U.S. Customs and Border Protection

Attachment M

Tailoring the NIST SP 800-53 Security Controls

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	Major update to Excel object to bring in line with NIST SP 800-53, Rev 3. Combined both worksheets.

CONTENTS

1.0 INTRODUCTION

Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004), directs organizations to categorize their information systems as low-, moderate-, or high-impact for each of the three IT security objectives (confidentiality, integrity, and availability). The overall categorization for the system is the highest impact assigned to any of the objectives, which FIPS 199 refers to as the "high-water mark." Therefore, if one of the objectives is categorized as high-impact, FIPS 199 states that the system will be categorized as a high-impact system. FIPS 200 (*Minimum Security Requirements for Federal Information and Information Systems*) requires the implementation of NIST SP 800-53 (as amended) security controls applicable to the impact level of the system being evaluated.

For DHS, the high water mark requirement is amplified to reflect the actual security requirements for controls to meet. This policy amplification is a Department-level risk-based decision that is consistent with FISMA policy which requires DHS to "cost-effectively reduce information security risks to an acceptable level." The tailoring of controls and use of compensating controls is also consistent with providing the safeguards necessary to reduce the risks in a specific operational environment. At DHS, the necessary security controls, supporting the security objectives, required for an IT system will be implemented without the requirement to implement extra controls that may not be necessary. This is the minimum DHS standard; however, any program that wishes to implement more than the minimum control can still implement them when appropriate.

This policy amplification is also consistent with the NIST information security guidance which promulgates the "concept of risk based decisions." The due diligence required by FIPS 199 of determining the exact impact level each type of information contained on the system, and each of the security objectives, will lead to well defined impact levels for confidentiality, integrity, and availability of the system as a whole. It is important, when using a risk-based decision to minimize the security controls, that all of the information and the risks to that information be clearly defined and documented. In that way, the DAA can make an informed decision on the level of risk that is acceptable for the system and its information in the specific operational environment.

As a result, in the DHS FIPS 199 Workbook, impact levels (high, moderate, low) can be assigned to each security objective. This means, for example, that a system with low risk availability, high risk integrity, and low risk confidentiality will not be required to implement all high controls across the board. Rather the controls that fall out of the analysis will be implemented (i.e., high levels for integrity controls, low for the confidentiality and availability controls). NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, should be applied specific to the security objective determined impact level.

2.0 TAILORING THE NIST SP 800-53 CONTROLS

NIST 800-53 allows for the controls required for the IT system to be tailored based on an assessment of the risk and on organization-specific security requirements. NIST 800-53 provides guidance on tailoring the controls via scoping considerations and via the use of compensating controls (summarized below). An appropriate FIPS 199 characterization of the system for confidentiality, integrity, and availability and appropriate tailoring of the required

800-53 controls based on the characterization will help ensure that the controls implemented for the system make sense and provide the needed protection.

Scoping considerations for the tailoring of the 800-53 controls include the following (see NIST 800-53 for more detailed information):

- Technology-related considerations. Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system.
- Infrastructure-related considerations. Security controls relating to facilities (e.g., physical controls such as locks and guards, environmental controls) are applicable only to those sections of the facilities that directly protect or support the information system.
- Public access-related considerations. Security controls for a public access information system should be applied with discretion since some of the controls required for the system may apply to some users but not to those users accessing the system through public interfaces. For example, identification and authentication controls and personnel security controls may be required for personnel involved in maintaining and supporting the information system but not for users accessing the system through public interfaces in order to obtain publicly available information. However, the controls may apply to users who are accessing the system through public interfaces in order to access or change private/personal information.
- Scalability-related considerations. Security controls are scalable either by the size of the organization involved or the FIPS 199 security categorizations of the information system being protected, or both. For example, the contingency plan for a system within a large organization and with a high impact for availability is likely to be longer and provide more implementation detail than the contingency plan for a system within a smaller organization and with low impact for availability. Organizations should use discretion in scaling the security controls to the particular environment to ensure a cost-effective, risk-based approach to security control implementation.
- Common security control-related considerations. Some of the controls applicable to an information system may be addressed at the Department level by controls designated as common controls managed at the Department level. Security controls designated as common controls may affect the implementation of controls at the Component level. Components are responsible for ensuring that all required controls for the system are addressed, either at the Department level through common security controls or at the Component level.

Compensating controls are controls that are implemented in lieu of NIST 800-53 controls and that provide protection for the system that is equivalent or comparable to the protection provided by the NIST controls. For example, an organization with significant staff limitations may have difficulty in meeting the separation-of-duties security control but may employ compensating controls by strengthening the audit and accountability controls and personnel security controls within the information system. Compensating controls must be selected from the NIST SP 800-53 security controls, the organization must provide the rationale and justification for how the compensating controls provide an equivalent security capability or level of protection for the system, and the organization must assess and formally accept the risks associated with employing the compensating controls. The use of compensating security controls should be

documented in the system security plan and approved by the authorizing official for the information system.

The attached spreadsheet identifies the security objective(s) (C = confidentiality, I = integrity, and A = availability) for each NIST 800-53 control by impact level (L = low, M = moderate, and H = high) and provides information on the possible tailoring of these controls (double-click on the icon to open the spreadsheet). The spreadsheet is also accessible via the CISO page on DHS Connect.

M - 800-53 Controls.xls