

# **NOAA/NESDIS**

## **Risk Management Framework Assessment & Authorization Process 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

## Table of Contents

1.1	Background and Purpose.....	7
2.0	Scope .....	8
3.1	Roles, Responsibilities, and Coordination .....	8
3.2	Head of Agency/Chief Executive Officer .....	8
3.3	Risk Executive Function .....	9
3.4	Chief Information Officer (CIO).....	9
3.5	Authorizing Official (AO).....	10
3.6	Information Owner/Steward .....	11
3.7	Senior Agency Information Security Officer (SAISO).....	11
3.8	Authorizing Official’s Designated Representative (AODR).....	11
3.9	Common Control Provider (CCP).....	11
3.10	Information System Owner (ISO, or SO) .....	12
3.11	Information System Security Officer (ISSO) .....	12
3.12	Information Security Architect.....	13
3.13	Information System Security Engineer.....	13
3.14	Security Control Assessor (SCA) .....	14
4.0	Management Commitment .....	15
5.1	Compliance.....	15
5.2	References.....	15
6.1	NESDIS A&A Process Policy.....	15
6.2	Policy Maintenance .....	15
6.3	Policy Feedback Process.....	16
6.4	Policy Effective Date .....	16
7.1	NESDIS A&A Process Procedures.....	17
7.2	Step 1 Procedures: Categorize Information System.....	17
7.3	Step 2 Procedures: Select Security Controls .....	19
7.4	Step 3 Procedures: Implement Security Controls .....	24

7.5	Step 4 Procedures: Assess Security Controls.....	26
7.6	Step 5 Procedures: Authorize Information System .....	29
7.7	Step 6 Procedures: Monitor Security Controls.....	31



**UNITED STATES DEPARTMENT OF COMMERCE**  
**National Oceanic and Atmospheric**  
**Administration**  
NATIONAL ENVIRONMENTAL SATELLITE, DATA, AND  
INFORMATION SERVICE

**MEMORANDUM FOR:** Distribution

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

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

This is to announce the issuance of one new, and four 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

- NESDIS *Risk Management Framework Assessment & Authorization Process Policy and Procedures* (an update of the previous publication entitled the *NESDIS Certification & Accreditation Process Policy and Procedures*),
- NESDIS *Federal Information Processing Standard 199 Security Categorization Policy and Procedures* (updated to reference the Risk Management Framework),
- NESDIS *Federal Information Processing Standard 200 Controls Selection and Tailoring Policy and Procedures* (updated to reference the Risk Management Framework),
- NESDIS *System Security Plan Development and Maintenance Policy and Procedures* (updated to reference the Risk Management Framework), and the
- NESDIS *IT Systems Component Inventory Management Policy and Procedures* (new).

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.

NESDIS Quality Procedure [NQP] – 3401  
Revision 2.2

Effective Date: September 1, 2011  
Expiration Date: Until Superseded

These documents will be posted to the Chief Information Division's Web site at <https://intranet.nesdis.noaa.gov/ocio/itsecurity/handbook/itsecurityhandbook.php>. If you have any questions, please contact the NESDIS IT Security Officer, Nancy DeFrancesco, at [Nancy.DeFrancesco@noaa.gov](mailto:Nancy.DeFrancesco@noaa.gov) or phone (301) 713-1312.

**NESDIS RISK MANAGEMENT FRAMEWORK ASSESSMENT AND  
AUTHORIZATION PROCESS POLICY AND PROCEDURES**

**Record of Changes/Revisions**

<b>Version</b>	<b>Date</b>	<b>Section</b>	<b>Author</b>	<b>Change Description</b>
1.0	08/31/2009	Sections 3.1, 3.2, 3.3, 3.7, 3.9, 7.1, 7.2, and 7.4	N.DeFrancesco	Address final comments and finalize for CIO issuance.
1.1	10/27/2009	Cover page	N.DeFrancesco	Correct spelling of “Accreditation” on cover page
2.0	08/11/2011	All	N.DeFrancesco	Update to align with NIST SP 800-37 Revision 1, the RMF A&A process
2.1	9/01/2011	All	N.DeFrancesco	Removed Draft markings and finalized

## 1.1 Background and Purpose

The Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541, *et seq.*, and the Office of Management and Budget (OMB) 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) *Information Technology Security Program* (ITSPP) require compliance with National Institute of Standards and Technology (NIST) guidance; specifically, NIST Special Publications (SPs). NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 2010), provides recommendations for implementing the security assessment and authorization (A&A) process.

Security assessment and authorization are important activities that support the NESDIS risk management process and are integral to the organization's information security program.

The information and supporting evidence which must be provided for the security A&A of an information system are collectively referred to as the security authorization package. The costs however, for developing a compliant A&A package that demonstrates adequate protection of NESDIS information systems and upon which management can make fully informed risk-based decisions, can be substantial and overly burdensome without a NESDIS-wide and NESDIS-specific standardized A&A approach. To achieve the highest degree of cost effectiveness with regard to security and the A&A process, the NESDIS Chief Information Division (CID) augments this publication through issuance of supplemental policies, procedures, handbooks, and guides that provide a foundation for consistent implementation of information system security practices across NESDIS including, but not limited to:

- NESDIS *Federal Information Processing Standards Publication (FIPS) 199 Policy and Procedures*
- NESDIS *FIPS 200 Security Control Selection and Tailoring Policy and Procedures*
- NESDIS *System Security Plan Development and Maintenance Policy and Procedures*
- NESDIS *Continuous Monitoring Planning Policy and Procedures*
- NESDIS *Policy and Procedures for Conducting Security Controls Assessments*
- NESDIS *Vulnerability Scanning Policy and Procedures (under development)*
- NESDIS *Penetration Testing Policy and Procedures (under development)*
- NESDIS *Plan of Action and Milestones Management Policy and Procedures*
- NESDIS *Configuration Management Policy and Procedures (under development)*
- NESDIS *Common Control Policy and Procedures (draft currently out for comment)*
- NESDIS *IT Security Training Policy and Procedure*
- NESDIS *Guide for Determining Minimum Documentation Requirements for System Interconnections*

- *NESDIS Annual Risk Assessment Update Guidance*

The purpose of this document is to communicate NESDIS policy and describe the NESDIS-specific process procedures for implementation of the A&A requirements of NIST SP 800-37 Revision 1 within NESDIS. Users of this document must also utilize NIST SP 800-37 Revision 1 to understand the entire A&A process for NESDIS systems. In addition, it also provides a roadmap of NESDIS specific policies and procedures required to successfully plan and implement A&A. This document is not intended to be a stand-alone A&A handbook and intimate knowledge and understanding of NIST SP 800-37 Revision 1 is recommended to successfully execute A&A. Training on the NESDIS A&A process is available online.<sup>1</sup>

## **2.0 Scope**

The scope of this document is limited to NESDIS-specific A&A implementation policy and procedures. While it closely follows NIST SP 800-37 Revision 1, it does not fully replace the NIST defined process of A&A. 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 must comply with this process.

## **3.1 Roles, Responsibilities, and Coordination**

NIST SP 800-37 Section 2.2 describes the roles and responsibilities of key participants involved in an agency's security A&A process. The roles and responsibilities described below for key participants involved in NESDIS A&A efforts are consistent with those described by NIST.

## **3.2 Head of Agency/Chief Executive Officer**

Within NESDIS, the agency head is the NESDIS Assistant Administrator (AA). The AA is the highest-level senior official or executive within NESDIS with the overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the Nation resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Agency heads are also responsible for ensuring that: (i) information security management processes are integrated with strategic and operational planning processes; (ii) senior officials within the organization provide information security for the information and information systems that support the operations and assets under their control; and (iii) the organization has trained personnel sufficient to assist in complying with the information security requirements in related legislation, policies, directives, instructions, standards, and guidelines.

### 3.3 Risk Executive Function

The NESDIS senior executive leadership, in consultation with the NESDIS ITSO, performs the Risk Executive function and is responsible for establishing the NESDIS-wide approach for managing agency-wide risk. Consistent with this oversight role, the risk executive (function) is the group within NESDIS that helps to ensure that: (i) risk-related considerations for individual information systems, to include authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success. The risk executive (function) coordinates with the senior leadership of an organization to:

- Provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization;
- Develop a risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole;
- Facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization;
- Provide oversight for all risk management-related activities across the organization (e.g., security categorizations) to help ensure consistent and effective risk acceptance decisions;
- Ensure that authorization decisions consider all factors necessary for mission and business success;
- Provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation;
- Promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility;
- Ensure that the shared responsibility for supporting organizational mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities; and
- Identify the organizational risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible.

### 3.4 Chief Information Officer (CIO)

The NESDIS CIO has insight into all IT operations of NESDIS is an organizational official responsible for: (i) designating a senior information security officer; (ii) developing and maintaining information security policies, procedures, and control

techniques to address all applicable requirements; (iii) overseeing personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained; (iv) assisting senior organizational officials concerning their security responsibilities; and (v) in coordination with other senior officials, reporting annually to the head of the federal agency on the overall effectiveness of the organization's information security program, including progress of remedial actions. Consistent with this oversight role, the NESDIS CIO also serves in the following roles to provide organizational perspective with respect to the risk of operating information systems within NESDIS.

- AODR for all FIPS 199 High impact NESDIS systems.
- AO (in a co-AO capacity) for all FIPS 199 Moderate impact systems.

### 3.5 Authorizing Official (AO)

Within NESDIS, an AO must be a member of the NESDIS senior management team, such as an Office/Program Director or Deputy Director. The AO must ensure that adequate resources are allocated to A&A activities – from system security categorization to post-authorization.

Although section 4F of the NOAA IT Security Manual designates the Line Office Chief Information Officer (CIO) as the AO for all systems, the following specific designations have been made within NESDIS:

- For all systems designated High-impact in accordance with Federal Information Processing Standard (FIPS) 199, the NESDIS Assistant Administrator (AA) has been appointed as the AO in writing by the NOAA CIO.
- For all FIPS 199 Moderate-impact systems that are not owned by the NESDIS CID, the NESDIS CIO and the Office Director responsible for the information system's budget serve together as co-AOs, with the Office Director being the primary AO. The co-AOs have equal approval authority for the system A&A and other risk acceptance documentation (such as the FIPS 199 analysis, the FIPS 200 determination, and Interconnection Security Agreements), but the primary co-AO is the AO responsible for funding the system. For CID-owned systems, the NESDIS CIO is the sole AO. *[Note: within the text of the Section 7 procedures in this document, the term "AO" includes co-AOs where a Moderate-impact system is involved.]*
- For all FIPS 199 Low impact systems, the Office Director overseeing the operation of the information system is the sole AO.

The AO must appoint a system owner (SO) in writing. A template for SO appointment is available online

at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/SO\\_Appointment\\_Memo\\_te\\_mplate\\_03172011.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/SO_Appointment_Memo_te_mplate_03172011.doc). The AO also must approve the FIPS 199 security categorization and the FIPS 200 security controls requirements baseline of systems for

which they are responsible. The AO may approve the system's security plan (SSP) but may delegate this approval to their Designated Representative.

### **3.6 Information Owner/Steward**

The *information owner/steward* is an organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. In information-sharing environments, the information owner/steward is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with or provided to other organizations. The owner/steward of the information processed, stored, or transmitted by an information system may or may not be the same as the system owner. A single information system may contain information from multiple information owners/stewards. Information owners/stewards provide input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted. The information owner/steward(s) is/are identified in the FIPS199 analysis as well as in the SSP section 5.

### **3.7 Senior Agency Information Security Officer (SAISO)**

The NESDIS Information Technology Security Officer (ITSO) performs all SAISO responsibilities within NESDIS as described in NIST SP 800-37 Revision 1. The NESDIS ITSO shall review NESDIS A&A packages for quality and compliance with applicable laws, directives, policies, and guidance. Consistent with this oversight role, the NESDIS ITSO also serves as AODR for all FIPS 199 Moderate impact NESDIS systems to provide organizational perspective with respect to the risk of operating information systems within NESDIS.

### **3.8 Authorizing Official's Designated Representative (AODR)**

The NESDIS CIO serves as AODR for all NESDIS High impact systems. The NESDIS IT Security Officer (ITSO) serves as the AODR for all NESDIS Moderate impact systems. AODR for Low impact systems may be appointed in writing by the AO if desired. The AODR may approve the SSP, ensuring that the security categorization and control requirements baseline approved by the AO/co-AOs have been properly documented in the SSP. The AODR also serves as a liaison between the AO and other roles involved in A&A activities.

### **3.9 Common Control Provider (CCP)**

The CCP is similar to a SO, but is only responsible for the implementation and maintenance of a subset of NIST SP 800-53 controls which will be inherited as

common controls by other information systems. The CCP is responsible for the documenting the controls in a security plan, appropriately assessing<sup>2</sup> the controls, documenting the control findings in a Security Assessment Report (SAR), and producing a Plan of Action and Milestone (POA&M) for deficiencies identified during assessments. In addition, the CCP is responsible for providing input to the NESDIS Chief Information Division (CID) on all applicable data calls and reporting requirements. NESDIS documentation and supporting evidence requirements for certification and accreditation of common controls are identical to an information system (i.e. SSP, Risk Assessment, etc.). Within the context of a set of common controls, the CCP must perform the same responsibilities as an information system owner. Throughout this policy and procedure, all responsibilities of SO also apply to CCP. Common Control Providers using this policy and procedure should assume responsibilities for all SO responsibilities within the context of the identified common controls set. The NESDIS *Common Control Policy and Procedures* (under development) will provide more information on the responsibilities of the NESDIS CCP. The CCP must obtain NESDIS CIO approval before offering services to systems NESDIS-wide.

### **3.10 Information System Owner (ISO, or SO)**

The SO must be appointed in writing by the AO. This appointment memo must be maintained by the AO with a copy provided to the NESDIS ITSO. The SO is responsible addressing the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements. In coordination with the ISSO, the SO is responsible for the development and maintenance of the SSP and ensures that the system is deployed and operated in accordance with the agreed-upon security controls. In coordination with the information owner/steward, the SO is also responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior). Based on guidance from the AO, the SO informs appropriate organizational officials of the need to conduct the security authorization, ensures that the necessary resources are available for the effort, and provides the required information system access, information, and documentation to the SCA as agreed in the SAP. The SO receives the security assessment results in the form of a SAR from the SCA. After taking appropriate steps to reduce or eliminate vulnerabilities, the SO assembles the authorization package and submits the package to the authorizing official or the authorizing official designated representative for adjudication.

### **3.11 Information System Security Officer (ISSO)**

The ISSO must be appointed in writing by the SO. This documentation must be maintained by the SO and a copy provided to the NESDIS ITSO. The ISSO assists the NESDIS ITSO with execution of the NESDIS IT Security Program requirements at the system level, including facilitating timely completion of system continuous monitoring

activities, coordinating with the NESDIS ITSO regarding the annual security controls assessment, and responding to IT security data calls. The ISSO must be a voting member of the system's Configuration Control Board or key reviewer in the system's configuration change control process to ensure all changes to the information system are properly evaluated for security and risk considerations. The ISSO is an individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the information system owner. The information system security officer also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The information system security officer has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many organizations, is assigned responsibility for the day-to-day security operations of a system. This responsibility may also include, but is not limited to, physical and environmental protection, personnel security, incident handling, and security training and awareness. The information system security officer may be called upon to assist in the development of the security policies and procedures and to ensure compliance with those policies and procedures. In close coordination with the information system owner, the information system security officer often plays an active role in the monitoring of a system and its environment of operation to include developing and updating the security plan, managing and controlling changes to the system, and assessing the security impact of those changes.

### **3.12 Information Security Architect**

Within NESDIS, the NESDIS ITSO and Alternate ITSO serve in this role. The *information security architect* is an individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes. The information security architect serves as the liaison between the enterprise architect and the information system security engineer and also coordinates with information system owners, common control providers, and information system security officers on the allocation of security controls as system-specific, hybrid, or common controls. In addition, information security architects, in close coordination with information system security officers, advise authorizing officials, chief information officers, senior information security officers, and the risk executive (function), on a range of security-related issues including, for example, establishing information system boundaries, assessing the severity of weaknesses and deficiencies in the information system, plans of action and milestones, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities.

### **3.13 Information System Security Engineer**

Within NESDIS, SOs may have one or more personnel serving in this role. The *information system security engineer* is an individual, group, or organization responsible for conducting information system security engineering activities. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration.

Information system security engineers are an integral part of the development team (e.g., integrated project team) designing and developing organizational information systems or upgrading legacy systems. Information system security engineers employ best practices when implementing security controls within an information system including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques. System security engineers coordinate their security-related activities with information security architects, senior information security officers, information system owners, common control providers, and information system security officers.

### **3.14 Security Control Assessor (SCA)**

The NESDIS IT Security Branch performs the independent SCA services for NESDIS systems of all impact categorizations under a fee-for-service arrangement with the. The *security control assessor* (also referred to as “Certifier” or “Certification Agent”) is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., 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). SCAs also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. The SCA performs compliance reviews of the SSP and CP documents prior to AODR approval to help ensure that the plans adequately address implementation of the system’s security requirements baseline. The SCA also performs an assessment of the residual risk from the determined severity of weaknesses or deficiencies discovered in the information system and recommends corrective actions to address identified vulnerabilities in the system. In addition, the SCA prepares the final security assessment report (SAR) containing the results and findings from the assessment. Prior to initiating the security control assessment activities, the SCA must first document a security assessment plan (SAP) that is based on the AODR-approved SSP to document the set of security controls to be assessed each year in accordance with NIST SP 800-53A Revision 1 as well as the methodology to be followed. For control assessments that require independence<sup>3</sup>, the NESDIS ITSO approves the designation of the SCA. For control assessments that do not require independence, the SO may appoint the SCA.

Within NESDIS, the SCA role is filled by a team of personnel including a Lead SCA and the SCA support team staffed by CID contractors. The Lead SCA—also referred to as the *Certifier* or *Certification Agent*—must possess one of the SCA professional certifications required by Commerce Interim Technical Requirement 006, *Information System Security Training for Significant Roles*.

## 4.0 Management Commitment

The NESDIS CID supports the NESDIS AA's strong emphasis on securing NESDIS information and information systems. Through the issuance of this policy and accompanying procedures, NESDIS is committed to the NIST process of accepting risk and authorizing information systems to operate in accordance with federal and departmental laws, policies, and procedures.

## 5.1 Compliance

The NESDIS ITSO monitors—through periodic quality reviews and monthly performance metrics—implementation of the A&A process within NESDIS to ensure compliance with applicable laws, directives, policies, and guidance. The ITSO reports monthly to the AA, and to the CIO and Office Directors as necessary, but at least monthly, 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

- DOC ITSPP section 4.4 (January 2009)
- NOAA *Risk Management Framework Process* (v9, June 14, 2010)

## 6.1 NESDIS A&A Process Policy

As required by DOC ITSPP section 4.4.1, the NESDIS-specific A&A process and procedures shall align with the NIST requirements. NIST SP 800-37 Revision 1 prescribes practices for the six A&A steps: (1) Categorize Information System, (2) Select Security Controls, (3) Implement Security Controls, (4) Assess Security Controls, (5) Authorize Information System, and (6) Continuous Monitoring. NIST SP 800-37 Revision 1 identifies a number of tasks and subtasks required for each phase of a general A&A process. This document provides NESDIS-specific procedures for implementing each step of the A&A process and should be used as companion document for implementation of NIST SP 800-37 Revision 1 within NESDIS and not as a replacement document.

## 6.2 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<sup>4</sup> 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.hq.secteam@noaa.gov](mailto:nesdis.hq.secteam@noaa.gov) regarding any errors found in the document or other clarifications or updates that are required.

### **6.4 Policy Effective Date**

This policy and the procedures contained herein are effective upon issuance.

## 7.1 NESDIS A&A Process Procedures

Throughout the procedures at key points in the A&A process, this document identifies the work products and action milestones that must be completed before moving into the next Step of the A&A process. The procedures describe required activities and milestones and provide references to supplemental policy and procedures as well as documentation templates required by the procedures. Moving to the next Step in the A&A process without successfully creating the products or meeting the milestones may significantly impact the ability to succeed in subsequent Steps and obtain or maintain system authorization to operate.

## 7.2 Step 1 Procedures: Categorize Information System

The System Owner is responsible for completion of the following Security Categorization tasks in the Initiation phase of the system life cycle.

- Task 1-1: Security Categorization

The SO must coordinate with Information Owners/Stewards to prepare/update the FIPS 199 analysis document, route it through the NESDIS ITSO for compliance review, and obtain AO approval. A template for the FIPS 199 analysis document is online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_FIPS\\_199\\_Template\\_v3.0\\_120309.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_FIPS_199_Template_v3.0_120309.doc). The SO should refer to specific requirements for preparing and processing the FIPS 199 in the *NESDIS Federal Information Processing Standard 199 Security Categorization Policy and Procedures*, online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_FIPS\\_199\\_PP\\_v1.0\\_093009.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_FIPS_199_PP_v1.0_093009.pdf).

- Task 1-2: Information System Description

The SO must document SSP sections 1 and 3 through 10 and 12, as well as Appendices A through E and M, to describe the system authorization boundary, environment, regulations, and points of contact for system responsibility. The SO would assign security engineers to develop system diagrams, hardware and software inventories,<sup>5</sup> and would also assign personnel to key roles.

The SO must use the NOAA-mandated template to document the SSP (online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_NOAA\\_nnnn\\_S\\_SP\\_Template.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_NOAA_nnnn_S_SP_Template.doc)). For more information on developing a compliant SSP, refer to the *NESDIS System Security Plan Development and Maintenance Policy and Procedures*, online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_SSP\\_Development\\_Maintenance\\_PP\\_v1.0\\_093009.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_SSP_Development_Maintenance_PP_v1.0_093009.pdf).

The SO would also appoint an ISSO in writing using the template online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/ISSO\\_AppointmentMemo\\_template\\_08152009.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/ISSO_AppointmentMemo_template_08152009.doc).

- Task 1-3: Information System Registration

For new systems, the SO must notify the ITSO and request a NOAA system identifier (system ID). The ITSO provides the SO a NOAA-mandated form to complete and then the ITSO sends the form with a memo to the NOAA Office of the CIO requesting that a NOAA system ID be set up in the Cyber Security Assessment and Management (CSAM) system. This activity should occur as early as possible in the system initiation life cycle phase. Once the system record is established in CSAM, the SO must update the General Information, POCs, Interconnections, and Information Types areas of the CSAM record. For more information on registering a new information system and populating the CSAM record for a new system, refer to the NESDIS Federal Information Security Management Act (FISMA) Inventory Management Policy and Procedures online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/final\\_docs/NESDIS\\_FI\\_SMA\\_InvMgmt\\_PP\\_v1.0\\_08-20-2010.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/final_docs/NESDIS_FI_SMA_InvMgmt_PP_v1.0_08-20-2010.pdf).

Table 7.1 identifies key outputs from Step 1.

<b>Step 1: Work Products and Actions</b>
AO-approved FIPS 199 analysis document uploaded to CSAM
Partial SSP containing system environment description and points of contact
ISSO Appointment Memo (SO signed), uploaded to CSAM
NOAA system ID registered in CSAM for new systems
Completed CSAM fields for system General Information, POCs, Interconnections, and Information Types

**Table 7.1 – Step 1 A&A Checklist**

### 7.3 Step 2 Procedures: Select Security Controls

The following tasks for A&A process Step 2 involve coordination among several roles: the SO, the CIO, the Common Control Providers, Security Architect and Engineers, the AO, and the AODR.

- Task 2-1: Common Control Identification

In the system Initiation phase, SO consults with the CIO and Security Architect regarding recommended common control security solutions available to NESDIS systems. The NOAA Common Controls document is one source for available common control solutions for all NOAA systems. The SO evaluates the available options, consults with the Common Control Provider as well as their Security Engineers to determine the feasibility of adopting the common control solution or an alternative solution. Decisions regarding cost-effectiveness of solutions and risk management should be discussed with the Risk Executive Function. The SO documents Common Control solutions adopted in the FIPS 200 analysis document for AO approval.

- Task 2-2: Security Control Selection

In the Initiation phase, the SO consults with the Security Architect to identify cost-effective control solutions that provide adequate security for the system. Within NESDIS, development of new systems may involve creation of a Level 1 Requirements Document as well as security requirement specifications for developer contracts. The SO must coordinate with the ITSO during system requirements definition to ensure that adequate security considerations are included in the system design. For examples, the SO might include the ITSO in Requirements Working Groups, Design Reviews, and in the routing chain for draft specification documents, or provide security-specific briefings to the ITSO regarding the security concept for the new system. At this time, the SO might also coordinate with the ITSO regarding scheduling of independent SCA services that may be required in Steps 3 and 4 of the A&A process.

The SO might also obtain ITSO approval of the *Information Security in Acquisitions Checklist* and other requirements in accordance with the *NESDIS Policy and Procedures for Ensuring Security in NESDIS IT Systems and Services Acquisitions* ([https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/final\\_docs/NESDIS\\_Security\\_in\\_Acquisition\\_PP\\_v1.0\\_08-20-2010.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/final_docs/NESDIS_Security_in_Acquisition_PP_v1.0_08-20-2010.pdf)).

The analysis of controls selected must consider information types identified in the FIPS 199 that require specific protections, such as privacy considerations and special identification and authentication needs for access to federal systems by remote users. The SO must:

- Complete the Privacy Threshold Analysis (PTA), sign it, send it to the NOAA Privacy Coordinator for approval, and upload the final PTA to the system

CSAM record. The SO also updates the SSP section PL-5 to reflect the results and date of the PTA, and includes the PTA in SSP Appendix G1. The PTA template is online

at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/DOC\\_CA\\_PTA\\_template\\_approved\\_NOAA\\_revisions\\_052010.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/DOC_CA_PTA_template_approved_NOAA_revisions_052010.doc).

- If required by the PTA, the SO then completes the Privacy Impact Assessment (PIA) and submits it to the NOAA Privacy Coordinator for approval. Upon receipt of an email from the NOAA Privacy Coordinator that the PIA is acceptable, the SO uploads the PIA to the system CSAM record. The SO also updates the SSP section PL-5 to reference the PIA, and includes the PIA in SSP Appendix G2. The PIA template is online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NOAA\\_PIA\\_template.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NOAA_PIA_template.doc).
- Complete the E-Authentication Threshold Analysis (ETA), sign it, and upload it to the system CSAM record. The SO also updates SSP section IA-8 control implementation description to reflect the date and results of the ETA. The ETA template is online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/DOC\\_CA\\_030409\\_DOC\\_EAuthentication\\_Threshold\\_Analysis\\_Template\\_Pilot\\_Draft.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/DOC_CA_030409_DOC_EAuthentication_Threshold_Analysis_Template_Pilot_Draft.doc).
- If required by the ETA, the SO then completes the E-Authentication Risk Assessment (ERA) and uploads ERA reports produced by the tool to the system CSAM record. The SO also updates SSP section IA-8 control implementation description to reflect the date and results of the ERA. The ERA tool is available for download at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/eRAv1.52.zip](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/eRAv1.52.zip).

The PTA, PIA, ETA, and ERA contribute to the considerations made by the SO in selection of adequate security control solutions and identifying specific information types or access needs that require special protection because they may be subject to risk of compromises of confidentiality, integrity, and availability. Therefore, risk is another factor to consider in selection of controls. The SO must develop an initial Risk Assessment Report (RAR) that identifies internal, external, and natural threats to the system as well as vulnerabilities in the system that could be exploited by the identified threats to compromise the system security. The development of an initial RAR involves coordination with various system personnel, information owners, the security architect, and AO or AODR. The NESDIS *Annual Risk Assessment Update Interim Technical Guidance* (online

at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/final\\_docs/NESDIS\\_Risk](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/final_docs/NESDIS_Risk)

[Assessment Update ITG v1.0 08-20-2010.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/final_docs/NESDIS_Risk_Assessment_Update_ITG_v1.0_08-20-2010.pdf)) provides some tips for the content of a RAR, but the SO must adhere to the recommendations of NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, (online at <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>), in developing an

initial RAR. A suggested template for use in developing the RAR is online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/final\\_docs/NOAA50xx\\_RAR\\_vx.x\\_mm-dd-yyyy\\_Template\\_v5.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/final_docs/NOAA50xx_RAR_vx.x_mm-dd-yyyy_Template_v5.doc)). Upon completion of the RAR, the SO uploads the RAR to the system CSAM record; updates the SSP section 16 control RA-3 to reference the RAR date, version, and title; and adds the RAR to SSP Appendix L. The SO also creates POA&Ms<sup>6</sup> in CSAM to track implementation of planned controls identified in the risk assessment as missing or inadequate.

- Task 2-3: Monitoring Strategy

In the Initiation phase, the SO, or Common Control Provider, must develop a plan for continuous monitoring of selected controls after system deployment, and document the strategy in Appendix H of the SSP as well as reference the date, version, and title of the Plan in SSP section 16 under control CA-7. The Continuous Monitoring Plan should assign responsibility to a specific role/position within the system and account for DOC, NOAA, and NESDIS policy requirements as well as any system-specific requirements for periodic controls monitoring, including but not limited to:

1. Quarterly vulnerability scanning (RA-5), including required scanning for unauthorized wireless access points for AC-18(2) as required by DOC ITSPP.
2. Semi-annual account reviews (AC-2).
3. Monthly Plan of Actions and Milestones (POA&M) updates (CA-5).
4. System maintenance (MA-2), including routine patching schedules (SI-2)
5. Annual SSP update (PL-2) including: review/update of the supporting documentation such as the PTA and PIA, if required (PL-5); continuous monitoring plan (CA-7); ETA and ERA, if required (IA-8); FIPS 199 analysis; FIPS 200 analysis; and system component inventory (CM-8).
6. Annual contingency plan (CP), business impact analysis (BIA), and CP test plan and results (CPTPR) updates; CP training, CP testing, and backup and recovery test (CP-2, CP-3, CP-4, and CP-9/CP-10).
7. Annual physical access record reviews (PE-2) and monthly visitor access record reviews (PE-8).
8. Semi-annual update of FISMA Inventory information in CSAM (PL-1).
9. Annual reviews of access agreements (PS-6 -- see DOC ITSPP, which requires agreements for people such as supervisors with access to PII – may not apply to all systems, depending on what the SSP requires for implementation of PS-6).
10. Annual risk assessment updates (RA-3), which would at a minimum coincide with scheduling of the annual independent security controls assessment for CA- 2.
11. Semi-annual SI-7 integrity scans required by DOC ITSPP.
12. Annual role-based training of personnel with significant ITSec roles (AT-3), and professional certification (and certification renewal) of the ISSO as required by

DOC CITR-006.

13. Annual incident response training (IR-2, IR-3).

- Task 2-4: Security Plan Approval

Moving into the Development/Acquisition phase, the objective of the SSP review and AODR approval is to validate and authorize the adequacy of the cost-effective controls selected to protect the system. Upon completion of the control selection analysis, the SO documents selected controls, prepares the FIPS 200 analysis to document the security controls baseline, and obtains AO approval of the baseline. A template for the FIPS 200 analysis document is online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_FIPS\\_200\\_Template\\_v2.0\\_12009.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_FIPS_200_Template_v2.0_12009.doc). The SO should refer to specific requirements for preparing and processing the FIPS 200 in the *NESDIS Federal Information Processing Standard 200 Control Selection and Tailoring Policy and Procedures*, online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_FIPS\\_200\\_v1.0](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_FIPS_200_v1.0)

[093009.pdf](#). Upon receiving AO approval, the SO uploads the FIPS 200 analysis document to the system CSAM record and adds the document to the SSP Appendix N.

If the SO created POA&Ms as a result of the risk assessment, the SO must obtain written AO approval of the POA&Ms in accordance with NESDIS policy. Upon approval of the POA&Ms by the AO, the SO submits the AO's approval notification to the ITSO and requests that the POA&M status be approved in the CSAM system.

Upon approval of the requirements baseline from the AO, the SO must complete the control implementation descriptions in section 16 of the SSP and submit the SSP to the ITSO for compliance review.<sup>7</sup> The ITSO, within 5 business days, completes the NOAA-mandated *SSP Compliance Review Checklist* ([https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/final\\_docs/NOAA50xx\\_CID\\_SSP\\_Compliance\\_Review\\_Checklist\\_Template\\_SP800-53Rev3\\_v2.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/final_docs/NOAA50xx_CID_SSP_Compliance_Review_Checklist_Template_SP800-53Rev3_v2.doc)) and provides the completed Checklist to the SO or ISSO for uploading to CSAM and for action if unacceptable deficiencies are identified. The SO or ISSO, within 5 business days, revises the SSP and resubmits to the ITSO for a second review. This cycle repeats until the Checklist documents no unacceptable deficiencies, at which time the SSP is routed to the AODR for approval.

Table 7.2 identifies key outputs from Step 2.

<b>Step 2: Work Products and Actions</b>
E-Authentication Threshold Analysis (ETA) uploaded to CSAM
E-Authentication Risk Assessment (ERA), if required by the ETA, uploaded to CSAM
SSP Appendix G1: Privacy Threshold Analysis (PTA) uploaded to CSAM
SSP Appendix G2: Privacy Impact Analysis (PIA), if required by the PTA, uploaded to CSAM
SSP Appendix H: Continuous Monitoring Plan/Strategy uploaded to CSAM
SSP Appendix L: Risk Assessment Report (RAR) uploaded to CSAM
SSP Appendix N: AO-approved FIPS 200 analysis document uploaded to the system’s CSAM record
Updated SSP section 16 for control “Assignments” for system-specific control implementation requirements as well as the control implementation descriptions for controls in the system requirements baseline and to reference POA&Ms created for planned controls
Draft POA&Ms created in CSAM for planned controls identified in the SSP
NOAA-mandated SSP Compliance Review Checklist completed by ITS0 uploaded to CSAM
AODR-approved SSP uploaded to CSAM

**Table 7.2 – Step 2 A&A Checklist**

## 7.4 Step 3 Procedures: Implement Security Controls

In the system Development/Acquisition and Implementation life cycle phases, the SO considers the analysis for control selection and SSP documentation of control implementation requirements in Step 2 and implements the controls as approved for the system.

- Task 3-1: Security Control Implementation

The SO must implement the controls approved by the AO in the FIPS 200 security requirements baseline and as described in the AODR-approved SSP. Security architecture, security engineering, and secure coding practices are employed in configuring system components for use within the system. The security engineers and ISSO coordinate with Common Control Providers to integrate the common control solutions into the system functionality. If some controls are not able to be fully implemented, compensating controls to assure adequate and mitigating controls may be necessary to mitigate residual risk to the system until the control can be fully implemented in accordance with the documented POA&Ms. The SO enlists the assistance of security controls assessors—as scheduled in Task 2-2—to test the effectiveness of initial control deployment to identify and correct weaknesses in control implementation prior to placing the system in operation. If these development-phase assessments are performed by independent assessors, the results can be re-used in the Step 5 as the basis for authorization of the system.

- Task 3-2: Security Control Documentation

As a result of the initial control deployment and testing, the SO may need to refine or modify the control implementation descriptions in the SSP. The SO updates the SSP as needed to ensure the accuracy and completeness of the control implementation descriptions. All changes are tracked in the SSP Record of Changes.

The SO documents the following during Step 3:

1. System baseline IT architecture standards (CM-2).
2. System configuration settings (CM-6) adopted for securing system components, including documentation of exceptions to NIST-approved configuration checklists.<sup>8</sup>
3. Authorized and unauthorized ports, protocols, and services (CM-7).
4. Finalized system Configuration Management Plan (CM-9).
5. Finalized system-specific Incident Response Plan (IR-8).
6. Contingency Plan (CP) and Business Impact Analysis (BIA) approved by the AODR (CP-2), and CP Test Plan and Results (CPTPR) document (CP-4).<sup>9</sup>

Templates for these documents are available on the NESDIS IT Security Handbook website

at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/final\\_docs/NESDIS\\_CP\\_P-P\\_v1.0\\_08-20-2010.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/final_docs/NESDIS_CP_P-P_v1.0_08-20-2010.pdf). The SO must submit the CP documentation to the ITSO for NOAA-mandated compliance review. The ITSO, within 5 business days, completes the NOAA-mandated *Compliance Review Checklist*

for each document (also available on the NESDIS IT Security Handbook website) and provides the completed Checklist to the SO or ISSO for uploading to CSAM and for action if unacceptable deficiencies are identified. The SO or ISSO, within 5 business days, revises the document and resubmits to the ITSO for a second review. This cycle repeats until the Checklist documents no unacceptable deficiencies. When determined compliant, the SO signs the CP, routes it to the AODR for approval, and then uploads all CP documents to CSAM.

7. Security Education, Training, and Awareness (SETA) Plan (AT-3/AT-4) (optional, but recommended). Guidance for developing a SETA Plan is provided in section 7.2 of the *NESDIS IT Security Training Policy and Procedures* (online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_Training\\_P\\_P\\_v1.0\\_093009.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_Training_P_P_v1.0_093009.pdf)).

The inputs to A&A Step 4 are the products from Steps 1, 2, and 3. **Therefore, the SO must ensure completion of A&A activities through Step 3 no later than 60 calendar days<sup>10</sup> prior to the target system authorization date. Any delay will result in a minimum day-for-day slip of the target authorization date.<sup>11</sup>**

Table 7.3 identifies key outputs from Step 3.

<b>Step 3: Work Products and Actions</b>
Updated SSP uploaded to CSAM
SSP Appendix J: AODR-approved Contingency Plan uploaded to CSAM
SSP Appendix K: ITSO reviewed CTPR uploaded to CSAM
Finalized Configuration Management Plan uploaded to CSAM
Finalized Incident Response Plan uploaded to CSAM
Security Education, Training, and Awareness Plan (if applicable)
Completed NOAA-mandated CP Compliance Review Checklist uploaded to CSAM
Completed NOAA-mandated BIA Compliance Review Checklist uploaded to CSAM
Completed NOAA-mandated CTPR Compliance Review Checklist uploaded to CSAM

**Table 7.3 – Step 3 Checklist**

## 7.5 Step 4 Procedures: Assess Security Controls

The tasks in A&A process Step 4 occur in the Development/Acquisition and Implementation life cycle phases. The objectives of Step 4 are to evaluate the effectiveness of security controls, create the Security Assessment Report (SAR), and determine appropriate and feasible actions for remediating deficiencies found. The SCA is primarily responsible for the completion of 3 of the 4 tasks in A&A process Step 4.

The SO is required to participate in the assessment of the system and is responsible for contributing to the task for determining remedial actions that will be tracked in POA&Ms.

- Task 4-1: Assessment Preparation

The SCA documents an A&A Project Plan (obtain template online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/it\\_security\\_handbook.php](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php)

[p](#)) and a Security Assessment Plan (SAP), which describes the Scope and Methodology to be followed by the SCA for evaluating the effectiveness of controls implemented within the system. The SAP describes a variety of techniques including interviews of personnel, examination of documents, and testing controls through compliance scans, direct observation, vulnerability assessment scanning, and penetration testing.<sup>12</sup> It also lists the SCA team personnel, key system points of contact, the controls selected for assessment, the assessment procedures, the component sampling plan to be used by the assessment team for determining component compliance with system configuration policy, and the assessment schedule. For an initial assessment of a system in the Implementation life cycle phase, for purposes of initial authorization to operate, the SCA plans to assess all required controls implemented in the system authorization boundary, but not less than 71% of the required controls. Controls are selected based on risk and volatility, with consideration for controls mandated by DOC, NOAA, and NESDIS for assessment annually.

The SCA coordinates with the SO and third-party SCAs in the development of the SAP as well as supplemental Rules of Engagement (ROE) for vulnerability assessment scanning and penetration testing.<sup>13</sup> The SAP must be based on the AO/AODR-approved SSP from [Task 2-4](#), as updated in [Task 3-2](#), to ensure that the required controls baseline is assessed against the intended implementation of controls as approved by the AO and AODR. The assessment must follow the guidance in NIST SP 800-53A Revision 1, *Guide for Assessing Security Controls in Federal Information Systems and Organizations*, section 3.2. The SCA approves the SAP in writing and obtains signed concurrence from the SO to ensure that the SO approves the scope, methodology, and schedule, and agrees to make specified documents and personnel available to the assessment team. The SCA, SO, ISSO, and third-party SCA support team approve the ROE.

- Task 4-2: Security Control Assessment

The SCA executes the SAP that was approved by the SCA and SO in Task 4-1. If independent testing was performed by an SCA during the Risk Assessment in [Task 2-2](#) or during control implementation ([Task 3-1](#)), the SCA may re-use the results in determining the status of the security controls. Vulnerability scanning must cover at least 95% of the components in the system's official inventory.<sup>14</sup> For detailed procedures in conducting security control assessments within NESDIS, refer to the *NESDIS Policy and Procedures for Conducting Security Controls Assessments*

online

at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_Control\\_Assessment\\_PP\\_v1.0\\_08312009.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_Control_Assessment_PP_v1.0_08312009.pdf).

- Task 4-3: Security Assessment Report

The SCA must document the results of the assessment and analysis of the data gathered from Task 4-2 in a variety of reports that summarize the analysis and conclusions, including:

1. The NOAA-mandated Security Controls Assessment spreadsheet template to document the NIST SP 800-53A Revision 1 assessment results (online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/it\\_security\\_handbook.php](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php));
2. A Vulnerability Assessment Report (VAR) to document the scan-to-inventory analysis, the determination regarding use of authentication in scanning, and the analysis of scan results; and
3. A Penetration Testing Report (if applicable) to document the results of penetration testing.

The SCA must vet these reports with the ISSO and SO to validate the findings and ensure accuracy prior to preparation of the SAR. The SCA must upload to CSAM the reports as well as supporting artifacts used as evidence of conclusions documented in the reports. The SCA will also summarize the findings of these detailed reports and develop a Security Assessment Report (SAR) that adheres to the guidance in NIST SP 800-53A Revision 1 Appendix G. The SAR summarizes the scope and methodology from the SAP developed in Task 4-1 as well as the results of the controls assessment documented in the aforementioned reports. For more information on developing the SAR, refer to the *NESDIS Security Assessment Report Policy and Procedures* online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/final\\_docs/NESDIS\\_Security\\_Assessment\\_Report\\_P-P\\_v1.0\\_08-20-2010.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/final_docs/NESDIS_Security_Assessment_Report_P-P_v1.0_08-20-2010.pdf).

The SCA develops and delivers the SAR to the SO for review and comment.

- Task 4-4: Remedial Actions

As time allows, the SO is afforded an opportunity to correct any deficiencies identified and request re-assessment by the SCA before presentation of results to the AO. The SCA then must re-

assess control effectiveness and update the detailed results reports as necessary. The SCA then updates the RAR to determine the residual risk to the system from confirmed weaknesses identified and uploads the RAR to the system’s CSAM record. The SCA incorporates a summary of the RAR update in the SAR and also updates the SAR to reflect their independent recommendation regarding authorization of the system to operate. The SCA finalizes the SAR and uploads it to CSAM.

Table 7.4 identifies the outputs from Step 4.

<b>Task 7.4: Work Products and Actions</b>
Security Assessment Plan (SAP) uploaded to CSAM
Vulnerability Assessment Rules of Engagement (ROE) uploaded to CSAM
Penetration Testing ROE (if applicable) uploaded to CSAM
SCA Report (completed NOAA spreadsheet template) uploaded to CSAM
Vulnerability Assessment Report uploaded to CSAM
Penetration Testing Report (if applicable) uploaded to CSAM
Assessment artifacts uploaded to CSAM
Update RAR uploaded to CSAM
Security Assessment Report (SAR)

**Table 7.4 – Assess Security Controls Checklist**

## 7.6 Step 5 Procedures: Authorize Information System

The purpose of A&A Step 5 in the system Implementation life cycle phase is to obtain an AO decision regarding initial authorization of system operation. This initial authorization to operate marks the transition from the Implementation phase of the life cycle to the Operations and Maintenance phase. The SO, assisted by the Lead SCA/Certifier, presents the final risk determination to the AO.

- Task 5-1: Plans of Action and Milestones (POA&Ms)

For controls found not fully implemented, the SO must work with the SCA to create draft POA&Ms, or document justification for partially or not implementing controls so that the Lead SCA/Certifier and SO can ask the AO for risk acceptance at the authorization meeting. For more information on developing POA&Ms, refer to the *NESDIS Plan of Action and Milestones (POA&M) Management Policy and Procedures* online

at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/POAM\\_Management\\_PP\\_v1.1\\_091409.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/POAM_Management_PP_v1.1_091409.pdf). At the completion of this Task, the draft POA&Ms will be populated, including planned start and finish dates. If the SO determines that compensating controls will be developed for implementation, or that it is not feasible or cost-effective to remediate a specific weakness, the SO revises the FIPS 200 analysis to document the rationale for implementing compensating controls or for requesting full or partial control tailoring. The SO should refer to specific requirements for preparing and processing the FIPS 200 in the *NESDIS Federal Information Processing Standard 200 Control Selection and Tailoring Policy and Procedures*, online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_FIPS\\_200\\_v1\\_0\\_093009.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_FIPS_200_v1_0_093009.pdf).

- Task 5-2: Security Authorization Package

The SCA assists the SO in assembly of the final A&A security authorization package and development of the briefing for the AO. The security authorization includes the SSP including the draft FIPS 200 analysis update (if applicable), the SAR, and the draft POA&Ms. NOAA defines the A&A package “core documents” in the *NOAA Risk Management Framework Process* (v9, June 14, 2010). Following are the activities involved in developing the final security authorization package in NESDIS:

1. The Lead SCA develops briefing slides that summarize:
  - a. key information about the system from the SSP (such as the system mission/purpose, security categorization and information types that are drivers for the high water-mark categorization), facility locations, and number of components in the official inventory;
  - b. Scope and methodology from the SAP as well as scope

- limitations/restrictions encountered during the assessment as described in the SAR;
- c. Assessment results as detailed in the SAR;
  - d. Draft POA&Ms for AO approval, including completion dates and associated risk;
  - e. Requests for additional requirements baseline tailoring (if applicable);
  - f. Discussion of residual risk;
  - g. Completed *Assessment and Authorization Checklist for NESDIS Authorizing Officials* (online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/CA\\_Checklist\\_for\\_NESDIS\\_AOs\\_v2\\_102009.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/CA_Checklist_for_NESDIS_AOs_v2_102009.pdf)); and
  - h. Certifier's recommendation for system authorization.
2. The Lead SCA pre-briefs the SO and AODR to ensure that the briefing includes sufficient information for the AO to understand the residual risk of operating the system and the risk accepted if the system is authorized to operate.
  3. The Lead SCA, SO, and AODR coordinate to finalize the briefing for the AO. For high-impact systems, the Lead SCA, SO, and AODR also coordinate in pre-briefing the NESDIS Deputy Assistant Administrator (DAA) prior to briefing the AO (who is the NESDIS Assistant Administrator). After this pre-brief, the Lead SCA, SO, and AODR finalize the AO briefing based on input from the DAA.
- Task 5-3: Risk Determination

The Lead SCA, SO, and AODR brief the AO on the residual risks of operating the system in its current environment, and discuss the recommendation for acceptance of risk. The AO asks questions regarding POA&Ms and assessment findings to fully understand the weaknesses and determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
  - Task 5-4: Risk Acceptance

Once the SCA has briefed the AO on the risks associated with operating the information system, the AO considers the *Assessment and Authorization Checklist for NESDIS Authorizing Officials* in confirming that all NESDIS A&A requirements were met to fully determine the status of security controls and disclose the magnitude of residual risks to the system. The AO then makes an

authorization decision taking into consideration the risk to agency assets, personnel, and reputation.<sup>15</sup> The decision is formally documented in the authorization decision memo drafted by the SCA. Any AO-directed actions or conditions are also documented in the authorization memo, including the authorization termination date. The AO also approves POA&Ms and requests for permanent risk acceptance presented by the SO in a revised FIPS 200 analysis.

After the authorization decision is rendered, the SO has 5 business days to finalize POA&Ms and complete the updates to the SSP to reflect any AO authorization conditions, approvals of POA&Ms, and additional controls baseline tailoring. If conditional terms are stipulated in the authorization decision, the SO must create POA&Ms in CSAM to document the plan for satisfying the conditions as well as finalize POA&Ms presented to and approved by the AO in the authorization briefing. Once the SSP update is completed and POA&Ms are finalized in CSAM, the SO assists the Lead SCA in assembling the final A&A package and updating CSAM to reflect the authorization artifacts (e.g., decision memo and briefings) and new authorization termination date as well as dates of all updated documents and uploading core documentation.

Table 7.5 identifies the outputs from Step 5.

<b>Task 7.5: Work Products and Actions</b>
Security Authorization Package
Security Authorization Decision memo signed by the AO
AO-approved POA&Ms finalized in CSAM
Updated SSP to reflect AO mandates and authorization decision uploaded to CSAM
Final A&A artifacts uploaded to CSAM and CSAM dates updated within 5 business days of authorization

**Table 7.5 – Authorize Information System Checklist**

### **7.7 Step 6 Procedures: Monitor Security Controls**

Once authorized to operate, the system moves into the Operation and Maintenance life cycle phase. SOs (and Common Control Providers) are responsible for maintaining the approved configuration of their information system by executing a robust configuration management plan to control and document changes to the information system and a continuous monitoring process to monitor continued control effectiveness. In this Step, the SO executes the Continuous Monitoring Plan developed in A&A [Task 2-3](#).

- Task 6-1: Information System Environment Changes

NIST SP 800-53 documents the requirements for a configuration management program in the “Configuration Management” family of controls. The SO, or ISSO, implements and maintains the Configuration Management Plan. For each change to the system environment, the SO, assisted by the ISSO, must perform a security impact analysis to determine the additional risk to the information system of implementing the change and

if the risk presented by the change requires AO approval. A form for documenting the security impact analysis is available online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/Security\\_Impact\\_Analysis\\_Form\\_Draft\\_v1.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/Security_Impact_Analysis_Form_Draft_v1.doc). The SO and ISSO may discuss changes that increase the risk of operating the information system with the NESDIS ITSO/Security Architect, AODR, or AO for recommendations regarding impact.<sup>16</sup> Changes determined to have a significant adverse affect on risk to the system environment or architecture (with or without increased risk to the organization) may require AO approval prior to implementation.<sup>17</sup> The SO must report any change that may be considered significant to AO and to the NESDIS CIO via the AA Monthly IT Forecast slide (template online at [https://intranet.nesdis.noaa.gov/ocio/documents/IT\\_System\\_Forecast\\_Slide\\_v3.ppt](https://intranet.nesdis.noaa.gov/ocio/documents/IT_System_Forecast_Slide_v3.ppt)). The NESDIS ITSO will periodically inspect change requests and the associated security impact analysis to ensure that changes are appropriately authorized and reported to the NESDIS CIO and system AO when required.

Table 7.6.1 identifies the outputs from Task 6-1.

<b>Task 7.6.1: Work Products and Actions</b>
Configuration Change Control Request documentation
Security Impact Analysis for system changes
Configuration Change Control Board meeting minutes
Updated system hardware and software inventories

**Table 7.6.1– Information System Changes Task Checklist**

- Task 6-2: Ongoing Security Control Assessments

Ongoing security assessments ensure that the controls continue to be implemented as documented in the AO/AODR-approved SSP, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Assessments may be performed by SO staffs for daily monitoring of controls, under a fee-for-service arrangement with the NESDIS CID for the annual independent controls assessment requirement, or as announced by other external parties such as the Office of Inspector General. Independent assessments are required on an annual basis for purposes of maintaining the system’s authorization to operate.

The SO must ensure that periodic monitoring assessments are performed and documented in accordance with the activities and schedules in the system’s Continuous Monitoring Plan, such as periodic user account reviews and integrity scans. The SO or ISSO maintains records of completed internal reviews and assessments as evidence that continuous monitoring activities were performed.

Review checklists that are signed and dated by the reviewer facilitate documentation of required reviews. The SO or ISSO updates the RAR if necessary during the year to reflect new weaknesses identified through the conduct of internal reviews and assessments. The SO creates POA&Ms to address new weaknesses, and coordinates with the AODR to obtain new POA&M approval.

In addition, the SO must perform quarterly vulnerability assessment scanning of all components in the system environment that have one or more IP addresses. To achieve adequate depth and breadth of scanning, the scanning must be performed using authentication and cover at least 95% of components in the system component inventory. If the AC-18(2) control is applicable to the system, the SO must also conduct and document the quarterly scanning for wireless access points. The SO submits the quarterly scanning results to the NESDIS ITSO on or before the 15<sup>th</sup> of the 3<sup>rd</sup> month of each quarter.

The SO must coordinate with the NESDIS ITSO regarding scheduling of the required independent annual security controls assessment. In consultation with the SO in preparation of the A&A Project Plan and SAP (see [Task 4-1](#)), the SCA selects a subset of the required system controls (approximately 1/3<sup>rd</sup> each year after initial authorization to operate such that all required controls are independently assessed at least once over a 3-year period). The SCA must include in the selection of controls for the annual assessment all POA&Ms closed since the last annual assessment. The SCA conducts the assessment as described in [Task 4-2](#) and the SCA documents the assessment results as described in [Task 4-3](#).

The assessment must be completed annually by the anniversary of the system’s authorization date. Upon completion of the assessment, the SO must update CSAM to reflect the date that the annual controls assessment was completed. For detailed procedures in conducting security control assessments within NESDIS, refer to the *NESDIS Policy and Procedures for Conducting Security Controls Assessments* online at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/NESDIS\\_Control\\_Assessment\\_PP\\_v1\\_0\\_08312009.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/NESDIS_Control_Assessment_PP_v1_0_08312009.pdf).

The Lead SCA/Certifier coordinates with the SO to prepare POA&Ms to address new weaknesses found as described in [Task 5-1](#).

Table 7.6.2 identifies the outputs from Task 6-2.

<b>Task 7.6.2: Work Products and Actions</b>
A&A Project Plan
Security Assessment Plan (SAP) uploaded to CSAM
Vulnerability Assessment Rules of Engagement (ROE) uploaded to CSAM
Penetration Testing ROE (if applicable) uploaded to CSAM
SCA Report (completed NOAA spreadsheet template) uploaded to CSAM
Vulnerability Assessment Report uploaded to CSAM
Penetration Testing Report (if applicable) uploaded to CSAM
Assessment artifacts uploaded to CSAM
Updated RAR uploaded to CSAM

Updated Security Assessment Report (SAR) uploaded to CSAM
Final assessment artifacts uploaded to CSAM and CSAM dates updated within 5 business days of assessment completion

**Table 7.6.2– Ongoing Security Control Assessments Task Checklist**

- Task 6-3: Ongoing Remedial Actions

The SO is responsible for completing remedial actions in accordance with AO-approved POA&Ms. All POA&Ms are managed in the CSAM system and the SO must complete monthly reviews and update POA&Ms as necessary to ensure that they are kept accurate and kept up-to-date. Progress of POA&M completion is scrutinized by the AO to monitor the reduction of risk that comes with implementing corrective actions—and the extension of accepted risk that comes with implementation delays. The SO is required to manage POA&Ms proactively, consulting with the ITSO and/or AODR regarding challenges with timely POA&M completion, and to enlist AO assistance with resolving difficult resource and mission issues in advance of POA&M delay. Through the CSAM system, NESDIS CID, NOAA OCIO, and DOC OCIO have instant visibility into the status of all POA&Ms. More detail on managing the POA&Ms can be found in the NESDIS *Plan of Action and Milestones Management Policy and Procedures*.

Table 7.6.3 identifies the outputs from Task 6-3.

<b>Task 7.6.3: Work Products and Actions</b>
Updated PO&AMs in CSAM
Completed Change Control Requests
POA&M closure artifacts uploaded to CSAM including revised system documents that were updated or developed as indicated by POA&M milestones

**Table 7.6.3– Ongoing Remedial Actions Task Checklist**

- Task 6-4: Key Updates

The SO must ensure that changes within the system environment are documented, authorized, and reflected in the SSP. The SO must update the SSP and supporting documentation at least annually, update the Record of Changes (even if no substantive changes were made to the content of the document), and test the contingency plan at least annually. The Continuous Monitoring Plan developed for [Task 2-3](#) should be used to guide and schedule the update activities.

The SSP is the aggregation of the system’s FIPS 199 security categorization, FIPS 200 security requirements baseline and implementation requirements, and supporting documentation and procedures for control implementation. The SSP is a living document that is required to reflect the current state of the security controls and the system description. Any changes (actual or planned) to the information system must be documented in the SSP. More detail on maintaining the SSP can be found in the NESDIS *System Security Plan Development and Maintenance Policy and Procedures*.

The SO must update CSAM to reflect the date of the annual documentation updates, and upload updated documentation to CSAM as a historical record. The SO must also submit annual updates of the SSP, CP, BIA, CPTPR to the ITSO, who must follow the NOAA-mandated ITSO compliance review process as described in Tasks [2-4](#) and [3-2](#).

**Important Note:** The inputs to the independent annual security controls assessment activities of Task 6-2 are the products from Task 6-4. **Therefore, the SO must ensure completion of Task 6-4 activities no later than 60 calendar days<sup>18</sup> prior to the target system re-authorization or annual anniversary date. Any delay will result in a minimum day-for-day slip of the target authorization date or the annual assessment completion date.<sup>19</sup>**

<b>Task 7.6.4: Work Products and Actions</b>
SSP Appendix A: AO-approved FIPS 199 analysis document uploaded to CSAM (updated in years of authorization termination or significant system change)
E-Authentication Threshold Analysis (ETA) uploaded to CSAM (updated in years of authorization termination or significant system change)
E-Authentication Risk Assessment (ERA), if required by the ETA, uploaded to CSAM (updated in years of authorization termination or significant system change)
SSP Appendix G1: Privacy Threshold Analysis (PTA) uploaded to CSAM (updated in years of authorization termination or significant system change)
SSP Appendix G2: Privacy Impact Analysis (PIA), if required by the PTA, uploaded to CSAM (updated in years of authorization termination or significant system change)
Updated SSP Appendix H: Continuous Monitoring Plan uploaded to CSAM
SSP Appendix I: Updated and new interconnection security agreements and service level agreements uploaded to CSAM
Updated SSP Appendix J: AODR-approved Contingency Plan update uploaded to CSAM
Completed NOAA-mandated CP Compliance Review Checklist uploaded to CSAM
Updated SSP Appendix K: ITSO reviewed CPTPR uploaded to CSAM
Completed NOAA-mandated CPTPR Compliance Review Checklist uploaded to CSAM
Updated SSP Appendix L: Risk Assessment Report (RAR) uploaded to CSAM
SSP Appendix N: AO-approved FIPS 200 analysis document uploaded to the system's CSAM record (updated in years of authorization termination or significant system change)
Updated BIA uploaded to CSAM
Completed NOAA-mandated BIA Compliance Review Checklist uploaded to CSAM

Updated Configuration Management Plan uploaded to CSAM
Updated Incident Response Plan uploaded to CSAM
Security Education, Training, and Awareness Plan (if applicable)
NOAA-mandated SSP Compliance Review Checklist completed by ITSO uploaded to CSAM
AODR-approved SSP update uploaded to CSAM

**Table 7.6.4– Key Updates Task Checklist**

- Task 6-5: Security Status Reporting

The status of the information system security posture must be reported to the AO on a regular basis. At a minimum, the NESDIS CIO reports on information security performance metrics, and Office Directors report on their status on IT security compliance, at the NESDIS AA Monthly Staff Meeting. This meeting is attended by the NESDIS AA (who serves as the AO for all high-impact systems) and the Office Directors (who serve as SOs for high-impact systems and AOs for moderate- impact systems). The SO is responsible for ensuring the accuracy of data in the CSAM system that is used to develop the Monthly metrics, as well as for monitoring actual versus planned A&A project plan activity completion; and for ad hoc reporting to the OCIO on other IT security requirements such as training status. SOs must present their information system’s status at the monthly NESDIS

Assistant Administrator meeting. SOs must use the NESDIS published template for reporting at the NESDIS AA monthly meeting<sup>20</sup>.

Table 7.6.5 identifies the outputs from Task 6-5.

<b>Task 7.6.5: Work Products and Actions</b>
Monthly AA Briefing Slides
Various FISMA Reporting documents
Ad Hoc Data Call Reports (as needed by NESDIS/NOAA/DOC/OMB)

**Table 7.6.5– Security Status Reporting Checklist**

- Task 6-6: Ongoing Risk Determination and Acceptance

*In years that the system authorization terminates*, the Lead SCA works with the SO to prepare the security authorization package for transmittal from the SO to the AO exactly as described in [Task 5-2](#), and coordinates with the SO, and AODR to brief the AO as described in [Task 5-3](#). The AO renders a new authorization decision and the activities are performed exactly as described in [Task 5-4](#).

*In years that the system authorization does not terminate*, the Lead SCA works with the SO to prepare a security authorization package to submit to the AO for review and acknowledgement. The package contains:

1. Cover transmittal memo signed by the SO;
2. SSP or key information pertinent to the determination of risk by the AO;
3. SAR, or SAR Executive Summary explaining the residual risk of continued operation of the system and the independent SCA’s recommendation for continued operation;
4. Completed *Assessment and Authorization Checklist for NESDIS Authorizing Officials*;
5. Draft POA&Ms for AO approval; and
6. Revised FIPS 200 analysis for AO approval (*if* the SO requests additional control requirements tailoring).

The assembled security authorization package is submitted to the AO by the Lead SCA, SO, or AODR along with a drafted annual security authorization acknowledgement memo for signature by the AO. The memo signed by the AO should indicate that the AO has reviewed the security authorization package, approved the POA&Ms, and either re-affirms or changes the terms of the system’s authorization to operate. The SO provides a copy of the signed memo to the NESDIS ITSO and uploads the memo to the system’s CSAM record. Upon written approval of the POA&Ms by the AO, the SO or ISSO coordinates with the ITSO to finalize the POA&Ms in CSAM within 5 business days of the date of the AO memo.

Table 7.6.6 identifies the outputs from Task 6-6.

<b>Task 7.6.6: Work Products and Actions</b>
Security Authorization Package
Security Authorization Decision memo signed by the AO (in years of authorization termination) or Security Authorization Acknowledgement memo signed by the AO (in years that the system authorization is not scheduled for termination); upload the memo to CSAM
AO-approved POA&Ms finalized in CSAM
Updated SSP to reflect AO mandates and authorization decision uploaded to CSAM
Final A&A artifacts uploaded to CSAM and CSAM dates updated within 5 business days of authorization

**Table 7.6.6– Ongoing Risk Determination and Acceptance Task Checklist**

- Task 6-7: Information System Removal and Decommissioning

Approaching the system Disposal life cycle phase, the SO coordinates with the ITSO, AODR, and AO to plan a controlled decommissioning of the system that preserves data archives and federal

records, and ensures that system components are rendered clear of any sensitive government information. The SO must develop and implement an information system decommissioning strategy and formally document a Decommissioning Plan that describes required actions when a system is removed from service. The SO would sign the Decommissioning Plan and route to the AO for final approval. A copy of the approved Plan is submitted to the ITSO with a request to retire the system in the CSAM database. Upon receipt of the approved Decommissioning Plan, the ITSO notified the NOAA OCIO in writing and requests removal of the system from the NESDIS FISMA systems inventory.

Table 7.6.7 identifies the outputs from Task 6-7.

<b>Task 7.6.7: Work Products and Actions</b>
AO-approved system Decommissioning Plan
ITSO-signed memo requesting that NOAA remove the system from the NESDIS FISMA systems inventory
Equipment sanitization and disposal records

**Table 7.6.7– Information System Removal and Decommissioning Task Checklist**

## Approval Page

Document Number: NQP-3401, Revision 2.2	
Document Title Block: <b>Risk Management Framework Assessment &amp; Authorization Process Policy and Procedures</b>	
<b>Process Owner:</b> NESDIS Chief Information Division	Document Release Date: September 1, 2011

Prepared by:

  
Erica Boyd  
Ambit- Associate Consultant  
NESDIS Chief Information Office

3/25/15  
Date:

Approved by:

  
Irene Parker  
Assistant Chief Information Officer - Satellites

3/25/15  
Date:

### Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
2.2	March 25, 2015	----	ALL	Baseline NQP-3401