DSS Monthly Newsletter

June 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

Guidance on Overdue Periodic Reinvestigations:
Overdue PRs: DMDC will be sending JPAS messages on subjects with Overdue PRs. If the PR is due, please submit an e-QIP as soon as possible. If the subject no longer requires access, please remove the subject from access in JPAS (no PR is due). If the subject has separated from your company, please post a separation date. If the e-QIP was submitted through another agency, please send an RRU with the agency information. If you receive the JPAS message in error (subject does not require a PR), please submit an RRU to indicate that.

Clarification Regarding JCAVS Person Summary Screen PRINTOUTS:
http://www.dss.mil/about_dss/news/20140527.html

DSS Rescinds ISL 2007-01:
http://www.dss.mil/about_dss/news/20140516a.html

Notice for Contractors with GSA-approved Class 5 security containers manufactured by Fedsafes:
http://www.dss.mil/about_dss/news/20140507.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 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!

ATTENTION ISFD USERS - ISFD ACCOUNT ADMINISTRATION UPDATE:
All ISFD users are strongly encouraged to access their accounts at least once every 30 calendar days, to avoid deactivation and deletion. Per regulatory guidance, ISFD accounts are managed with regularly executed deactivation and deletion purges. Accounts reflecting 30 consecutive days of inactivity will be locked, and accounts reflecting an inactive status of 45+ days are subject to deletion. A user whose account is deleted will need to submit the appropriate System Access Request (SAR), to obtain access. Please contact the DoD Security Services Center at 888-282-7682, if you have any questions. Thank you!

OBMS and NCAAISS Update:
The ODAA Business Management System (OBMS) and the National Industrial Security Program (NISP) Common Access Information System (NCAISS) are currently scheduled for release in July 2014. Industry is encouraged to check the DSS website in July for updated information for establishing user accounts.

What is NCAISS?

NCAISS is a web application that provides identity and access management services to authenticate users and provide single sign-on access (SSO) to multiple DSS applications. The first applications will be the ODAA Business Management System (OBMS).

NCAISS Benefits:

- Web-based portal to implement approved DoD PKI authentication
- Users no longer need to remember multiple account credentials (usernames/passwords).
- Provides an automated system access request (SAR) workflow
- Alleviate the requirement for the paper-based access request form
- Provides automated email notifications which increased transparency

OBMS

The ODAA Business Management System (OBMS) is designed to automate the Certification and Accreditation (C&A) process. The system will provide real-time metrics and tracking for security plans. OBMS requires public key infrastructure (PKI) authentication at login and will not allow for user IDs and passwords. In preparation for system deployment, it is important for every ISSM to take steps necessary to acquire a Common Access Card (CAC) or External Certificate Authority (ECA) PKI prior to OBMS deployment.

Requirements for Access:

- Common Access Card (CAC), External Certification Authority (ECA) or approved Corporate DoD PKI certificates.
- Users must request an NCAISS account before an OBMS account can be activated and associated with the user's PKI certificate.

The OBMS internet and intranet webpages will be turn-on 30 days before deployment. Content will include links for the following:

- The NCAISS Portal
- The OBMS Application
- Training Course within STEPP (CS120.16) OBMS– External User (Contractor Submitter)
- User Manuals

SECURITY EDUCATION AND TRAINING

New SPēD Physical Security Certification available:
The Defense Security Service is pleased to announce the SPēD Physical Security Certification (PSC) production version is now open for registration and testing. The PSC assesses candidates' knowledge on a broad range of physical security-centric competencies including physical security concepts, physical access control, security systems, physical security planning, and plan implementation.

The PSC is open to Federal Government civilians, military, and contractor security professionals. To get started, go to the "Request to Become SPeD Certified" website at http://www.cdse.edu/certification/index.html. If you already have a STEPP account and have checked the SPēD participation box in your STEPP User Profile, then go to your My SPēD Certification webpage https://i7lp.integral7.com/durango/do/login?ownername=dss&channel=dss&basechannel=integral7, to verify your account information and request an authorization to test.

CDSE WEBINARS
The unofficial start of summer has just begun, and there's no better way to kick it off then to make plans to attend our June industrial security Learn@Lunch webinar, "The Classified Foreign Visit Process," on Thursday, June 12, 2014, at either 11:30 a.m. or 2:30 p.m. EST. This webinar will discuss the processes and procedures for classified visits by foreign nationals to cleared U.S. contractor facilities and visits by U.S. contractor to foreign entities. In addition to reviewing the NISPOM requirements, best practices and available resources will also be provided.

Go to: http://www.cdse.edu/catalog/webinars/industrial-security/classified-foreign-visit-process.html to sign up for this webinar today.

Thanks,
ISR
Defense Security Service