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.