DHS 4300A Sensitive Systems Handbook

Attachment D

To Handbook v11.0

Type Accreditation

Version 11.0

August 5, 2014

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
4.0	June 1, 2006	Initial release
5.0	March 1, 2007	No change
6.0	May 14, 2008	References to the withdrawn NIST Special Publication 800-26 were deleted and replaced with NIST Special Publication 800-53 Revision 2. Section 4.0 Master C&A Package
6.1	September 23, 2008	No change
7.0	August 7, 2009	Introduced new terminology Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53
8.0	May 25, 2011	Introduced new terminology for 4300A v8
9.1	July 24, 2012	Edited for grammar and style.
11.0	August 5, 2014	No changes.

CONTENTS

1.0 Introduction

To streamline the Security Authorization process, DHS Components are encouraged when possible to pursue type accreditation. Type accreditation is appropriate for a general support system (GSS) deployed at multiple sites but operating in a specified environment. For example, several DHS organizations provide services over large distributed environments such as field sites at airports and border crossings. These field sites are equipped with remote network connections, client-server solutions, and other resources, that must be accredited for operation, and accounted for in DHS IT security risk analyses and Federal Information Security Management Act (FISMA) reports. The cost to independently evaluate and accredit each of these sites is prohibitive. A type accreditation, however, allows for consolidating common security controls across the sites and for conducting a single master Security Authorization. To account for unique physical and logical variations at the site level, a description of any differences and the associated risks at each site are documented, and the site-specific documents are incorporated as attachments or appendices to the master Security Authorization package.

2.0 Defining Boundaries for Systems with Common Security Controls

National Institute of Standards and Technology NIST Special Publication 800-37 (SP 80037) provides guidelines for establishing information system security boundaries. The key guidelines that NIST provides in making a boundary determination include:

1. The information resources should generally be under the same direct management control. Direct management control does not necessarily imply that there is no intervening management.
2. The resources should have the same function or mission objective.
3. The resources should have operating characteristics and security needs that are essentially the same.
4. The resources should reside in the same general operating environment (or in the case of a distributed information system, the resources should reside in locations with similar operating environments).

NIST SP 800-37 allows agencies to centrally manage common security controls in a dispersed environment. Relevant attributes for common security controls are the following:

1. Common security controls can apply to a common information system, subsystem, or application (which may include common hardware, software, or firmware) deployed at multiple operational sites.
2. The development, implementation, and assessment of common security controls can be assigned to responsible agency officials or to organizational elements, but not to information system owners whose systems will implement or use those common security controls.
3. Results from common security controls assessment can be used to support the Security Authorization processes of agency information systems where those controls have been applied.

Another guideline for defining an information system boundary when common security controls are implemented is the security categorization of the individual information resources as defined by Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information

Systems." The resources must be defined to operate under the *same security categorization* (low, moderate, or high) for selecting a set of common security controls.

Perhaps most importantly, DHS requires that a system security boundary must encompass system components that are governed by a single policy and are accredited by a single Authorizing Official (AO). If the system policy or the AO varies at any of the sites, for any of the distinct system components, or for any of the information residing within the boundary, that entity (site or system component) must be placed within the boundary of another system or as an independent system.

Using these guidelines, DHS Components can define a single information system encompassing or providing services at a number of sites.

3.0 SECURITY AUTHORIZATION FOR SYSTEMS WITH COMMON SECURITY CONTROLS

By identifying system boundaries based on the NIST guidance and DHS requirements stated above, DHS will implement a more cost-effective approach for performing accreditation on many of the systems deployed within the Department. By consolidating common controls and conducting a single master Accreditation Package, the effort toward a master Security Authorization will be reused at each of the sites. To account for unique physical and logical variations at the site level, a description of any differences and the associated risks at each site must be documented. The site-specific documents must be incorporated as attachments or appendices to the master Security Authorization package.

The Security Assessment process is the comprehensive assessment of the management, operational, and technical security controls in an information system. Using a common controls approach, the assessment process will evaluate two factors:

1. Certify the master Security Authorization package describing the common controls to be implemented across sites.
2. Certify the differences from the master Security Authorization package for the particular site. This includes a definition of how controls and any unique requirements have been implemented at the individual sites.

With a well-designed master Security Authorization package, the unique site implementations that need to be addressed during the authorization process are minimized. This will also more effectively control the environment and site-specific changes.

The Security Authorization process includes the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Using a common controls approach, the process will evaluate the risks at the "master" level and then evaluate any additional risks associated with physical and logical deviations at the site level to make a single decision to operate for the entire system.

4.0 MASTER SECURITY AUTHORIZATION PACKAGE

The master Security Authorization Package (SAP) package is critical for a successful deployment of this type of accreditation. The resulting authorization should be sufficiently robust to represent the risk associated with the system and the complex nature of the deployment. Additional attention must be paid to the possible site variations and complexities of the entire system. Therefore, the effort and cost are generally higher than most typical Accreditation Packages.

Within DHS, a master SAP must include the following basic documents:

1. An approved Security Plan (SP)

2. A Security Assessment Report (SAR)
3. A Security Assessment Plan (SAP)
4. A Contingency Plan (CP)
5. A Plan of Action and Milestones (POA&M) when risks and control weaknesses have been identified
6. An Accreditation Decision Letter (ATO) signed by the appropriate AO
7. Supporting materials such as:
   - Contingency Test Plan (CPT) results
   - FIPS 199 Assessment
   - Privacy Impact Assessment (PIA) statement
   - E-Authentication statement
   - Self-Assessment Report completed in accordance with NIST SP 800-53

[Note: DHS policy requires that the SAP contain all of the documents listed above and that they be uploaded into the Trusted Agent FISMA tool where they become Security Authorization "artifacts."]

The assumption for a successful deployment is a high quality master package, specifically delineating system controls to a level of detail that enables recognition and definition by the site of their deviations from the controls. Significant findings for the master SAP or poor quality and detail should be considered to be an early indication of poor risk planning and should be considered by the AO in making any risk-based decision. Site-Specific Material

The master Security Authorization Package (SAP) provides an understanding of common controls and how they will be implemented across the deployment sites. The site-specific materials do not need to address considerations already covered in the master SAPSAP, but emphasis must be placed on all variances from the common controls and actual site-specific implementation, configurations, and system environment, including physical attributes of the system environment and administrative procedures supporting the system). Each site within the authorization boundary provides documentation that will be used to support the Security Authorization of the entire system. The documentation contains two critical types of information:

1. Site-specific details (for example deviations from functionality, configurations, and physical controls)
2. Site-specific risk analysis (for example analysis of additional risks that result from deviations at the site)

The effectiveness of the site-specific approach is dependent on three factors:

1. The quality of the master SAP
2. The configuration management process for implementing and configuring new sites
3. The communication strategy for ensuring that sites understand the common controls and know how to properly implement and configure them

In making an authorization decision, the organization's challenge is in determining how effectively these three factors have been implemented.

As part of the Security Assessment Report (SAR) for each site, emphasis should be placed on the following key topics supporting the site implementations:

1. Configuration management and control
2. Communications with sites
3. Site-specific deviations from common controls

4. Site-specific security impact analysis

5.0 SITE-SPECIFIC CONSIDERATIONS

Some site-specific considerations are the following:

- **Configuration Management and Control.** Because each site has a unique of common controls implementation, the processes for managing, controlling, and documenting installations and changes for each site deployment is critical to success. It is especially important that configuration of the common security control mechanisms be strictly controlled throughout this process, and that deviations be documented so that risks associated with modifications can be assessed prior to authorization.
- **Communication with Sites.** Personnel at each field site are responsible for effectively implementing common controls as elaborated in the master SAP. In order to locally implement the plan, sites must be aware of and maintain an understanding of their responsibilities in support of the master SAP. They will best achieve the requisite awareness and understanding through effective communications. Knowledge of local contacts, user responsibilities, escalation procedures, and incident reporting procedures are some of the common communication issues that must be clearly documented for a successful deployment. Site input and adherence to documented master administrative procedures can assist in this communication.
- **Site-Specific Deviations.** Each site will have unique requirements and design considerations. Depending on the level of the master SAP's detail, site-specific deviations may be as simple as creation and maintenance of an installation checklist that records implementation details (for example local points-of-contact (POC) and Internet Protocol (IP) addresses). Additionally, site-specific procedures and instructions (e.g., location of backup media and standard operating procedures) may augment general administrative procedures for performing back-ups and for other routine tasks that are a part of the master SAP. All deviations that could influence potential system security risks must be accounted for in site-specific documentation. This is especially true for any security controls that are not implemented at a particular site (for example physical controls) because the master SAP may be dependent on a control not implemented to prevent exploitation of system vulnerabilities that are not obvious at the site level.
- **Site-Specific Security Impact Analysis.** Based on site-specific deviations, an impact analysis must be conducted to determine if any additional risk has been introduced to the overall system due to site-specific variations. This analysis must be performed at the master level and also at the site level, since variations at one site can affect the overall system posture.

Additional risk may be addressed by requiring a review of the common controls selected to determine whether the residual risk has been affected. Any residual risk could potentially result in development of a POA&M for remediation at the site.