses via Mozilla Firefox web browser.

CYBERSECURITY AND INFORMATION SYSTEMS SECURITY MANAGER (ISSM) TOOLKITS

In August 2014, CDSE launched two toolkits relating to Cybersecurity and ISSMs. Each toolkit has been a valuable resource, and as we work to keep the toolkits as relevant as possible, CDSE welcomes your input! Please forward comments (including ideas for additions and modifications) to the Cybersecurity Training Team at: cybersecurity.training@dss.mil.