U.S. Customs and Border Protection

Attachment D

Type Accreditation

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 21, 2010	No Changes.

CONTENTS

1.0 INTRODUCTION....1
2.0 DEFINING BOUNDARIES FOR SYSTEMS WITH COMMON SECURITY CONTROLS....1
3.0 C&A FOR SYSTEMS WITH COMMON SECURITY CONTROLS....2
4.0 MASTER C&A PACKAGE....3
5.0 SITE-SPECIFIC MATERIAL....3
6.0 SITE-SPECIFIC CONSIDERATIONS....4

1.0 INTRODUCTION

In order to streamline the C&A process, CBP is encouraged to pursue type certification/accreditation where possible. A type certification/accreditation is appropriate for a general support system deployed at multiple sites but operating in a specified environment. For example, several organizations within DHS provide services over large distributed environments (e.g., field sites at airports and border crossings). These field sites are equipped with remote network connections, client-server solutions, and other resources, all of which must be accredited for operation and accounted for in DHS IT security risk analyses and FISMA reports. The cost to independently evaluate and accredit each of these sites is prohibitive. A type certification/accreditation, however, allows for common security controls across the sites to be consolidated and for a single master C&A to be conducted. 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 C&A package.

2.0 DEFINING BOUNDARIES FOR SYSTEMS WITH COMMON SECURITY CONTROLS

NIST Special Publication (SP) 800-37 provides guidelines for establishing information system security boundaries. The key guidelines provided by NIST in making a boundary determination include:

- 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.
- The resources should have the same function or mission objective and essentially the same operating characteristics and security needs.
- The resources should reside in the same general operating environment (or in the case of a distributed information system, reside in various 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:

- Common security controls can apply to a common information system, subsystem, or application (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites.
- The development, implementation, and assessment of common security controls can be assigned to responsible agency officials or organizational elements (other than the information system owners whose systems will implement or use those common security controls).
- The results from the assessment of the common security controls can be used to support the security C&A 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 Designated Accrediting Authority (DAA). If either the system policy or the DAA is different at any of the sites, for any of the distinct system components, or for any of the information residing within the boundary, then that entity (e.g., site, hardware component) must be placed within the boundary of another system or as a system unto itself.

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

3.0 C&A 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 C&A, the effort toward the master C&A 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 C&A package.

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

1. Certify the master C&A package describing the common controls to be implemented across sites.
2. Certify the differences from the master C&A 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 C&A package, the unique site implementations that need to be addressed during certification are minimized. This will also more effectively control the environment and site-specific changes.

Accreditation is 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 accreditation 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 C&A PACKAGE

The master C&A package is critical for a successful deployment of this type of accreditation. The resulting certification 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 C&A packages.

Within the DHS, a master C&A package must include the following basic documents:

- An approved System Security Plan (SSP)
- A Security Assessment Report
- A Security Test and Evaluation Plan
- A Contingency Plan
- A Plan of Action and Milestones (POA&M) when risks and control weaknesses have been identified
- An Authority to Operate Letter signed by the appropriate DAA
- Supporting materials such as:
  - Contingency Test Plan results
  - FIPS 199 Assessment
  - Privacy Impact Assessment statement
  - E-Authentication statement
  - Self-Assessment Report completed in accordance with NIST SP 800-53 Revision 2

[Note: DHS policy requires that the C&A package contain all of the documents listed above and that they be uploaded into the Trusted Agent FISMA tool where they become C&A "artifacts."] The assumption for a successful deployment is that the master package is high quality, specifically delineating the controls of the system to the level of detail that allows the site to recognize and define their deviations to the controls. Significant findings for the master package or poor quality and detail should be considered to be an early indication of poor risk planning and should be considered by the DAA in making any risk-based decision.

5.0 SITE-SPECIFIC MATERIAL

The master C&A package provides an understanding of the 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 C&A package. However, emphasis must be placed on the differences between the common controls and actual site-specific implementation, configurations, and system environment (e.g., physical attributes of the system environment and administrative procedures supporting the system). Each site within the accreditation boundary provides documentation that will be used to support the C&A of the entire system. The documentation contains two critical types of information:

- Site-specific details (e.g., deviations to functionality, configurations, and physical controls)

- Site-specific risk analysis (e.g., additional risks that are perpetrated by the deviations at the site)

The effectiveness of the site-specific approach is dependent on (1) the quality of the master C&A package, (2) the configuration management process (for implementing and configuring new sites), and (3) the communication strategy for ensuring sites understand and know how to properly implement and configure the common controls. The challenge for the organization is determining how effective these three factors have been implemented for the system in order to make an accreditation decision.

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

- Configuration management and control
- Communications with sites
- Site-specific deviations from the common controls
- Site-specific security impact analysis

6.0 SITE-SPECIFIC CONSIDERATIONS

Some site-specific considerations are the following:

- **Configuration Management and Control.** Because each site is a unique implementation of common controls, the processes for managing, controlling, and documenting installations and changes (each site deployment) is critical for success. The configuration controls must be sufficient to ensure that a robust process is enforced for the management and controls at the site deployments. It is especially important that the configuration of the common security control mechanisms be strictly controlled through this process, or that deviations are documented so the risks associated with those modifications can be assessed for accreditation.
- **Communication with Sites.** Personnel at each field site are responsible for effectively implementing the common controls as elaborated in the master SSP. In order to implement the plan locally, the sites must be aware of and maintain an understanding of their responsibilities in support of the master plan. This is achieved through effective communications. Knowing local contacts, user responsibilities, escalation procedures, and incident reporting procedures are some of the common communication issues that must be clearly documented and implemented 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 detail of the master C&A package, the site-specific deviations may be as simple as an installation checklist to record implementation details (e.g., local point-of-contact, Internet Protocol Addresses). Additionally, site-specific procedures and instructions (e.g., location of backup media and standard operating procedures) may augment the general administrative procedures (e.g., for performing back-ups) that are a part of the master package. All deviations that could affect the potential security risk to the system must be accounted for in the site-specific documentation. This is especially true for any security controls that are not implemented at a particular site (e.g.,

physical controls), because the master plan may be dependent on that control to prevent the exploitation of system vulnerabilities that are not obvious at the site level.

- **Site-Specific Security Impact Analysis.** Based on the 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 (at least informally), 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 the development of a POA&M for remediation at the site.