NESDIS

Security Assessment Report Policy and Procedures

September 28, 2012

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 FOR: Distribution

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 often 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.

NESDIS Security Assessment Report Policy and Procedures

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
0.1	8/14/2009	All	Noblis	Initial Draft Delivery
0.2	9/10/2009	All	ITSO	Updated for ITSO comments
0.3d	1/30/2010	2.0, 7.0, 7.2, 7.4, 7.5	ITSO	Updated for IRMT Security Team comments
0.4d	5/17/2010	Appendix A	Noblis	Minor grammatical updates based on ISSO Comments
0.5d	7/14/2010	Header/footer, 5.1	ITSO	Delete FOUO markings; updated References; changed "CT&E" to "assessment"
1.0	8/10/2010	All	ITSO	Finalize and prepare for issuance
1.1	6/30/2012	All	ITSO Support Staff	Biennial Update
2.0	9/28/2012	All	ITSO	Finalize and prepare for CIO issuance

1.0 Background and Purpose

The Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541, *et seq*., and the Office of Management and Budget Circular A-130 Appendix III require management authorization (accreditation) of all information systems to store, process, or transmit federal data. The Department of Commerce (DOC) *IT Security Program Policy* (ITSPP) requires compliance with National Institute of Standards and Technology (NIST) guidance, specifically NIST Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, for implementing the security Assessment and Authorization (A&A) process. NIST SP 800-37 establishes the Security Assessment Report (SAR) as one of the three key documents contained in the system Security Authorization Package, along with the System Security Plan (SSP) and Plan of Action and Milestones (POA&M). It states that the purpose of SAR is to provide the results of determining the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements. NIST SP 800-37 (Subtask 4.3) also states that "The results of the security assessment, including recommendations for correcting any deficiencies in the security controls, are documented in the security assessment report."

For National Environmental Satellite, Data, and Information Service (NESDIS), the SAR is prepared by or the Certification Agent (CA) (or "Certifier") in accordance with the requirements of NIST SP 800-53A, Revision 1, *Guide for Assessing Security Controls in Federal Information Systems and Organizations*, Appendix G. The purpose of the *NESDIS Security Assessment Report Policy and Procedures* is to document the requirements of the SAR preparation so that it is acceptable to NESDIS, National Oceanic and Atmospheric Administration (NOAA), and DOC.

2.0 Scope

The scope of this document is limited to establishing the NESDIS requirements for preparation of the SAR, and is to provide the requirements for the content of the SAR. This document does not provide detailed instruction on how to conduct security control assessment activities. See the *NESDIS Policies and Procedures for Conducting Security Controls Assessments* for such guidance.

NESDIS provides a SAR template on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_policy/it_security/it_security_policy.php that is compliant with the recommendations of NIST SP 800-53A, Revision 1, Appendix G.

All NESDIS employees and contractors responsible for preparing or supporting security control assessment report activities for NESDIS information systems, including contractor-owned and -operated systems which contain NESDIS information, must comply with the policies and procedures identified in this document.

3.1 Roles, Responsibilities, and Coordination

The roles and responsibilities for key participants involved in security controls assessment for NESDIS systems are consistent with those described by NIST. Participants in the assessment process and their roles and responsibilities are listed below.

3.2 Authorizing Official (AO)

The AO determines the required level of security control assessor independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The AO determines if the content of the security assessment report is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.

3.3 Chief Information Officer (CIO)

The NOAA Assistant CIO for Satellite and Information Services establishes and oversees the NESDIS-specific security assessment reporting requirements.

3.4 Information Technology Security Officer (ITSO)

The NESDIS ITSO oversees the independent CA function for NESDIS systems of all impact categorizations. The NESDIS ITSO reviews for adequacy the selection of the security assessment targets, Security Assessment Plans, and reviews SARs for coverage, comprehensiveness, completeness, and correctness in determining the adequacy of the report for use to determine risks supporting A&A of the system.

3.5 System Owner (SO)

The SO provides the security control assessment team with the necessary access to the information system, system documentation, and system personnel so that the team may adequately assess the security controls. The SO is also responsible for reviewing the SAR and providing comments or clarifications to the security control assessor. The SO must also address all SAR recommendations by converting them into POA&Ms[1] or by updating the security controls baseline[2]. The SO is responsible for communicating the assessment results to the AO when requesting initial system authorization or annual system re-authorization.

3.6 Certification Agent (CA)/ Certifier

The NESDIS ITSO oversees the independent CA function for NESDIS systems of all impact categorizations. Certifier responsibilities as described in NIST SP 800-37 Revision 1 may be performed by the NESDIS ITSO or by direct support federal staff or contractors as delegated. The CA is responsible for determining the adequacy of the system documentation – including the SAR – and communicating the results of the security assessment, including recommendations for corrective actions, to the SO.

3.7 Security Control Assessor/Assessment Team

The security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

[1] See NESDIS *Plan of Action and Milestones Management Policy and Procedures* for more information.

[2] See NESDIS *FIPS 200 Security Control Selection and Tailoring Policy and Procedures* for more information.

Assessors should also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and recommend actions for correcting identified deficiencies in the security controls. In addition, assessors may assist the CA in preparing the final SAR containing the results and findings from the assessment.

4.0 Management Commitment

The NESDIS Chief Information Division (CID) supports the NESDIS Assistant Administrator's strong emphasis on securing NESDIS information and information systems. Through the issuance of this policy and procedures document, the OCIO demonstrates its commitment to the consistent and comprehensive security assessment supporting A&A for every NESDIS system.

5.1 Compliance

NESDIS requires the assessment team or Certifier to prepare and coordinate the SAR in compliance with the policies and procedures described in this document. The NESDIS ITSO/CA will review the SAR and supporting artifacts to ensure compliance with this policy. SARs found not in compliance will be returned for revision, thereby jeopardizing the timely authorization of the system.

5.2 References

- DOC ITSPP section 4.4.1, Row 2 (January 2009)
- NOAA *Risk Management Framework Process* (v10.0, November 2011)
- NESDIS *Risk Management Framework Assessment & Authorization Process Policy and Procedures* (v2.1, September 1, 2011)
- NIST SP 800-53A Revision 1, Appendix G (June 2010)

6.1 Policy

As required by DOC ITSPP section 4.4.1, the NESDIS-specific SAR procedures shall align with the NIST SP 800-37 Revision 1 prescribed practices for A&A and the NIST SP 800-53A Revision 1 recommendations for report format and content. NIST SP 800-37 identifies a number of tasks and subtasks required for each phase of a general A&A process. This document provides NESDIS-specific procedures for developing the SAR as one of the A&A subtasks and should be used as companion document for implementation of NIST SP 800-37 and NIST SP 800-53A within NESDIS and not as a replacement document.

6.2 Policy Maintenance

The NESDIS ITSO shall review this policy and procedures bi-annually 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.

6.3 Policy Feedback Process

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

6.4 Policy Effective Date

This policy is effective within 30 days of issuance.

7.1 SAR Development Procedures

Before preparing the SAR, NESDIS requires that the assessment team follows the NIST SP 800-53A methodology to assess and document the results of the security control implementation status.[3] Next, the team must document the summary results for the CA and ultimately the SO and AO. For NESDIS information systems, the assessors must ensure that NESDIS-specific concerns are addressed in the controls assessment or the SAR (see Appendix A: NESDIS-Specific Areas of Concern in the SAR).

The SAR shall be prepared by the CA and shall report deficiencies at a component level for each applicable control. For purposes of the NESDIS SAR, the concept of a component is an individual item or one instance of an item that is the subject of an evaluation. A component may be a single facility, a building, a room, a document, a piece of IT equipment, an operating system, an application, or an element of information depending on the subject of the control.

The Federal Information Processing Standard (FIPS) 199 categorization (i.e., high, moderate, or low) and the FIPS 200 controls baseline tailoring and selection drive the control baseline requirements for the system.[4] For A&A, every control in the system's security controls requirements baseline shall be addressed as either:

- **Not Selected.** If the AO has approved not including the control as part of the system's controls baseline as recommended by NIST SP 800-53 for the system's FIPS 199 categorization, then the control should be identified as "Not Selected." Controls that are Not Selected are not assessed by the assessment team.
- **Satisfied.** If the assessment team has thoroughly assessed and documented the assessment evidence for the security control and determined that the control meets the control implementation as defined in the system's SSP, then the control can be identified as "Satisfied."
- **Other than Satisfied.** If the assessment team has thoroughly assessed and documented the assessment evidence for the security control and determined that the control does not meet the control implementation as defined in the system's SSP, the control must be identified as "Other than Satisfied." The "Other than Satisfied" category can be further broken down into "Not Satisfied" or "Partially Satisfied."

The SAR is also a report of the security assessment process. As such, it provides the scope and methodology for the assessment of the system status at a particular time (as documented in the Security Assessment Plan approved prior to commencing the assessment

[3] See the NESDIS *Policies and Procedures for Conducting Security Controls Assessments* for controls assessment documentation requirements. [4] See the NESDIS *Federal Information Processing Standards Publication (FIPS) 199*

policy and Procedures and the NESDIS *FIPS 200 Security Control Selection and Tailoring Policy and Procedures* for more information.

if for a certification assessment). The SAR must also be updated during the system certification coordination process to represent the system as accurately as possible at the time of final submission to the AO. This SAR coordination and finalization process occurs after the initial SAR is delivered to the SO for review. The SO may challenge the results of a control finding or immediately mitigate deficiencies, and present the assessment team with additional evidence to reverse an identified control deficiency. If the CA is satisfied that the control is implemented properly, the SAR must be updated to reflect the new assessment.

The SAR is the resulting product used by the AO to evaluate the security posture of the information system and make a credible risk-based authorization decision for authorizing the system to operate. The process of creating the SAR involves five steps as described below in sections 7.1 through 7.5:

- Plan the Control Assessment
- Perform the security assessment – Security Testing and Evaluation (ST&E) or Security Control Assessment (SCA)[5]
- Collect the testing artifacts and document the results
- Assess the results and create the SAR
- Validate the results with the SO and the ITSO (SAR coordination)

Each of these steps is discussed in detail below.

7.2 Plan the Control Assessment

Control Assessment Planning provides for coordination of the activities and preparation of the templates and forms necessary to collect and analyze the results of the testing. The conduct and documentation of the assessment is addressed in detail in the *NESDIS Policy and Procedures for Conducting Security Controls Assessments*. For the purposes of the SAR, the key step in control assessment planning is the selection of the targets for assessment. NIST SP 800-53A allows the assessment team to assess a subset of system components if they are similarly configured. The Security Assessment Plan[6] and the SAR must document the rationale used to select the specific targets and as well as the rationale for why limiting testing to those targets provides for adequate coverage to make a determination for each control implementation. This information must be documented in the SAR.

7.3 Perform the Controls Assessment

The Controls Assessment must be performed in accordance with the *NESDIS Policy and Procedures for Conducting Security Controls Assessments*. The results from the control assessment must be documented in the assessment report, using the

[5] ST&E is an assessment performed for the purpose of system developer “factory” testing of security control functionality prior to delivery to the government for purposes of Interim Authorization to Test (IATT) in the production system environment test bed. SCA is an assessment performed specifically for the purpose of system authorization as part of the initial and annual authorization to operate process.

[6] See the NESDIS *Risk Management Framework Assessment & Authorization Process Policy and Procedures*, section 7.4, for more information on the security assessment plan.

NOAA Security Controls Assessment Report template. The current versions of the IT security policies, procedures, templates, and checklists can be found on the NESDIS IT Security Handbook Resources website at: https://intranet.nesdis.noaa.gov/ocio/it_policy/it_security/it_security_policy.php. The summary of the results must be transferred into the SAR where appropriate.

7.4 Controls Assessment Template and Artifacts

The assessment team shall submit all testing artifacts collected during the test execution with the final assessment report. The SO will maintain the artifacts for delivery to the ITSO, AO, NOAA, and DOC if required. The *Security Control Assessment Policy and Procedures* document defines acceptable control testing artifacts.

7.5 SAR Assessment and Preperation

Once the testing is completed, the CA must assess the results and prepare the SAR. The CA must document the following in the SAR:

- Summary information for each control family
- The methodology utilized for testing
- The depth and coverage of testing
- Details of the vulnerability scan results
- Details of the penetration testing results (if applicable)
- Evaluation of the system inventory
- Details of the secure configuration baselines
- Detailed security control testing results
- Recommended corrective actions for mitigating the deficiencies identified
- The risk determination
- The authorization recommendation
- Details of the web application scan results (if applicable)
- The scan-to-inventory coverage calculation from the vulnerability assessment (for more information, see the *NESDIS Vulnerability Scanning Policy and Procedures*, currently under development)
- Summary results from the Privacy Impact Assessment or Privacy Threshold Assessment
- Summary of the E-authentication Risk Assessment
- Summary of how the CA and assessment team was organizationally independent of the SO

This additional information may be integrated into the SAR where appropriate or included as a NESDIS specific section of the SAR.

7.6 SAR Coordination

Once the SAR is drafted, the CA must share the draft SAR with the SO and provide the SO 10 business days to review, correct any deficiencies, dispute the results, confirm the POA&Ms and risk-acceptance action items and provide their written feedback to the CA. If the SO corrects any deficiencies, they must include evidence with their written comments submitted. The CA or assessment team must re-assess the control(s) within five business days and revise the SAR as necessary to ensure accurate results are reported. If insufficient time exists to re-assess the control, the CA may document the SO's statement that the control has been implemented properly in the recommended corrective actions section. However, the SAR control assessment results should reflect the initial findings for which mitigation has not been independently validated. Under no circumstances should the control assessment be modified without independent re-assessment of supporting artifacts.

After the SO has provided input into the accuracy of the SAR, and the CA has updated the SAR based on new information from editorial changes and the results of any additional follow-up assessments, the CA finalizes and delivers the SAR to the SO along with the Certifier's Recommendation Memorandum signed by the CA at least 10 days prior to the authorization/re-authorization date for inclusion in the final Security Authorization Package for the AO's authorization decision.

Appendix A: NESDIS-Specific Areas of Concern in the SAR

A.1 Overview

The assessment team is responsible for assessing the security controls of the system. These controls are expressed in the System Security Plan (SSP) package that includes a number of ancillary documents supporting the SSP. This section addresses the critical assessment areas that must be addressed during the SCA of the control findings and preparation of the SAR. In the context of the SAR, the assessment is conducted for the purpose of gathering evidence of component control implementation. The SCA activity is conducted for the purpose of determining relevance of the assessment findings to whether the system adequately implements the control.

A.2 Content of the System Security Plan

The *NESDIS System Security Plan Development and Maintenance Policy and Procedures* document provides the template and overall guidance for developing the SSP within NESDIS. The SSP must address a variety of items in addition to providing a description of the implementation of the security controls. The assessment team examines the SSP for compliance with NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, during the assessment of control PL-2. Following is a list of critical issues that the assessor must examine to determine if the SSP meets NOAA and DOC requirements.

SSP Section 2 – This section must address the FIPS 199 impact level. The FIPS 199 impact level must be shown to be consistent with the FIPS 199 approval. It does not need to copy the full analysis if that analysis is included in the package and referenced either in the SSP or in the enclosed FIPS 199 approval.

SSP Section 7 – This section should address the operational status of the system, and subsystems (if different). For example, if a new subsystem is the reason for the A&A, the system may be operational while the new subsystem is completing development and should be separately identified as new.

SSP Section 9 – NOAA and DOC have specific content requirements that must be met for an acceptable SSP. This section must include a detailed topology narrative and graphic that clearly depict the system boundaries, system interconnections, and KEY devices within it as verified during assessment.[7] It must contain a coherent and concise description that includes how system components are dispersed in various geographic locations. A well defined authorization boundary is critical. Logical and physical diagrams need to be fully described in the SSP, as well as:

- The system component architecture and the information flows both must be described in this section.
- Boundary Protection for the external connectivity and the connection between subsystems of different impact levels must be clearly articulated. DOC requires that each public accessible network have a network-based IDS installed. In

[7] This does not require depicting all workstations on every desktop, but must include all perimeter security devices, firewalls, routers, switches, file/print/application servers, and example workstations and networked print devices.

addition, DOC requires that each host (server) that could be accessed, including all hosts on that network, must have a host-based IDS installed. This description must be consistent with the control implementation described in control SC-7.

- Remote access must be described and the reasons for use presented. This includes the use of VPN architectures for access from either home, remote work sites, or commercial access points. (The control implementation for AC-17 must be consistent with the description provided in this section.)
- If a Demilitarized Zone (DMZ) architecture is used for isolation of public access, the section must identify and describe the DMZ including each and every network component and every host in the DMZ. Address how the information gets to the DMZ servers and how it moves to and from the operational network.
- This section must describe how workstations (if applicable) are managed to provide consistency in configuration and application support. Describe how the workstations are identified to the network and how unauthorized workstations are identified or discovered. Address the use of laptops on the network. This topic must be consistent with control AC-19.
- Hardware and software inventory must be shown to be consistent with the network scans. The SSP diagrams and descriptions must be 100% consistent with the inventory as verified by assessment including device identifiers. The SSP and inventory must be 95% consistent with the scans. The summary data for the inventory is required in the system description. Detailed information may either be included in the SSP body or in a separate attachment. If separate, the summary must be shown to be consistent with the detailed data by the assessment team.

SSP Section 10 – This section addresses the environment within which the system operates. It must describe each facility, the interaction between the system and the management of the facility, and the protections afforded for the system by the facility. Every facility that supports components within the security boundary must be addressed including all backup sites for storage or contingency operation. This section must also address the major applications (not the software since that is part of software inventory) supported and the user environment including the general types of public users of the information provided to the public.

SSP Section 11 – Interconnections require detailed information about the system connected to, including points of contact, FIPS categorization, details of the physical connection, details of the interconnection agreements, and documentation of the formal approval for the connection. For logical connections that involve sharing information, the SSP must also document the information shared and any security concerns[8] for sharing that information. The assessment team must ensure that each interconnection identified in the SSP is documented in this section and supported by an Interconnection Security Agreement or acceptable alternative.

SSP Section 16 – The Minimum Security Controls section of the SSP documents the implementation details and plans for implementation of the security controls required

[8] Security concerns revolve around the confidentiality, availability or the integrity of the information shared.

by the FIPS 200 analysis and approval. Key elements for each description are addressed in a general form in this guidance. Detailed guidance is provided in appendix A of the NESDIS SSP Development P&P.

Implementation of the Common Controls – Where a common control is used for partial or full evidence of compliance for a control, the assessment must show evidence that the information system can actually take advantage of the common control implementation[9]. For Hybrid controls, the evidence must be provided that the system completed the full requirement of the common control. The SAR must identify each instance where this evidence is not provided.

Evidence of control implementation – Where a control is implemented on a single component, the evidence must identify the component and the result of the control assessment. Where the control is implemented on more than one component, the evidence must support the implementation on each of the individual components.

Where a control is implemented on a number of identical components (e.g, instance of an operating system), an adequate sample must be tested, and the results for each tested component provided. The SAR should summarize the result of the evidence as denoted above in the content description.

Accounting for “other than satisfied” results – Where the result of a test is other than satisfied, the identification of the POA&M, estimated completion date, and detailed corrective action plan must be documented in the SSP as a part of the security control implementation description. This content must be shown to be consistent with the POA&M provided in the security package.

Accounting for controls that are not implemented – The FIPS 200 approval identifies each control or control enhancement that is to be excluded from the baseline. The use of “Not Selected”, “Not Applicable”, and “Tailored” should be consistent with the FIPS 200 approval.[10]

A.3 Consistency Between Documents

The A&A package consists of three primary documents; the SSP, the POA&M, and the SAR. However, a number of other documents are processed separately that are considered part of the SSP. These include the test reports, scan results, inventories, risk assessment, FIPS approvals, interconnection agreements, Contingency Plans, rules of behavior, and other documents supporting the evidence of control implementation.

This section addresses those areas that have previously been identified as creating inconsistencies and that should be specifically addressed by the assessment team.

[9] For example, if the information system relies on the NOAA common control for spam control, the information system must receive all if its mail using the NOAA implemented mail services. If the information system implements its own mail services, the NOAA controls may not be applicable.

[10] It is also necessary to ensure that the FIPS 200 approval does not exclude security controls that the SO has decided to implement. Controls implemented by the SO that are excluded from the approved FIPS 200 may result in additional system risk that may not be acceptable to the AO. For example, if Voice over IP was excluded from the control baseline in the approved FIPS 200 but the SO decided to implement it anyway, even if the implementation is consistent with NIST SP 800-53 control requirements, it may introduce unnecessary and unapproved risk to the system.

Scan to Inventory – There are a number of reasons why the scans for a system differ from the documented inventory and many are justifiable. Due to this, NESDIS has established a 95% consistency requirement between the inventory provided in the SSP and the scan results. The assessment team shall document in the SAR summary the validation of the inventory and scan consistency to provide an inventory accuracy assessment. More details on the calculation of the scan to inventory coverage can be found in the Vulnerability Scanning Policy and Procedure.

FIPS 200 approval – The FIPS 200 approval serves to establish the control baseline for the system and component subsystems (where used). The assessment team is required to ensure the approved FIPS 200 is consistent with the SSP and the controls tested. Any deviation from the approved FIPS 200 must be documented in the SAR.

Approved FIPS 199 compared to the actual system information content – The assessment team shall determine if the FIPS 199 information components are inconsistent with the information processed, stored, or transmitted by the system. The result of this assessment shall be documented in the SAR.
Control discrepancy to POA&M – Any instance of a discrepancy that is incorrectly or incompletely addressed in the POA&M shall be documented in the control assessment of the SAR.

System description to control description – Any inconsistency between the SSP section 9 and section 10 descriptions and the control descriptions or test findings shall be documented in the control assessment of the SAR.

System diagrams to inventory – The system diagrams must precisely match the inventory and the descriptions in the SSP. Any discrepancy or inconsistency between the system diagram labels and the description and inventory shall be documented in the SAR in the general discussion of the inventory or in the discussion of the SSP section in the summary. The CA shall provide a summary statement of the findings in the summary of the SAR.

Test result to current system – In some cases the assessment results may not match the current implementation due to the SO taking corrective action subsequent to the conduct of the assessment. Where this has been shown to have occurred, the CA shall ensure the test results match the actual tests performed. If the SO claims a control is properly implemented after testing has completed, the CA may, at their discretion, update the SAR to document the SO’s claim of control satisfaction. However, the control test results must reflect the actual testing performed.

Risk Assessment report to Assessment results – In many cases the risk assessment was performed prior to the final assessment report being completed. As a result there are inconsistencies between the system risk assessment and the actual risk posture of the system. The CA shall document the necessary changes to the risk assessment under control RA-3 to accommodate changes occurring during the final control assessment of the system and ensure that it accurately reflects the POA&M.

A.4 Other Considerations

The A&A package, generically identified as the SSP, must also address specific items that are not specific to the SSP guidance provided in NIST SP 800-18. The issues generally support implementation of OMB, DOC and NOAA guidance supportive of FISMA requirements.

Secure Configuration Baselines are identified to be established under control CM-6. The following verification is to be performed for control CM-6:

- Secure baselines are identified for all operating systems, and minor applications (web servers, DB servers, LDAP, application servers, etc);
- The assessment team evaluated that the baselines to determine if they are secure (most restrictive mode consistent with operational requirements);
- The assessment team evaluated that the components are actually configured to the secure baseline with deviations identified and fully documented in CM process; and
- Verify and document if Security Technical Implementation Guides11 were used and tested for each operating system and database instance.

Penetration testing is performed in accordance with the *NESDIS Penetration Testing Policy and Procedures* (under development). The basic requirement is for FIPS 199 High impact and other selected systems to be subjected to penetration testing. The results are provided in support of control CA-2 (Security Assessments). The CA shall identify in the summary if the system was subject to penetration testing and if so, summarize the results. Key elements of the test verification are:

- Verify that the penetration testing meets the policy and procedures.
- Ensure the results are merged with the rest of the findings in testing and scanning.
- Document whether the SO corrected the results after testing occurred.
- Document whether the system was re-tested/verified after correction.
- Verify that the POA&M reflects the Penetration Test corrective actions required.

Contingency planning is implemented under the Contingency Planning family of controls in accordance with the *NESDIS Contingency Planning Policy and Procedures*. The assessment team shall document in the summary the following concerns:

- Verify that the Contingency Plan meets the requirements for the family in general.
- Ensure that evidence is provided that the defined recovery time is acceptable given the system's FIPS 199 impact level.
- Verify that the Contingency Plan was fully tested and documented in accordance with policy and requirements.
- Identify any significant deficiencies in the Contingency Plan based on the state of the system's controls, penetration test, scans, etc.

[11] See Defense Information Systems Agency website at http://iase.disa.mil/stigs/stig/index.html for more information.

Privacy Assessment is conducted under control PL-5. The assessment team shall verify and document in PL-5 the following:

- That a Privacy Threshold Analysis (PTA) and, if applicable, Privacy Impact Assessment (PIA) were performed and documented using the required templates (see the NESDIS IT Security Handbook Resources website https://intranet.nesdis.noaa.gov/ocio/it_policy/it_security/it_security_policy.php for current templates).
- That the PTA was approved by NOAA's Privacy Coordinator.
- That the information in the PTA/PIA is consistent with the information described in the SSP and FIPS 199 as processed by the system.

E-authentication Assessment must be conducted under OMB Memorandum 04-04 and used to determine NIST SP 800-63 compliance within control IA-8. The assessment team shall verify and document in the assessment of IA-8 the following:

- That the E-authentication Threshold Analysis (ETA) and, if applicable, E-authentication Risk Assessment (ERA) were conducted and properly documented using the required templates. See the NESDIS IT Security Handbook Resources website at https://intranet.nesdis.noaa.gov/ocio/it_policy/it_security/it_security_policy.php for current templates). An online tool for the ERA is available at http://www.idmanagement.gov/eauthentication.
- That the ERA, if applicable, is consistent with the data processed and document that under control IA-8.
- That the system fully implements the correct authentication mechanisms based on the results of the ERA, if applicable. If not, verify that the rationale is fully documented and approved by the AO.

Approval Page

Document Number: NQP-3408, Revision 01	
Document Title Block: **Security Assessment Report Policy and Procedures**	
Process Owner: NESDIS Chief Information Office	Document Release Date: September 28, 2012

Prepared by:

Erica Boyd

Erica Boyd
Ambit- Associate Consultant
NESDIS Chief Information Office

3/26/15
Date:

Approved by:

Irene Parker

Irene Parker
Assistant Chief Information Officer - Satellites

3/26/15
Date:

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
2.1	March 26, 2015	----	ALL	Baseline NQP-3408