DSS Monthly Newsletter

July 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

OBMS Pre-deployment Tips for Industry Partners
The Office of the Designated Approving Authority (ODAA) Business Management System (OBMS) is a secure, web-based application, to streamline and improve the Certification and Accreditation (C&A) process. We are pleased to announce we are less than 30 days away from the deployment of the OBMS. Among other things, OBMS is designed to improve Information System Security Managers' ability to submit and track system security plans, produce reports and metrics, and automate the Memorandum of Understanding/Agreement (MOU/A) tracking Process.

OBMS will be the single portal/method for submitting system security plans and related documents after a six-month transition period beginning at deployment. During the six-month transition, companies are encouraged to migrate to OBMS as early as possible. Once a site has transitioned to OBMS, the site should only submit security plans through OBMS and not both OBMS and the legacy email submission process.

Upon deployment, OBMS login will require the use of Public Key Infrastructure (PKI) or External Certificate Authority (ECA) certificates approved by DoD. OBMS does not offer the ability to log in with a user account and password combination. Sites should ensure appropriate management and/or employees have acquired appropriate credentials to enable login into the system. ISSMs are allowed to have access to multiple cage codes if approved. Each individual account in OBMS requires properly issued credentials for the specific individual utilizing the account. Users will have 10 days to activate their OBMS account once the account approved and created. Users will receive an email notification immediately upon account creation.

A few helpful hints to assist in preparing for OBMS deployment:

A. Individuals in industry should complete OBMS training for "Submitters" through the DSS CDSE STePP portal. The training provides an overview of the system, workflow, and screenshots to

aid in establishing a fundamental understanding of the system and how to submit system security plans.

B. Each site should ensure appropriate individuals have (or are in process) acquired the required login credentials (i.e. PKI or ECA).
C. ISSMs should familiarize themselves with OBMS workflow and determine if local work processes or procedures may be impacted. Local work practices should be used in part to determine which personnel will establish OBMS accounts.
D. ISSMs should work to create an Interconnected Master Security Plan to transition Interconnected System Profiles from Local Area Network (LAN) MSSPs. The existing interconnected system information is migrated within OBMS, but OBMS will not allow Industry to self-certify or create an interconnected system under a LAN or Multi-User System MSSP.
E. Complete the two-step process to register a new account and request OBMS access.
    a. Create a DSS single sign on (SSO) login account through the DSS portal (NCAISS) when the system becomes available.
    b. New login accounts will need to be used within 30 days (and no less than once per 30 days thereafter) to ensure the account is not disabled.
    c. Access the SSO portal through this link: https://sso.dss.mil/opensso/cert/login
    d. For reference and familiarity, the user manual and tutorial for the DSS NCAISS portal is located at http://www.dss.mil/diss/ncaiss.html.
    e. After the DSS single sign on (SSO) account has been created, request an OBMS account through the OBMS Quick link on the main portal page. Please note the OBMS account request link will be activated after OBMS is deployed.
    f. OBMS account requests will be automatically forwarded to Facility Security Officer (FSO) of record for a given CAGE for approval. ODAA is available to assist by email through the ODAA mailbox (ODAA@DSS.MIL) during the account request and vetting process.
    g. FSOs should request OBMS accounts first to activate their Cage Codes and associate their approved PKI credentials within OBMS.
    h. Users will have 10 days to activate their OBMS account once the account approved and created.
    i. Users will receive an email notification immediately upon account creation.

    Questions, feedback, concerns, or other requests for information may be directed to your assigned DSS Industrial Security Specialist and/or Information System Security Professional. In addition, please feel free to send the aforementioned items to the general ODAA mailbox ODAA@DSS.MIL.

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!

JPAS/SWFT PSSAR Rejection Update:
DMDC has validated that an out-of-scope Periodic Reinvestigation (PR) is not a rejection reason for JPAS/SWFT Personnel Security System Access Requests (PSSARs). If a subject has an out-of-scope PR, this may be indicated in the “Other Issues Not in Specified List" section of the PSSAR Processing Checklist rejection document provided by DMDC, if the PSSAR is rejected for another reason. However, this comment is for informational purposes only, to alert the applicant that action is needed on their PR. All

other necessary corrections should be made, and the PSSAR should be resubmitted to DMDC. The appropriate action should be taken by an alternate JPAS user in the applicant's organization to update the PR or downgrade the applicant's access as soon as possible.

ATTENTION ISFD USERS - ISFD ACCOUNT ADMINISTRATION UPDATE:
All ISFD users must 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.

Discontinued Issuance of 381-R Letters:
Starting 1 September 2014, the Defense Security Service (DSS) will discontinue the issuance of 381-R letters. Currently, a 381-R is provided to a facility when a company is issued a Facility Clearance (FCL) or a changed condition affecting the information on the 381-R is processed. Once the change takes effect, an email will be sent to the facility in lieu of a 381-R requesting the facility perform an Industrial Security Facilities Database (ISFD) FCL verification to view the change.

ISFD is the official system of record for facility clearance verification. Once the change takes effect, the 381-R will no longer be a reviewable item at recurring Security Vulnerability Assessments.

Access Magazine:
Please see the below link for the most recent Access Magazine:
http://www.dss.mil/documents/about/DSS%20ACCESS%20v3i2%20Web.pdf

OVERDUE PRs:
The first week of July, DMDC will post the following JPAS message on records that indicate an overdue PR: "DSS records indicate that the applicant has an out-of-scope investigation and the Period Reinvestigation is Overdue. If Access is required, please transmit an electronic Questionnaire for Investigations Processing (e-QIP). If an employee no longer has a requirement to access classified information, please debrief the employee from access in JPAS. If the subject is no longer employed with your company, please debrief and enter the separation date and code in JPAS. If an investigation request has been submitted through another Government Agency please transmit an RRU to DOD CAF IND providing information as to which Agency and when the request was submitted.

**** IF THE REQUESTED ACTIONS ARE NOT COMPLETED WITHIN 30 DAYS FROM THE RECEIPT OF THIS MESSAGE, DSS WILL ADMINISTRATIVELY WITHDRAW ELIGIBILITY WITHOUT PREJUDICE. ***** If you have already submitted the investigation request, please disregard this message. If you have any questions regarding this message, please view the guidance at:
http://www.dss.mil/psmo-i/indus_psmo-i_updates.html

SECURITY EDUCATION AND TRAINING

CDSE FSO TOOLKIT NEWS:
Your smartphone just got a little smarter! The FSO Toolkit is now available as a mobile web app; simply type http://m.cdse.edu/fso/ into your smartphone browser. For Android devices, open up your mobile browser settings and click on "add shortcut" or "Add to Home Screen" to add the Toolkit icon to your home screen. For iPhones, simply click on "Add to Home Screen" icon from the bottom menu bar to add the Toolkit to your home screen. This will allow you to access over 300 Facility Security Officer (FSO) products and resources anytime, anywhere.

Start using the FSO Toolkit from your smartphone today and join the crowd of security professionals who have helped us reach almost 100,000 views in the nine months since its launch.

Don't forget, if you become aware of any products or resources that you believe would benefit other FSOs or discover any problems within the FSO Toolkit, simply send us an email at: industrialsecurity.training@dss.mil and we'll make sure the Toolkit remains up-to-date for all to enjoy!

INDUSTRIAL SECURITY LEARN@LUNCH WEBINARS:
Join us for our next Learn@Lunch Counterintelligence webinar on Thursday, July 10; our topic will be "Supply Chain Risk Management."

Awareness and mitigation of supply chain threat is a major component of a successful supply chain risk management (SCRM) strategy for both the government and industry. The Department of Defense (DoD) seeks to minimize supply chain threat through an active awareness and threat mitigation campaign led by the intelligence and acquisition professionals. This webinar will highlight current DoD and DSS efforts that can be used by supply chain managers, CI professionals, and acquisition professionals to ensure the mitigation of supply chain threat and delivery of uncompromised DoD weapon systems to the warfighter.

This webinar is presented at 11:30 a.m. and 2:30 p.m. EST, so choose the time that best suits your schedule and sign up today at: http://www.cdse.edu/catalog/webinars/counterintelligence/supply-chain-risk-management.html

Thanks,
ISR
Defense Security Service