NOAA/NESDIS

Federal Information Processing Standard 200 Controls Selection and Tailoring Policy and Procedures

September 1, 2011

Prepared by:

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)**

Table of Contents

UNITED STATES DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
NATIONAL ENVIRONMENTAL SATELLITE.
DATA AND IINFORMATION SERVICE
Siler Spring, Maryland 209 10

September 30, 2012

MEMORANDUM Distribution

FOR: FROM: Catrina D. Purvis
NESDIS Chief Information Officer (Acting)

SUBJECT: Issuance of Updated NESDIS Information
Technology Security Policies and Procedures

This is to announce the issuance of ten updated NESDIS publications for implementing effective, compliant, and consistent information technology (IT) security practices within NESDIS. These documents highlight the specific steps necessary to ensure effective NESDIS implementation. Specifically issued under this memorandum are the

1. NESDIS *Federal Information Processing Standard 199 Security Categorization Policy and Procedures,* v3.0;
2. NESDIS *Plan of Action and Milestones Management Policy and Procedures,* v2.0;
3. NESDIS *Policy and Procedures for Determining Minimum Documentation Requirements for System /111erconnections,* v2.1;
4. NESDIS *Contingency Planning Policy and Procedures,* v2. 1;
5. NESDIS *Policy and Procedures for Ensuring Security i11 NESDIS IT Systems and Services Acquisitions,* v2. 1;
6. NESDIS *Security Assessment Report Policy and Procedures,* v2.0;
7. NESDIS *Federal Information Security Management Act (FISMA) Inventory Management Policy and Procedures,* v2 .0;
8. NESDIS *IT Security Training Policy and Procedures,* v2.l ;
9. NESDIS *Continuous Monitoring Planning Policy and Procedures,* v2. 1; and the
10. *Practices for Securing Open-source Project for a Network Data Access Protocol Server Software 011 NESDIS Information Systems,* v3.l.

These publications are part of the NESDIS-wide effort to maintain and enhance its foundation of NESDIS IT security policies and implementation practices that align with the latest Department of Commerce and NOAA policies, requirements, and standards. I wish to thank all who contributed reviewing and commenting on the drafts prior to publication to ensure that they are complete, current, and meaningful. These documents will be posted to the Chief Information Division's Web site at https://intranet.nesdis.noaa.gov/ocio/it security/handbook/itsecurityhandbook.php. If you have any questions, please contact the NESDIS IT Security Officer, Nancy Defrancesco, at Nancv.DeFrancesco@noaa.2ov or phone (30I) 713-1312.

FIPS 200 SECURITY CONTROLS SELECTION AND TAILORING POLICY AND PROCEDURES

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
Draft 1.0	7/24/2009	All	Noblis	Initial Draft
Draft 1.1	8/15/2009	All	ITSO	Updated for ISSO comments
Draft 1.2	8/20/2009	Page 14 wording	ITSO	Editorial correction
Draft 1.3	9/15/2009	3.5, 7.1.3, 7.2.1, 7.2.2	ITSO	Updated for NESDIS-wide comments and issue pre-final draft for comment
Final v1.0	9/30/2009	Date	ITSO	Finalize
Draft v1.1	8/15/2011	Update headers, footers, policy references	ITSO	FY2011 review and update
2.0 final	9/01/2011	All	ITSO	Removed Draft markings and finalized

1.0 Background and Purpose

In accordance with the Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541, *et seq*., all information systems are required to implement a minimum set of security requirements that provide an appropriate level of protection consistent with mission requirements, risk, technical constraints, operational constraints, and cost/schedule constraints. National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, requires that the System Owner (SO) implement a minimum baseline of security requirements in seventeen security-related control families to protect the confidentiality, integrity, and availability of their system based on the security impact of their system and system information. NIST provides guidance for security control selection and tailoring in NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, as well as supporting supplemental guidance and mandatory standards (i.e., other NIST SPs and FIPS).

The purpose of this Policy and Procedure is to communicate the NESDIS-specific policy and document the implementation procedures for managing NIST SP 800-53 control selection, tailoring, and approval of the FIPS 200 documentation of the baseline selection.

2.0 Scope

The scope of this document is limited to identifying the process for determining and obtaining approval of the FIPS 200 report, which documents the security baseline for the system. It will not address details for implementing the controls or requirements for testing the controls. It applies to all NESDIS employees and contractors responsible for the development, operation, and maintenance of NESDIS information systems, including contractor owned and operated systems that contain NESDIS information.

3.0 Roles, Responsibilities, and Coordination

The following summarizes the roles and their responsibilities in the NESDIS security control selection, tailoring, and management process.

3.1 Chief Information Officer (CIO)

The *Chief Information Officer* is responsible for establishing the organizational standards for selecting and tailoring security controls within NESDIS.

3.2 Authorization Official (AO)

The *Authorizing Official* is responsible for formally approving the selected control baseline as documented by the FIPS 200 analysis.

3.3 System Owner (SO)

The information *System Owner* is responsible for the development, implementation, and maintenance of the security control baseline in accordance with established regulations, policies, and security requirements. The SO will perform the initial control analysis and baseline selection in accordance with FIPS 200 and provide to the ITSO for review and concurrence.

4.0 Information Owner (IO)

The *Information Owner* shall provide input to information SOs regarding the security requirements and security controls for the information systems where the information resides.

4.1 Information Technology Security Officer (ITSO)

The *Information Technology Security Officer* is responsible for performing a quality review and interacting with the SO and ISSO to ensure that the FIPS 200 analysis meets the NIST SP 800-53 standards for control selection and tailoring. The ITSO will ensure the submitted FIPS 200 baseline is consistent with other NESDIS FIPS 200 baseline control selections, and will provide the AO with their recommendation for approval or rejection.

4.2 Information System Security Officer (ISSO)

The *Information System Security Officer* shall play an active role in developing and updating the system security control baseline. The ISSO assists the SO in the development of the security control baseline, including providing the technical limitations and requirements of the information system.

5.0 Management Commitment

The NESDIS Office of the CIO (OCIO) supports the NESDIS Assistant Administrator’s (AA’s) strong emphasis on securing NESDIS information and information systems. Through the issuance of this policy and accompanying process and procedures, it demonstrates this commitment by establishing and documenting a process for establishing and tailoring an IT security control baseline to ensure an appropriate level of security is implemented for the system.

5.1 Compliance

The NESDIS ITSO monitors – through periodic quality reviews and monthly performance metrics – documentation of security controls baselines within NESDIS to ensure compliance with applicable laws, directives, policies, and guidance. The ITSO reports to the AA monthly, and to the CIO and Office Directors as necessary regarding compliance. The AA, CIO, and/or Office Directors may initiate actions as necessary to correct reported deficiencies, including reallocation of resources to improve implementation of security practices, or removal of an individual from their role as AO, SO, ITSO, or ISSO.

5.2 References

- Department of Commerce (DOC) *Information Technology Security Program Policy* (ITSPP) section 4.0 (January 2009)
- NOAA IT Security Manual 212-1302 (March 2008)

6.0 Policy

As required by DOC ITSPP Section 4.0, the NESDIS-specific controls selection and tailoring process and procedures shall align with the requirements of FIPS 200 and NIST SP 800-53. Each NESDIS information system shall have an AO-approved IT security control baseline that provides an appropriate level of IT security for the system, and approval shall be documented in the AO's memo approving the system's control selection (Appendix A).

6.1 Policy Maintenance

The NESDIS ITSO shall review this policy and procedures biennially and update as necessary to reflect implementation challenges and new requirements. All updates to this policy shall be subject to a NESDIS-wide vetting process providing an opportunity for stakeholders to comment on the programmatic implications of updates.

6.2 Policy Feedback Process

NESDIS personnel are encouraged to notify the ITSO by e-mail to nesdis.hq.secteam@noaa.gov regarding any errors found in the document or other clarifications or updates that are required.

6.3 Policy Effective Date

This policy is effective upon issuance.

7.0 Control Selection and Tailoring Process and Procedures

The selection of the IT Security Controls baseline for a system serves as the entry point and lifecycle reference for evolving the delicate balance between security, cost, functionality, and ease of use. Federal agencies must meet the minimum security requirements in seventeen security-related areas as defined in FIPS 200 through the use of the security controls in accordance with NIST SP 800-53. As NIST SP 800-53 presents a broadly applicable spectrum of controls, not all controls presented will be applicable, and the list will not necessarily be comprehensive for a specific system, mission, or environment. While the baseline security controls recommended by NIST SP 800-53 are not necessarily absolutes, tailoring is only permitted under strict terms and conditions provided in the guidance described in Section 3.3 of NIST SP 800-53 and with the approval of authorizing officials.

NIST SP 800-53 provides guidelines for selecting security controls and provides a recommended minimum baseline along with guidance for appropriate tailoring and supplementing the baseline to achieve a set of IT security controls appropriate for the system. Figure 1 provides an overview of the entire control selection process described in NIST SP 800-53.

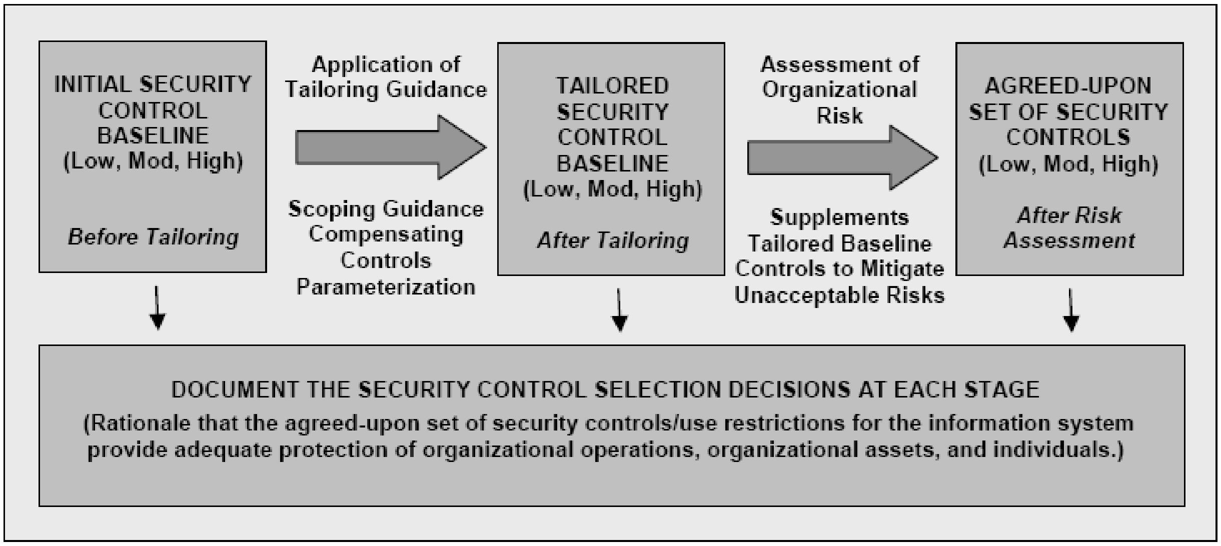
INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)
Before Tailoring
Application of Tailoring Guidance
Scoping Guidance
Compensating Controls
Parameterization
TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)
After Tailoring
Assessment of Organizational Risk
Supplements Tailored Baseline Controls to Mitigate Unacceptable Risks
AGREED-UPON SET OF SECURITY CONTROLS (Low, Mod, High)
After Risk Assessment
DOCUMENT THE SECURITY CONTROL SELECTION DECISIONS AT EACH STAGE
(Rationale that the agreed-upon set of security controls/use restrictions for the information system provide adequate protection of organizational operations, organizational assets, and individuals.)

Figure 1 NIST SP 800-53 Security Control Selection Process

When NESDIS considers selecting and tailoring the security control baseline, the focus is on the protection requirements for the system, data, and environment. The final baseline is determined as part of a NOAA/NESDIS-wide information security program that involves the management of risk to NOAA, its mission or to individuals associated with the operation of the information system. The selection of controls should not be constrained by technology currently used in the system.

7.1 Control Selection (FIPS 200) Procedures

7.1.1. Categorize: Establish Security Category of Information System (FIPS 199) The

starting point for the selection of the security control baseline is the Security Categorization, determined by using the process defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and implemented within NESDIS. The security categorization will determine if the system has a “Low,” “Moderate,” or “High” impact. See the NESDIS *Federal Information Processing Standards Publication (FIPS) 199 Policy and Procedures* for more details on creating the FIPS 199 analysis.

7.1.2. Select Initial minimum Security Controls

The corresponding IT Security control baseline found in the latest revision of NIST SP 800-53[1] is the initial baseline for the system. From this initial baseline, the SO must tailor the system baseline to fit the specific needs of the system. Some controls may not be selected for the control baseline tailored for a specific system. Appropriate rationales for not selecting controls are presented below.

The control baseline for the system shall be documented and maintained in the System Security Plan (SSP), and shall include the rationale for anycontrols, or portions of a control, that are removed from or used for supplementing the baseline. For additional guidance on developing the SSP and its format refer to the NESDIS *System Security Plan Development and Maintenance Policy and Procedures.*

7.1.3. Identify all Common/Hybrid Controls

The SO must review the common controls published by NOAA and NESDIS to select when those controls are appropriate to the operation of the system. Simply because a control is offered as a common control does not mean it can or must be utilized by a system or the organization managing and operating the system. For example, an Intrusion Detection System (IDS) offered as a common control cannot be claimed as a control implementation unless the system owner chooses to inherit (use) the common IDS and documents inheritance in the SSP.

Some common controls are also offered as hybrid controls in which a portion of the control is centrally defined and managed while other portions, such as the implementation, remain the responsibility of the local system. All controls offered as either common or hybrid controls must be evaluated to ensure that the portions of the control indicated to be satisfied by the common control provider is appropriately implemented for the local system. The SO shall supplement the common and/or hybrid controls as necessary to ensure the NIST SP 800-53 control is fully implemented. The SO is ultimately responsible for the security of their system, so it is their responsibility to ensure that all controls are fully implemented, or the rationale for not implementing a control is fully documented and approved by the AO.

7.1.4. Tailor for Technology-related Considerations

If a system is not configured to utilize a specific technology specified by a NIST SP 800-53 control – for example public key infrastructure technology or mobile code technology – then a basis exists to justify elimination of the controls associated exclusively with that technology from the baseline, but only after a careful analysis determines that the entire control can be eliminated. For example, if a system does not need to issue or utilize public key certificates, then SC-17 Public Key Certificates may be excluded from the baseline. On the other hand, while wireless technology is rarely utilized on NESDIS systems, High impact systems are required to scan for unauthorized wireless access points at least annually so only portions of the control may be excluded from the High baseline, even when the system does not implement wireless technologies.

7.1.5. Tailor for Operational/Environmental-related Considerations

7.1.5.1 Subset of the architecture subsystem boundaries

The SO may define subsets of the system that support specific functions that require different protection than other parts of the system. Some examples of such subsets include a DMZ for public access, control segments in an Industrial Control System (ICS) environment, or a specific enclave for processing and storing Privacy Act data. The FIPS 199 analyses and FIPS 200 control selection is required for each security enclave having a separate impact level, but these can be documented as separate sections of one FIPS 199 or FIPS 200 analysis for the system. However, once the control selection is completed, the Assessment and Authorization (A&A) of the system will include such subsets. The enclave must have a specific, identifiable boundary within the remainder of the system. A system may contain multiple security enclaves. Each enclave must be explicitly addressed for every control implementation that deviates from the primary control implementation. In general, controls in a baseline for a higher impact FIPS 199 analysis may not be removed from the enclave that drives that analysis. However, a lower impact enclave may utilize the less rigorous requirements of the lower baseline thus reducing development and implementation cost.

7.1.5.2 Physical Infrastructure-related considerations

Within a single facility (building or similar structure) within which an information system resides, the physical controls must be based on the high-water mark for the system within that facility. Where it is feasible, isolation of a higher impact subset of the system into a physical enclave within the facility essentially provides a mechanism for using the same subsetting concept as in the system controls.

7.1.5.3 Public access-related considerations

Public access to a Government system requires a specific subset of the system to be set aside for the unique security requirements involved in this type of access. Generally this is achieved by what is commonly called a DMZ where the policy and related technical controls, in particular access control and monitoring, are distinct from the remainder of the system.

7.1.5.4 ICS selection and implementation

Appendix I of NIST SP 800-53 and NIST SP 800-82 (*Guide to Industrial Control Systems (ICS) Security*) provide guidance on tailoring security controls on systems that may not be able to support normal IT security controls due to a combination of performance requirements and legacy hardware and software. This tailoring does not grant a free pass on the tailored controls. Instead, it requires rigorous compensating controls for the specific instances where a regular control cannot be implemented for operational reasons.

Tailoring should be limited to only those components or system subsets that are unable to implement a specific control for a specific operational reason. Just because a component is part of a system that has an ICS designation, that component is not necessarily eligible for ICS control tailoring. For example, a complex control system may be composed of a core set of legacy and proprietary "appliance" components that perform direct ICS activities, with a supporting set of more general-purpose components providing monitoring and analysis functions.

For each control that is tailored to accommodate ICS requirements, the SO must document the reason the control cannot be implemented as stated and discuss all compensating controls that have been implemented or enhanced to accommodate the tailoring. A control cannot be tailored out of the baseline for ICS reasons without applying appropriate compensating controls that are determined to provide equivalent protection. For Moderate and High impact systems, this determination must be made through independent controls assessment (see NESDIS *Policy and Procedures for Conducting Security Controls Assessments*). As the compensating controls can be quite burdensome, the ICS concept with accompanying compensating controls should only be employed where absolutely necessary.

7.1.6. Adjust for Security Objective-related Considerations

NIST SP 800-53 permits scoping based on the impact level identified for each security objective as determined by the FIPS 199 security categorization. Security controls that uniquely support a single security objective may be downgraded to the corresponding control for the impact level of that security objective.

NIST SP 800-53 goes on to state that this downgrading can only occur if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water mark; (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system. Since the application of the "high water mark" by definition raises all the security objectives with lower impact, the control requirements imposed for a control objective that was not initially at the higher level may be unnecessarily raised. NIST SP 800-53, Section 3.3, lists the specific controls for each security objective that can be considered for downgrading. NESDIS systems tend to have higher availability and integrity impact ratings than confidentiality. For systems that fall into this category, you can downgrade, justified by the lower confidentiality rating, the following controls or control enhancements: MA-3 (3), MP-2 (1), MP-

3, MP-4, MP-5 (1) (2) (3),[2] MP-6, PE-5, SC-4, and SC-9. When downgrading these confidentiality-only controls, care must be taken to ensure that the downgrading does not expose security relevant information such as password files, network routing tables, or cryptographic key management information.

In some cases, only a specific Control Enhancement is listed as being eligible for downgrade. For example, MA-3 (3) is listed as a candidate for downgrade due to the confidentiality of the system. This means that from the MA-3 Maintenance Tools requirement, the SO may tailor out Control Enhancement 3, the requirement to check maintenance equipment for capability to retain information, for a system with high integrity or availability impact but a moderate or low confidentiality impact. The SO must still implement the base control, MA-3, as well as control enhancements (1) and (2) which require the tools be inspected for improper modifications and to check the tools for malicious code.

The SO must ensure that they carefully analyze the control tailoring to ensure that any downgrades are consistent for threat environment identified in their risk assessment. As with other tailoring, controls that are downgraded must be fully documented with justification in the SSP.

7.1.7. Identification of Compensating Controls

Compensating controls are applied when a control cannot be implemented due to operational requirements. The conditions under which compensating controls may be employed are explained in NIST SP 800-53.

System owners may on occasion find it necessary to specify and employ compensating security controls. A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST SP 800-53, that provides equivalent or comparable protection for an information system. For Moderate and High impact systems, this determination must be made through independent security controls assessment (see NESDIS *Policy and Procedures for Conducting Security Controls Assessments*).

Once determined adequate by the NESDIS ITSO, a compensating control for an information system may be adopted for use by the system owner only under the following conditions: (i) the system owner selects the compensating control from NIST Special Publication 800-53, or if an appropriate compensating control is not available in the security control catalog, the organization adopts a validated compensating control; (ii) the system owner provides a complete and convincing rationale for how the compensating control provides an equivalent security capability or level of protection for the information system and why the related baseline security control could not be employed; (iii) the system owner assesses the adequacy of the control, and (iv) the authorizing official formally accepts the risk associated with employing the compensating control in the information system. The system owner must document approved use of compensating security controls in the security plan for the information system.

The use of a compensating control should not be used to avoid burdensome controls, as the actual compliant use of a compensating control is often more burdensome than using the original control. In addition, it is not sufficient to simply point to existing NIST SP 800-53 controls implemented on the system as adequate compensation if both the original control and the compensating control were part of the initial baseline. The initial baseline is designed to have related controls supporting each other, so if one of the controls is removed, the related control must be enhanced to pick up the issues addressed by the removed control. For example, control AC-5, *Separation of Duties*, can be compensated by increasing the auditing of system activities, but this increase must be explicitly addressed in the audit family controls. Discussion of the increased audit capabilities would include what additional actions are audited, and how the audit process and records are protected from unauthorized access by system administrators that are being monitored.

7.1.8. Organization-Defined Security Control Parameters

The next opportunity to tailor a control is through the use of *assignment* and *selection* operations for many of the controls. This permits the specific controls to be adjusted to support NOAA, NESDIS, Local Office, and system specific policies. Controls that call for assignment and selection tailoring are identified explicitly in NIST SP 800-53 and typically include items such as reactions to specific events or situations as well as parameters including specific time frames or counts of system events. For example, control AC-7, *Unsuccessful Login Attempts*, permits the assignment of how many unsuccessful logins (count *assignment*) are permitted during an organizationally defined time period (duration *assignment*) before an organizationally defined action (response *selection*) is performed. NESDIS has adopted the assignments that have been standardized by DOC in the ITSPP and/or the NOAA IT Security Manual. Where there is no DOC or NOAA standard, system owners may set a system-specific standard and document this in the SSP.

7.1.9. Supplement the Baseline

Additional controls can be added to the baseline from or in addition to the catalogue of controls in NIST SP 800-53 to protect against risks unique to the system. For example, control AC-9, *Previous Logon (Access)*

Notification, is not required for any baseline, but an SO should choose to select the control if a system function requires such notification to the user. If a risk has been identified that cannot be addressed by a control already defined in NIST SP 800-53, an organizational-defined control may be used, but only as a last resort.

7.1.10. Document the Final Baseline Requirements

FIPS 200 requires that security control baseline tailoring activities be coordinated with and approved by appropriate organizational officials. NESDIS requires that the SO obtain AO approval of the FIPS 200 security control baseline. The approval process is described below in Section 7.2. The ISSO must document the results of the FIPS 200 tailoring in the SSP template, essentially creating the first draft for the control descriptions section of the SSP. See the NESDIS *System Security Plan Development and Maintenance Policy and Procedures* for information on documenting the controls section of the SSP.

A thorough explanation of the rationale behind any tailoring of the control shall be provided as the first piece of information in the control implementation discussion. The discussion shall include an analysis of the operational, technical, and/or fiscal issues preventing implementation of the control. In addition, the discussion shall include an analysis of the change in the risk to the system resulting from the implementation of the tailored or compensating control from the risk that would be present if the original control were implemented. The control implementation details (e.g., specific products, security parameters, etc.) are not required for AO approval unless those details are necessary to explain the use and the adequacy of compensating controls. Controls that are only tailored using the identified assignment and selections requested by NIST SP 800-53 do not require explicit AO approval unless those assignments and/or selections deviate from DOC, NOAA, or NESDIS policies. Examples of assignments include setting minimum password length and number of invalid login attempts before taking an action. The specific action to take after the number of invalid login attempts has been exceeded is an example of a selection. The FIPS 200 analysis and approval memorandum which will be used to obtain AO approval is a subset of the SSP that extracts the specific not selected, tailored, compensated, and supplemented controls.

Controls identified in SP 800-53 as “not selected” for a FIPS 199 impact level controls baseline do not require justification and approval by the AO to be excluded from the baseline; therefore, they are not required to be listed in the FIPS 200 analysis or approval memorandum. This avoids confusion during the A&A and quality assurance of the security authorization package.

All controls modified, supplemented, or tailored, except as noted above, must be identified and justification for such tailoring provided in the FIPS

200 analysis and approval memorandum. All controls that are added to the baseline require explicit AO approval once the control is part of the approved baseline. An updated risk assessment and AO approval is required to remove that control from the baseline.

7.2 Security Control Approval Procedures

The AO must approve the SO selected security control baseline. To maintain a consistent security posture across all NESDIS mission systems, the ITSO will perform a quality and compliance review and provide feedback on all FIPS 200 analyses. Below is the process the SO must follow to obtain the necessary approvals before implementing the selected controls baseline for the information system.

7.2.1 ITSO Concurrence

The NESDIS ITSO provides an organizational perspective into the control selections of all information systems within NESDIS. The ITSO will perform a quality review of the FIPS 200 analysis submission for compliance, completeness, and reasonableness as it relates to the information system (for example, is the correct template used, are the information types and categorizations identified reasonable considering the system's purpose and mission, was the analysis performed correctly and resulting system categorization adequately supported, and are justifications for tailoring reasonable). In addition to the completed FIPS 200 analysis, the SO must submit the AO approved FIPS 199 and the initial SSP, including system diagrams and system description. The ITSO will use this information as the basis for review and analysis of the control selection. For all tailoring and compensating, the SO must provide sufficient rationale for modifying the control from the original NIST SP 800-53 control or for removing the control from the baseline. The ITSO may request additional information, documentation, or clarification for the control selections.

Once the review is complete, the ITSO will provide written feedback on the proposed security controls. If modifications are required, the SO must make the modifications and resubmit them to the ITSO for a second review. The ITSO will provide a memorandum to the SO indicating their concurrence with the selected security controls.

7.2.2 AO Approval

The SO is responsible for ensuring that the FIPS 200 analysis and the ITSO's concurrence are submitted to the AO for review and approval. If required, the AO will meet with the SO and the ITSO to discuss the controls selected. The SO should engage the AO to discuss the costs associated with the controls selected, including any additional funding required to meet the control requirements as documented. The SO should present the AO with a FIPS 200 approval memorandum using the NESDIS template at Appendix A (current versions of templates used in NESDIS can be found on the NESDIS IT Security Handbook website at:

https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php). The AO will document their approval of the FIPS 200 by signing the memorandum. The SO must deliver a copy of the AO approval memorandum that includes the FIPS 200 analysis to the ITSO. The SO must maintain the approved FIPS 200 documentation as part of the system A&A package.

7.2.3 Continuous monitoring / reevaluation schedules

Whenever a risk to the system is identified, the control baseline shall be reevaluated to identify updates to the baseline which would address the risk. The system owner must reassess the control baseline annually as part of the continuous monitoring process, as part of the Risk Assessment and SSP review and update, and whenever a risk to the system is identified. The SO must record the performance of annual reviews and all changes to the FIPS 200 in a Record of Changes/Revisions section of the document.

7.2.4 Reassessing the baseline

There are certain events which can trigger the immediate need to assess the security state of the information system commencing with the FIPS 199 and FIPS 200 analysis and if required, modify or update the current security control baseline. The system owner should evaluate the results of the ISSO’s security impact analysis of changes to the system, and if necessary, consult with the NESDIS ITSO to determine significance of the change. If the ITSO considers the change significant, the system owner should discuss with the authorizing official, who makes the final determination. Examples of such events include, but are not limited to:

- An incident results in a breach to the information system, producing a loss of confidence in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system.
- A newly identified, credible, information system-related threat to organizational operations and assets, individuals, other organizations, or the Nation is identified based on intelligence information, law enforcement information, or other credible sources of information.
- Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security state of the system (for example, changes to the system that are not addressed in the current security control baseline).
- Significant changes to the supported missions and/or business functions or to the information being processed, stored, or transmitted by the information system.

Appendix A: FIPS Pub 200 Security Controls Selection and Approval Memo Template

[Instructions: Copy the below text to a separate document, complete all shaded areas, remove highlighting before presenting to AO for signature on agency letterhead.]

MEMORANDUM FOR: <SO Name>
System Owner
<System Long Name with no acronyms>

FROM: <AO Name>
Authorizing Official
<Office>

SUBJECT: Approval of the Federal Information Processing Standard 200
Security Controls Baseline for <system long name>

I.We have reviewed the Federal Information Processing Standard (FIPS) 200 security controls baseline analysis, dated Month day, 20xx, for <system long name>, System ID NOAA50xx. I/We approve the baseline as described in the attachment. The baseline is consistent with the system's security categorization of <High, Moderate, or Low> as documented in the FIPS 199 analysis approved Month day, 20xx.

You are required to review the FIPS 200 and update it as necessary, at least annually as part of the System Security Plan and risk assessment annual review, as well as whenever a significant event occurs, including but not limited to: an incident results in a breach to the information system; a newly identified, credible, threat to organizational operations and assets, individuals, other organizations, or the Nation is identified, or upon significant change to the system environment. Also, you must update the FIPS 200 Record of Changes for each review and update performed. All FIPS 200 changes require my/our written approval, and at a minimum, you must submit it for my written approval at least every 3 years as part of the system assessment and authorization process, even if there has been no change to the FIPS 200.

You must retain this approval memo as part of the system's certification and accreditation package documentation.

Attachment

cc:
<ITSO Name>/ITSO/NESDIS CID
<ISSO Name>/<System Name> ISSO/<System Office>

Attachment

FIPS 200 Analysis for <System Name> (NOAA50xx)

FIPS Publication 200 requires the selection of security controls based on the FIPS 199 categorization. NIST Special Publication 800-53 provides guidance for the selection of the security controls. Using the FIPS Publication 199 categorization and NIST SP 800-53, the **<High/Moderate/Low>** baseline of controls as defined in NIST SP 800-53 Revision X has been selected for implementation in <System Name and Acronym> (NOAA50XX) with the following adjustments made through the selection and tailoring process:

*[**Note**: Text provided as an example only. Replace with system specific data. List all controls that are to be not implemented and completely tailored out of the minimum baseline, controls that are permanently only going to be only partially implemented, and provide narrative rationale to support why they ate not implemented or partially implemented. Delete this Note from the final document.]*

Control	Control Name	Status[1]	Rationale
All XX-1 controls	XX Control Policy And Procedures	Partially Implemented/ Common	Policies are a NOAA Common Control. System owner must document system-specific procedures.
AC-2	Account Management	Implemented/ Upgrade	Added control to the baseline because it provides necessary additional protection for adequate identity proofing prior to granting access.
AC-5	Separation of Duties	Not implemented/ Compensated	Organization staffing level does not permit sufficient division of duties. All Audit and Accountability (AU) controls have been increased to compensate for excessive duties.
AC-12	Session Termination	Partially implemented/ Compensated	AC-12 is tailored for partial implementation. AC-12 is not implemented in the Industrial Control System enclave because consoles must be active 24x7x365 to support critical mission operations. The control must be fully implemented for all other devices that do not support this part of the mission. Physical access controls (PE-3) and monitoring of physical access (PE-6) have been increased in the ICS enclave to compensate for active sessions on operator consoles.
AC-15	Automated Marking	Not implemented/ Downgrade	AC-15 was tailored out of the baseline. NIST SP 800-53 identifies AC-15 as a confidentiality-only control. Since NOAA50XX has a low confidentiality and AC-15 is not required for low confidentiality, AC-15 was removed from the baseline
AT-2	Security Awareness	Implemented/ Common	NOAA Common Control
IR-2	Incident Response Training	Implemented/ Common	NOAA Common Control
IR-3	Incident Response Testing and Exercises	Implemented/ Common	NOAA Common Control
IR-4	Incident Handling	Implemented/	NOAA Common Control

Control	Control Name	Status[1]	Rationale
		Common	
IR-5	Incident Monitoring	Implemented/ Common	NOAA Common Control
IR-6	Incident Reporting	Implemented/ Common	NOAA Common Control
IR-7	Incident Response Assistance	Implemented/ Common	NOAA Common Control
SC-17	Public Key Infrastructure Certificates	Not Implemented/ Not Selected	NOAA 50XX does not use PKI technology.

Note 1: The 7 Status options are: Implemented/Common; Implemented/Upgrade; Implemented but with Compensating Controls; Implemented/ Partially Compensated; Partially implemented/ Mitigated; Not Implemented/ Downgrade; and Not implemented/Not selected.

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
1.0	8/19/2008	All	System Owner	Initial Issuance
1.1	8/19/2009	Date and version	System Owner	Annual review
2.0	10/31/2009	Tailor AC-12	ISSO	Additional tailoring; requires AO approval

Signatures

We have reviewed the FIPS 200 analysis documented herein and concur that it reflects the security controls baseline that will adequately protect the NOAA50xx system.

Name Date
System Owner

Name Date
NESDIS ITSO

Approval Page

Document Number: NQP-3404, Revision 2.1	
Document Title Block: **Federal Information Processing Standard 200 Controls Selection and Tailoring Policy and Procedures**	
Process Owner: NESDIS Chief Information Office	Document Release Date: September 1, 2011

Prepared by:

Erica Boyd 3/25/15

Erica Boyd
Ambit- Associate Consultant
NESDIS Chief Information Office

Date:

Approved by:

Irene Parker 3/25/15

Irene Parker
Assistant Chief Information Officer - Satellites

Date:

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
2.1	**March 25, 2015**	**----**	**ALL**	**Baseline NQP-3404**