Armstrong Teasdale

Client Alert

October 24, 2011

Transitioning to the Updated ISFO Process Manual v3.0

By December 31, 2011, DSS will transition to the updated version (Version 3.0) of the Industrial Security Field Officer (ISFO) Process Manual for Certification and Accreditation. The intent of the manual is to explain the standards that must be in place for accreditation of industry information systems.

The updated version introduces a new baseline security configuration. Information systems created on or after December 31, 2011, *must* comply with the new baseline requirements and use new templates when submitting for accreditation.

DSS offers the following guidance to ease the burden of transition:

Configuration changes (such as password length, lockouts, etc.) are considered security relevant changes if applied to previously accredited (including self-certified) systems. Therefore, updating to the new configuration must be considered for reaccreditation.

Information Systems Security Manager (ISSM) self-certification authority does not automatically expire on December 31, 2011, however, the ISSM cannot self-certify any system to the new configuration settings until the ISSM has successfully demonstrated to the Information Systems Security Professional (ISSP) the capability to implement the new configuration.

ISSMs may continue to add workstations to a pre-existing accredited system if the workstations are configured to the previously approved settings and the system profile is properly updated in the appropriate areas. Two limitations may apply. First, an ISSM with existing self-certification authority for a local network (LAN) may continue to add workstations to the LAN as long as there are no other relevant security changes to the LAN. Second, an ISSM with existing self-certification authority for MUSA systems cannot self-certify a new profile under their existing authority unless he/she has demonstrated the ability to properly configure the operating system in accordance with the manual using one of the three methods listed below.

Systems under Master System Security Plan (MSSP) or System Security Plan (SSP) with a current Interim Approval to Operate (IATO) or Approval to Operate (ATO) are not required to implement the new requirements or templates. They will, however, need to implement the requirements or templates at their three-year reevaluation, or if a reaccreditation is necessary due to a security relevant change.

Using the National Industrial Security Program (NISP) Tool and providing a copy of the NISP Tool report are highly encouraged and may be used as evidence of the ISSM's ability to configure the system to the new settings. The NISP tool is available by request at the following ODAA mailbox email address: odaa@dss.mil. The subject line for your email request should read: "Req for doc NISP Chapter 8 Assessment Tool." For operating systems not supported by the DSS ODAA NISP tool, an onsite visit by the ISSP is required to validate the ISSM's ability to implement the configuration settings.

The ISSM may also demonstrate the ability to configure the system in accordance with the new settings during an unrelated scheduled visit by the ISSP. Once the ISSP has validated the ISSM's ability to configure the system, the ISSM may self-certify like systems to the new settings and submit an updated MSSP using the new templates. The onsite validation step may be waived and the system will go straight to ATO as long as the desktop review is satisfactory and there are no additional security relevant changes to the system.

If a previously approved MSSP with a large number of associated self-certified systems is updated and reaccredited due to a change in an associated profile (or at a three-year reevaluation), the ISSM may update one profile under the MSSP, document the plan/timeline for updating the remaining system profiles on a Plans of Actions and Milestones (POA&M), and submit the accreditation package to the Office of the Designating Approving Authority (ODAA), ISSP, and IS Rep.

The POA&M shall reflect an appropriate timeframe for completing the transition of the remaining profiles, not to exceed their scheduled expiration dates.

If an ISSM demonstrates the ability to configure an operating system to the new guidelines in a closed area, then it is not necessary for the ISSP to validate the same operating system in each environment. The ISSP will validate only the first instance of the operating system's configuration, in either environment.

Authorized users may request a copy of the updated Process Manual by sending an email to odaa@dss.mil. In addition, to ensure accurate response, please follow the instructions in the following link: http://www.dss.mil/isp/odaa/request.html#cert.

If you have any questions, please review the DSS website and/or contact:

Brian Kaveney / 314.621.5070
bkaveney@armstrongteasdale.com
