DSS Monthly Newsletter

April 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 TWO-March 2014: Deployment of the annual web-based survey to identify Facility Personnel Security Investigation requirements for FY15-17. The Survey was 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.

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!

JPAS RRUs and INCIDENT REPORTS:
Due to DoD CAF Consolidation, FSOs should no longer select DOHA when submitting RRUs and Incident Reports. FSOs should select DoD CAF Industry instead.

FOREIGN PASSPORTS:
FSOs are reminded to complete an incident report when they become aware that an employee is using a foreign passport. FSOs having knowledge of an employee using a foreign passport should report the incident via the JPAS "Report Incident" feature.

DoD CAF ADDRESS CHANGE
DoD CAF address (former DISCO): On Oct 2012, DISCO adjudication migrated to the Department of Defense Consolidated Adjudications Facility (DoD CAF). For documents previously sent to DISCO: please address to the DoD CAF Industry, Division 600, 10th Street, Fort Meade, MD 20755.

DSS AUTOMATION UPDATE (EXTERNAL)
FY 14, DSS will be transitioning all applications under the National Industrial Security Program (NISP) Common Access Information Security System (NCAISS).

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 include the Industrial Security Field Database (ISFD) and the ODAA Business Management System (OBMS). NCAISS will allow user to log in once from the DSS.mil website and access multiple systems and services.

NCAISS Benefits:

- Web-based portal to implement approved DoD PKI authentication
- Users no longer need to remember multiple account credentials (usernames/passwords).
- Provides self-service access requests that's processed through with an automated workflow
- Alleviate the requirement for the paper-based access request form
- Provides automated email notifications which increased transparency

ISFD
For our cleared industry partners, ISFD is our Agency's database of record that tracks all the facility clearance and supporting activities. Existing users and new users are required to obtain a NCAISS account to continue access to the application.

OBMS

OBMS will provide an automated workflow capability to support all aspects of the National Industrial Security Program (NISP) C&A process. The system is designed around a web-based portal that receives and stores System Security Plan (SSP) submissions from contractor site Information Systems Security Managers. In addition to a number of other features, the system will provide for automated tracking and notification throughout the system accreditation process. OBMS will replace the current e-mail

submission and feedback process with a robust portal where ISSMs can submit, track, and update system documentation.
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 Information Systems Security Manager (ISSM) to take steps necessary to acquire a Common Access Card (CAC) or External Certificate Authority (ECA) PKI prior to OBMS deployment.

OBMS Benefits:

- Web-based portal secured by DoD PKI authentication
- Provides a central repository for SSPs and C&A Records
- Real-time access to status information for accreditation packages while under review
- Automated notifications of SSP status changes
- Reporting features and capabilities to aid in monitoring the C&A process
- Interface for government stakeholders to submit supporting documentation
- Support for digital signatures on accreditation package documents
- A bulletin board forum for collaboration and knowledge sharing

Requirements for Access:

- Common Access Card (CAC) or External Certification Authority (ECA) for authentication thru NCAISS
- User account pre-registered in the authentication portal and activated in OBMS

SECURITY EDUCATION AND TRAINING

CDSE WEBINARS
To start Spring off on the right foot, CDSE will offer two industrial security Learn@Lunch webinars in April. The first industrial security Learn@Lunch webinar, "Cyber Insider Threat," is scheduled for Thursday, April 10, 2014 at 11:30 a.m. and 2:30 p.m. EST. This webinar will explore traditional espionage indicators in a cyber-environment, identify new indicators specifically related to the IT insider threat, and discuss observable and reportable behaviors that help to detect, deter, and neutralize the cyber insider threat.

Go to: http://www.cdse.edu/catalog/webinars/cyber-security/cyber-insider-threat.html to sign up for this webinar.

Our second Industrial Security Learn@Lunch webinar, "Standard Practice Procedures," is scheduled for Thursday, April 24 at 11:30 a.m. and 2:30 p.m. EST. This webinar will discuss the purpose of Standard Practice Procedures (SPP) in accordance with the NISPOM. It will cover when an SPP is needed, what information it should cover, and how it should be used.

Go to: http://www.cdse.edu/catalog/webinars/industrial-security/standard-practice-procedure.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