

NESDIS

System Security Plan Development and Maintenance 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

Record of Changes/Revisions.....	7
1.0 Background and Purpose.....	1
2.0 Scope	1
3.1 Roles, Responsibilities, and Coordination.....	1
3.2 Authorizing Official (AO)	1
3.3 Authorizing Official’s Designated Representative (AODR).....	2
3.4 Information System Owner (SO)	2
3.5 Information Technology Security Officer (ITSO)	2
3.6 Information System Security Officer (ISSO).....	2
3.7 Change Control Board (CCB)	2
4.0 Management Commitment	2
5.1 Compliance.....	2
5.2 References	3
6.1 Policy	3
6.2 Policy Maintenance.....	3
6.3 Policy Feedback Process.....	3
6.4 Policy Effective Date.....	3
7.1 System Security Planning	3
7.2 SDLC SSP Management Approach.....	4
7.1.1 Initiation.....	5
7.1.2 Development/ Acquisition	5
7.1.3 Implementation	6
7.1.4 Operations/Maintenance.....	6
7.1.5 Disposal	7
7.2 SSP Documentation Detail States.....	7
7.2.1 Initial Draft/Concept.....	7
7.2.2 Refined	7
7.2.3 Fully Documented	7
7.2.4 AO Approved.....	8

7.2.5	Independently Tested.....	8
7.2.6	POA&M Integrated	8
7.2.7	Continuous Monitoring/ CCB Updates	8
8.1	Procedures	9
8.2	Information System Name / Title.....	16
8.3	Security Categorization	16
8.4	System Owner	16
8.5	Authorizing Official.....	17
8.6	Other Designated Contacts	17
8.7	Assignment of Security Responsibility	17
8.8	Operational Status	18
8.9	Information System Type.....	18
8.10	General System Description / Purpose	18
8.10-	System Environment	20
8.11-	System Inter-connections / Information Sharing.....	20
8.12	Related Laws / Regulations / Policies.....	21
8.13	System Security Plan Completion Date.....	22
8.14	System Security Plan Approval Date	22
8.15	Rules of Behavior	22
8.16	Minimum Security Controls.....	23
8.17	SSP Appendix A: FIPS 199 Categorization.....	23
8.18	SSP Appendix B: Line Office & NOAA/NNN Personnel Lists	24
8.19	SSP Appendix C: System Description	24
8.20	SSP Appendix D: Environment Description/System Inventory	24
8.21	SSP Appendix E: Related Laws/Regulations/Policies.....	24
8.22	SSP Appendix F: Rules of Behavior (RoB).....	24
8.23	SSP Appendix G: Privacy Threshold Analysis (PTA)/ Privacy Impact Assessment (PIA).....	24
8.24	SSP Appendix H: Continuous Monitoring Plan	24
8.25	SSP Appendix I: Service Level Agreement	25
8.27	SSP Appendix K: Contingency Test Plan and Results	26
	Appendix A – SSP Acceptable Content.....	27
A.1	System Diagram Requirements.....	27

A.2	Security Control Documentation Requirements.....	28
	Appendix B - System Boundary Architecture Diagram.....	30



UNITED STATES DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration
NATIONAL ENVIRONMENTAL SATELLITE
DATA AND INFORMATION SERVICE
Silver Spring, Maryland 20910

September 30, 2012

MEMORANDUM

Distribution

FOR: FROM:

Catrina D. Purvis
NESDIS Chief Information Officer (Acting)

SUBJECT:

Issuance of Updated NESDIS Information
Technology Security Policies and Procedures

This is to announce the issuance of 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 in 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*, v2.1;
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 on NESDIS Information Systems*, v3.1.

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 Nancy.DeFrancesco@noaa.gov or phone (301) 713-1312.

**NESDIS SYSTEM SECURITY PLAN DEVELOPMENT AND MAINTENANCE
 POLICY AND PROCEDURES**

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
Draft 1.0	06/01/2009	All	Noblis	1 st Draft
Draft 2.0	08/22/2009	All	ITSO	Updated for comments
Pre-final Draft 3.0	9/15/2009	3.0, 5.1, 6.0, 7.0, section numbering	ITSO	Updated for NESDIS-wide comments and issued as pre-final draft for comment.
Final v1.0	9/30/2009	Date	ITSO	Finalize
Draft v1.1	8/15/2011	Headers, footers, add Appendix E, policy references and terminology; delete Appendices C and D; add references to SSP Compliance Review Checklist mandated by NOAA and the NESDIS P&P for IT Systems Inventory.	ITSO	FY2011 review and update
V2.0 final	9/01/2011	All	ITSO	Removed Draft markings and finalized

1.0 Background and Purpose

The Federal Information Security Management Act [(FISMA), Public Law 107-347] requires the documentation of plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. The Department of Commerce (DOC) *IT Security Program Policy* (ITSPP), Section 4.12.2, requires compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, when developing System Security Plans (SSPs).

This policy and procedures are intended to assist system owners to determine 1) what level of detail must be documented in the SSP, and 2) compliance with SSP development and maintenance requirements as the system progresses through each phase of the System Development Life Cycle (SDLC). Failure to document the appropriate level of detail in NESDIS SSPs has significant negative impact on the Authorizing Official's (AOs) ability to use it as a basis for making fully informed risk-based accreditation decisions. Failure to develop and maintain the SSP as the system progresses throughout the SDLC results in substantial and overly burdensome costs during assessment and authorization (A&A) reviews. A standard NESDIS SSP development and maintenance approach is necessary to achieve highest degree of security and cost effectiveness across NESDIS systems.

Accordingly, the purpose of this document is to provide NESDIS-specific policies and procedures for developing and maintaining the SSP with the required level of detail as the system progresses through each phase of the SDLC.

2.0 Scope

The scope of this document is limited to NESDIS-specific SSP development and maintenance policies and procedures, and is intended to be used as a companion to NIST SP 800-18. This document is not intended to be a stand-alone SSP guide and intimate knowledge and understanding of NIST SP 800-18 is required to develop a fully compliant SSP.

All NESDIS employees and contractors responsible for the development and maintenance of SSPs for NESDIS information systems, including contractor-owned and -operated systems that contain NESDIS information, must comply with the policies and procedures identified in this document.

3.1 Roles, Responsibilities, and Coordination

The NIST SP 800-18, the DOC ITSPP, and the NOAA Security Manual describe roles and responsibilities of key participants in the development and maintenance of the SSP. NESDIS supplements those key participant roles and responsibilities as follows.

3.2 Authorizing Official (AO)

The AO is responsible for approving the SSP. The AO may however delegate the SSP approval function to the AO's Designated Representative. However, the AO cannot delegate approval of specific elements of the SSP, including the approval of the

security categorization,¹ the security controls baseline,² and interconnection security agreements.³

3.3 Authorizing Official's Designated Representative (AODR)

The AODR is responsible for approving the SSP on behalf of the AO, if such function is delegated from the AO.

3.4 Information System Owner (SO)

The SO is ultimately responsible for ensuring the protections of the system are accurately documented in a SSP at the appropriate level of detail throughout each phase of the SDLC. The SO may however; delegate the SSP development and maintenance function to the Information System Security Officer (ISSO).

3.5 Information Technology Security Officer (ITSO)

The ITSO is responsible for performing quality reviews of the SSP before the SO submits the SSP to the AO for approval and periodically throughout the SDLC.

3.6 Information System Security Officer (ISSO)

The ISSO is responsible for developing and maintaining the SSP throughout the SDLC, if such function is delegated from the SO. The ISSO is a voting member of the Change Control Board (CCB) responsible for assessing the security impact for all system changes and is responsible for updating the SSP to reflect changes. The ISSO is also responsible for maintaining the appropriate security posture of the information system in accordance with the approved SSP.

3.7 Change Control Board (CCB)

The CCB is responsible for ensuring that all changes to the information system are appropriately documented in the SSP and supporting documents before the change request (CR) is closed. The CCB is also responsible for ensuring risk assessments are performed and appropriately documented for each change.

4.0 Management Commitment

The NESDIS Chief Information Division (CID) supports the NESDIS Assistant Administrator's (AA's) strong emphasis on securing NESDIS information and information systems. Through the issuance of this policy and procedures document, the NESDIS CID demonstrates its commitment to implementing a cost effective IT Security program with a standard approach to the development and maintenance of current and comprehensive SSPs throughout the SDLC.

5.1 Compliance

The NESDIS ITSO shall review the SSP and its supporting documents for compliance with this policy as mandated by NOAA IT Security Manual 212-1301, Section 5.C.1. SOs with SSPs found not to be in compliance with this policy may be reported to the NESDIS Chief

Information Officer and/or the system's AO. At the AO's discretion, the system's Authorization to Operate (ATO) may be revoked and/or SO removed from their appointment as system owner.

5.2 References

- DOC ITSPP Section 4.12.2 (January 2009)
- NOAA IT Security Manual (March 2008)

6.1 Policy

As required by DOC ITSPP Section 4.12.2, NESDIS system owners shall establish and update annually, a system security plan for each NESDIS information system that complies with the recommendations of NIST SP 800-18. SSPs shall be documented in accordance with the NOAA format.⁴ The NESDIS ITSO shall monitor the completeness and accuracy of SSPs created and maintained by system owners. The SSP shall reflect the requirements documented in the latest version of NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, as tailored by the system's FIPS 200 report. The current version of NIST SP 800-53 is revision 3, dated August 2009.

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 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 regarding any errors found in the document or other clarifications or updates that are required.

6.4 Policy Effective Date

This policy is effective upon issuance.

7.1 System Security Planning

Executing a risk management approach for systems means integrating security early and throughout the SDLC. Integration requires an early start and regular updates of the SSP to ensure adequate security planning, acquisition, development, and deployment throughout the SDLC.⁵ "System security planning is an important activity that supports the SDLC and should be updated as system events trigger the need for revision in order to accurately reflect the most current state of the system."⁶ Accordingly, the SSP is a living document which must provide a summary of security requirements for the information system and describe the security controls planned or in place for meeting those requirements. Life cycle management of the SSP will help document security relevant decisions and provide assurance that security is fully considered in all SDLC phases.

7.2 SDLC SSP Management Approach

NESDIS requires SDLC Management of the SSP as depicted in the center row to the figure 1 below. The figure also depicts where SSP development and maintenance activities occur within the A&A process defined in NIST SP 800-37 Revision 1 , *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and the SDLS phases defined in NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*.

System Development Life Cycle Management of the SSP								
System Development Life Cycle (NIST SP 800-64 Revision 2)	Initiation		Development/ Acquisition		Implementation/ Assessment	Operation/ maintenance	Disposal	
SSP SDLC Management (NIST SP 800-18 Revision 1)	FIPS 199, BIA, and PIA complete		Security Requirements Analysis, Security Architecture, FIPS200 Baseline Security Controls, SSP, and Risk Assessment complete		Security Assessment Report and rest of A&A security authorization package complete		SSP and Risk Assessment updated yearly	FISMA Inventory Updated
	SSP Development					SSP Maintenance		
Authorization & Assessment Process	Step 1: Security	Step 2: Select Controls	Step 3: Implement Controls		Step 5: Authorization	Step 6: Continuous Monitoring		
			Step 4: Assessment					

FIGURE 1 - SYSTEM DEVELOPMENT LIFE CYCLE MANAGEMENT OF THE SSP

“A typical SDLC includes five phases: initiation, development/ acquisition, implementation/ assessment, operations/ management, and disposal. Each phase includes a minimum set of security tasks needed to effectively incorporate security in the system development process.”⁷

⁵ NISTSP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*

⁶ NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*

⁷ NIST SP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*

Correspondingly, with the NESDIS SDLC SSP Management approach, each SDLC phase requires differing levels of detail in the SSP. The sections below provide a high level description of NESDIS SSP documentation requirements for each SDLC phase.

7.1.1 Initiation

During the Initiation Phase when the system design and development teams begin to define the information system, the SO must also begin to develop the SSP. This early state of the SSP must include a narrative that describes the system's mission/purpose and a general system description including the proposed architecture and user base. During this phase, SO must also identify the information types to be processed/ stored by the system and document the associated security impact categorization of the system in a draft FIPS 199 for AO approval. The NESDIS *Federal Information Processing Standards Publication (FIPS) 199 Policy and Procedures* provides detailed guidance on creating and receiving AO approval of the FIPS 199 security categorization. The SO must also perform, document, and submit for AO approval the initial business impact analysis (BIA) and privacy impact assessment (PIA).⁸

While the system may not be fully defined, an early start on the SSP allows the requirements to mature as needed and in a cost effective manner. For example, the system description may only document the overall concept of the system and very high level description of the system including only planned services. It will likely not have a comprehensive topological diagram since the full design of the system is likely in flux. However, the information must be sufficient to provide input to perform an initial risk assessment, determine architectural constraints and requirements, and plan the employment of common services. Engineering security into a system or product's initiation phase can substantially reduce the need for costly additive security controls.

7.1.2 Development/ Acquisition

The Development/ Acquisition phase of the SDLC focuses on requirements refinement, performing an initial risk assessment, and security planning. The requirements refinement activity reviews the functional and security requirements during initial hardware and software acquisition and expands on the high level requirements (FISMA compliance, Common Criteria, FIPS 140-2 compliance) to create detailed requirements for the development phase.

The risk assessment provides a framework for the detailed requirements creation by identifying system risks and the mitigation required to reduce the risk. As part of the requirement analysis activity, the SO must use the FIPS 199 categorization to create the security control requirements in accordance with FIPS 200 and NIST SP 800-53 control selection and tailoring. The NESDIS *Federal Information Processing Standards Publication (FIPS) 200 Security Controls Selection and Tailoring Policy and Procedures* provides detailed guidance on creating and receiving AO approval of the FIPS 200 security baseline requirements analysis.

⁸ The current versions of all templates and checklists used in NESDIS can be found on the NESDIS IT Security Handbook website at: https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

In this phase of the SDLC, the SO must update the SSP to capture the risk assessment findings from the development/ acquisition phase system architecture, design, and requirements. As the development/ acquisition phase progresses, the implementation details will evolve and the SO must update the SSP's planned control descriptions to actual in place control implementation details.

The SO must also update the system's topology diagrams and interconnection information. At the end of development/ acquisition phase, the overall implementation for securing the information system must be defined and sufficiently documented in the SSP to support security testing.

7.1.3 Implementation

During the SDLC Implementation Phase, the SO must update the SSP with the descriptions of remaining in place implementation details including:

- System Topographical Diagrams
- System Hardware and Software Inventory
- Contingency Plan
- Incident Response Plan
- Security Awareness and Training Plan
- Configuration Management Plan
- Privacy Threshold Analysis/Privacy Impact Assessment
- E-Authentication Threshold Analysis/ E-Authentication Risk Assessment
- System Interconnection Agreements
- Security Configuration Checklists
- Security Control Implementation

In addition, this phase includes the Assessment and Authorization steps of the A&A process. As a result of the security controls assessment, the SO must update the SSP to reflect the results from testing and AO directives regarding the operations of the system. The SSP should be fully compliant with NIST guidance and DOC, NOAA, and NESDIS policy and process/procedures at the end of this phase. For more information about the A&A process, please reference the NESDIS *Risk Management Framework Assessment & Authorization Process Policy and Procedure*.

7.1.4 Operations/Maintenance

During the SDLC Operations/Maintenance Phase, the SO must update the SSP content whenever changes are made to the information system. The Configuration Control Board (CCB) must ensure the SSP content is up to date by mandating changes to the SSP and supporting documentation before a change request are closed. The SO must also keep the system diagrams and inventories up to date. A robust configuration management process will provide the framework for ensuring the SSP is properly maintained and kept up to date. The SO must update the SSP at least annually even if no configuration changes occur.

7.1.5 Disposal

During the SDLC Disposal phase, the SO must update the SSP to address both system and information status per National Archives and Records Administration (NARA) guidance and assist with management and disposition of associated Federal records.

The SSP must document the disposition of the hardware, software, data, and configuration information.

7.2 SSP Documentation Detail States

As provided in the SDLC SSP Management Requirements section above, the NESDIS SO is required to update SSP content as the system evolves throughout the SDLC. The **TABLE 1 - SSP Level of Detail Requirements Matrix** provided in the Section 8.0 Procedures section of this document will assist the SO in determining what level of documentation detail must be provided in the SSP during each phase of the SDLC. This will ensure the appropriate content is available for AO, ITSO, CIO, and Certifier reviews during system A&A.

The Table 1 - SSP Level of Detail Requirements Matrix identifies the following seven documentation detail states for SSP content:

7.2.1 Initial Draft/Concept

The Initial Draft/Concept documentation state provides an early stage description of the topic area. It includes early mission statements, high level system descriptions and/or expected/anticipated information. It is not intended to be detailed information of the final implementation. The purpose of documenting this information is for the SO to keep track of any early decisions or direction within the topic area. The initial draft documentation must be updated as the information changes, concepts are refined, and decisions finalized. This level of content is most typical within the Initiation phase of the SSP SDLC.

7.2.2 Refined

The Refined information documentation state provides moderately detailed information about the expected implementation of the topic area. This information should be more detailed than the initial draft, but still subject to changes due to technical hurdles, contracting proposal refinement, or other modification. The overall concept of the refined documentation should be solid; however the details may need additional information to be considered final. This level of content is most typical of the Development/ Acquisition phase of the SSP SDLC.

7.2.3 Fully Documented

The Fully Documented documentation state provides full implementation details or a detailed plan of implementation in the case of identified Plans of Action and Milestones (POA&Ms). Full system design is in place and implementation has begun. Contracts have been awarded and kickoffs have occurred. All parties involved are in agreement that this is the expected final description of the topic area. Minor adjustments may be made, but are not anticipated. The SO has signed off on the design and implementation of the information system as documented. This level of content is most typical within the

Implementation/ Assessment, Operations / Maintenance, and Disposal phases of the SSP SDLC.

7.2.4 AO Approved

The AO Approved documentation state requires that the NESDIS ITSO has completed the mandated SSP Compliance Review and that the AO (or, in most instances, the AODR) has approved the SSP. The SSP Compliance Review Checklist mandated by NOAA for use by the ITSO is available on the NESDIS IT Security Handbook website. The SO must complete any changes to the SSP directed by the ITSO in the Checklist prior to signature by the AO/AODR. This level of content is typical within the Implementation / Assessment, Operations / Maintenance, and Disposal phases of the SSP SDLC.

7.2.5 Independently Tested

The Independently Tested documentation state requires that the Certifier has performed independent testing of the details in the SSP and documented the results in the security assessment report (SAR). The SO has documented the results of the assessment in the SSP to reflect the independently tested implementation of the system. This level of content is most typical within the Implementation/ Assessment, Operations/ Maintenance, and Disposal phases of the SSP SDLC.

7.2.6 POA&M Integrated

The POA&M Integrated documentation state requires that the SO has fully documented the deficiencies from the security control assessment (or other testing report) in the SSP. The SO has also fully documented the planned implementation to correct the deficiencies in the SSP. The AO has formally accepted the POA&M and revised SSP. This level of content is expected within both the Operations/Maintenance and Disposal phases of the SSP SDLC.

7.2.7 Continuous Monitoring/ CCB Updates

The Continuous Monitoring/ CCB Updates documentation state requires that the Configuration Control Board (CCB) has a process in place for accepting or rejecting change requests to the system. The SO documents the results of the CCB decisions in the SSP and supporting documentation. The SSP and POA&Ms are updated to reflect the CCB approved changes. The SSP must include detailed plans or implementation details for POA&M and Configuration Change Request (CCR). This level of content expected within both the Operations/Maintenance and Disposal phases of the SSP SDLC.

8.1 Procedures

The procedures below provide the steps for how to use the Table 1- SSP Level of Detail Requirements Matrix to assist the SO in determining what level of detail must be provided in each section of the SSP during each phase of the SDLC. Additional guidance is included in Appendix A and Appendix B of this document regarding expectations for the level of detail required in documenting specific sections of the SSP.

- 8.1.1 Before developing any SSP content, determine which of the five SDLC phases appropriately reflects the system's current state.
- 8.1.2 In the far left column of the Table 1- SSP Level of Detail Requirements Matrix, locate the section(s) of the SSP for which you are developing content.
- 8.1.3 Determine which of the Documentation Detail States is required for that section(s) of the SSP for the appropriate SDLC phase using the Table 1- SSP Level of Detail Requirements Matrix as a guide.
- 8.1.4 Reference the SSP section below Table 1 that corresponds to the section you are developing for a description of what minimum information and detail must be documented.

TABLE 1 – SSP LEVEL OF DETAIL REQUIREMENTS MATRIX

SSP Level of Detail Requirements Matrix		Documentation Detail State						
SSP Sections ⁹	SDLC Phases ¹⁰	Initial Draft/ Concept	Refined	Fully Documented	AO Approved	Independently Tested	POA&M Integrated	Continuous Monitoring / CCB Updates
1 – Information System Name / Title	Initiation	X	X					
	Development/ Acquisition			X				
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
2 – Security Categorization	Initiation	X	X					
	Development/ Acquisition			X	X			
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
3 – System Owner	Initiation	X	X	X				
	Development/ Acquisition			X	X			
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
4 – Authorizing Official	Initiation	X	X	X				
	Development/ Acquisition			X				
	Implementation/ Assessment			X				
	Operations/ Maintenance			X				
	Disposal			X				
5 – Other Designated	Initiation	X						

⁹ As defined in the NOAA SSP Template. The current versions of all templates and checklists used in NESDIS can be found on the NESDIS IT Security Handbook website at:

https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

¹⁰ As defined in NIST SP 800-64 Revision 2, October 2008.

SSP Level of Detail Requirements Matrix		Documentation Detail State						
SSP Sections ⁹	SDLC Phases ¹⁰	Initial Draft/ Concept	Refined	Fully Documented	AO Approved	Independently Tested	POA&M Integrated	Continuous Monitoring / CCB Updates
Contacts	Development/ Acquisition		X					
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
6 – Assignment of Security Responsibility	Initiation	X	X					
	Development/ Acquisition			X				
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
7 – Operational Status	Initiation			X				
	Development/ Acquisition			X				
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
8 – Information System Type	Initiation	X	X					
	Development/ Acquisition			X	X			
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
9 - General System Description / Purpose	Initiation	X						
	Development/ Acquisition		X					
	Implementation/ Assessment			X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
10 – System	Initiation	X						

SSP Level of Detail Requirements Matrix		Documentation Detail State						
SSP Sections ⁹	SDLC Phases ¹⁰	Initial Draft/ Concept	Refined	Fully Documented	AO Approved	Independently Tested	POA&M Integrated	Continuous Monitoring / CCB Updates
Environment	Development/ Acquisition		X					
	Implementation/ Assessment			X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
11 – System Inter-connections / Information Sharing	Initiation	X						
	Development/ Acquisition		X					
	Implementation/ Assessment			X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
12 – Related Laws / Regulations / Policies	Initiation	X	X					
	Development/ Acquisition			X	X			
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
13 – System Security Plan Completion Date	Initiation	X	X					
	Development/ Acquisition		X					
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
14 – System Security Plan Approval Date	Initiation							
	Development/ Acquisition							
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
15 – Rules of Behavior	Initiation	X	X					

SSP Level of Detail Requirements Matrix		Documentation Detail State						
SSP Sections ⁹	SDLC Phases ¹⁰	Initial Draft/ Concept	Refined	Fully Documented	AO Approved	Independently Tested	POA&M Integrated	Continuous Monitoring / CCB Updates
	Development/ Acquisition			X				
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
16 – Security Control Baseline	Initiation	X						
	Development/ Acquisition		X					
	Implementation/ Assessment			X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
Appendix A – FIPS 199 Categorization	Initiation	X	X					
	Development/ Acquisition			X	X			
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
Appendix B: – Line Office & NOAA Personnel Lists	See row for Section 5 above							
Appendix C: – System Description	See row for Section 9 above							
Appendix D: – Environment Description/ System Inventory	See row for Section 10 above							
Appendix E: – Related Laws/ Regulations/ Policies	See row for Section 12 above							
Appendix F: – Rules of Behavior	See row for Section 15 above							
Appendix G1: –	Initiation	X	X	X	X			

SSP Level of Detail Requirements Matrix		Documentation Detail State						
SSP Sections ⁹	SDLC Phases ¹⁰	Initial Draft/ Concept	Refined	Fully Documented	AO Approved	Independently Tested	POA&M Integrated	Continuous Monitoring / CCB Updates
Privacy Threshold Analysis	Development/ Acquisition			X	X			
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X	X		
	Disposal			X	X	X	X	X
Appendix G2: – Privacy Impact Assessment	Initiation	X	X	X	X			
	Development/ Acquisition			X	X			
	Implementation/ Assessment			X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
Appendix H: – Continuous Monitoring Plan	Initiation							
	Development/ Acquisition	X	X	X	X			
	Implementation/ Assessment			X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
Appendix I: – Service Level Agreement (including ISAs, IATs, MOAs, and MOUs)	Initiation							
	Development/ Acquisition	X	X					
	Implementation/ Assessment		X	X	X			
	Operations/ Maintenance			X	X			
	Disposal			X	X			
Appendix J: – Contingency Plan	Initiation	X	X					
	Development/ Acquisition		X	X				
	Implementation/ Assessment			X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			

SSP Level of Detail Requirements Matrix		Documentation Detail State						
SSP Sections ⁹	SDLC Phases ¹⁰	Initial Draft/ Concept	Refined	Fully Documented	AO Approved	Independently Tested	POA&M Integrated	Continuous Monitoring / CCB Updates
Appendix K: – Contingency Test Plan and Results	Initiation							
	Development/ Acquisition	X	X					
	Implementation/ Assessment		X	X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
Appendix L: – Risk Assessment	Initiation	X	X	X	X			
	Development/ Acquisition		X	X	X			
	Implementation/ Assessment			X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal			X	X			
Appendix M: – Designation Letters	Initiation	X	X	X	X			
	Development/ Acquisition			X	X			
	Implementation/ Assessment			X	X			
	Operations/ Maintenance			X	X			
	Disposal							
Appendix N: – FIPS 200 Approval Memo	Initiation	X	X	X	X			
	Development/ Acquisition		X	X	X			
	Implementation/ Assessment			X	X	X		
	Operations/ Maintenance			X	X	X	X	X
	Disposal							

The NESDIS tailored NOAA SSP Template should be regarded as a starting point that dictates the data that must be included in the SSP. The SO is permitted to modify the template to suit local requirements, as long as the required information is provided and easily identifiable.

The following sections describe the NESDIS expectations for each section of the SSP in more detail:

8.2 Information System Name / Title

During the SDLC Initiation phase, the SO must provide a draft/concept level system name in the SSP. The SO may not have the official NOAA system name or title yet, but the locally known title of the IT system needs to be documented in the SSP. By the start of the Development/ Acquisition phase of the SSP SDLC, the system owner must request the NOAA official IT System name from NESDIS OCIO. Once this name and number are assigned, the SO can fully document the name and ID in the SSP. The AO will approve the name and ID as a part of the overall SSP approval process. The SO does not need to take additional actions to request AO approval of system name and ID. This section will not likely change from this point on during the entire Implementation/ Assessment, Operations /Maintenance, and Disposal phases of the SSP system life cycle.

8.3 Security Categorization

In the SSP SDLC Initiation phase, the system owner must document the preliminary FIPS 199 security categorization in the SSP. The system owner may not have all of the information types fully documented or AO approval of the FIPS 199 at this stage; however, the SO must create and document the anticipated FIPS 199 categorization. Any known data types and their associated impact levels should be included in the Draft FIPS 199 calculation. The SO should also have initiated communications with the ITSO for concurrence with the anticipated FIPS 199 categorization to reduce the impact of a possible incorrect determination. The SO must follow the NESDIS *Federal Information Processing Standards Publication (FIPS) 199 Policy and Procedures* for creating the FIPS 199.

By the start of the Development/ Acquisition phase, the SO should have completed the FIPS 199 calculation, received ITSO concurrence, and obtained AO approval. The SO must update the SSP to reflect the AO approval of the FIPS 199, including the FIPS 199 calculation with all information types. At this point, the security categorization should not change during the Development/ Acquisition, Implementation/ Assessment, and Operations/ Maintenance phases of the SDLC unless data types are added or removed from the information system. The security categorization section must not be changed during the disposal phase of the SSP SDLC.

8.4 System Owner

The development organization must identify the system owner early on in the SDLC. The NESDIS Office of Systems Development (OSD) performs most of the acquisition and development activities for new information systems. Since the system will eventually transition to the Office of Satellite and Product Operations (OSPO), a representative from the operating division is a key stakeholder in the design and development of the system and therefore must be involved at the early stages of the SDLC. During the initiation phase of the SDLC, the development organization and the CID must identify the development and operations system owners. The development system owner must be identified and documented early in the initiation phase to ensure that early system decisions are acceptable to the organization. The operational SO should be involved in the development process to ensure all their needs are met.

To oversee daily management of the system during the remaining SDLC phases, the SO must be fully documented and AO approved. The AO must appoint the SO in writing. The SO must file a copy of the SO appointment memo in SSP Appendix M as well as file a copy in the Cyber

Security Assessment and Management (CSAM) system in addition to submitting a copy for record to the ITSO.

8.5 Authorizing Official

The AO for FIPS 199 high impact information systems is the NESDIS Assistant Administrator. For Moderate impact systems, the co-AOs are the NESDIS CIO and the responsible office director. For Low impact systems, the AO is the responsible office director. During the initiation phase of the SDLC, the information system will have a refined FIPS 199 categorization, which will indicate the AO assignment based on the impact level. The SSP must reflect the AO assignment during each phase of the SDLC.

For FIPS 199 high impact systems, the NESDIS CIO is the AO's Designated Representative (AODR). For Moderate impact systems, the NESDIS ITSO is the AODR. The SSP must reflect the contact information for the AODR if applicable.

8.6 Other Designated Contacts

This section of the SSP identifies other persons with responsibility within the information system's lifecycle. SOs must identify all additional roles involved in the A&A process, including the Certifier, Program Manager, and any other system specific personnel. The SO must provide a complete list of system personnel responsible for the information system, including system administrators, developers, operators, auditors, and any other category of personnel responsible for operations of the system. This list should not include general users of the information system. Some additional roles to consider adding are key contractor personnel, A&A package development team, and user representatives. NIST SP 800-37 and supporting documentation document other roles and responsibilities that could be included in this section.

During the initiation phase, the SO must identify key personnel and document their contact information in this section of the SSP. It is possible this information is not yet finalized and personnel not yet identified. The SO should attempt to document these positions early in the process; however it is likely these positions will change over time. The SO is responsible for updating the SSP to document the current personnel assigned to the key roles. Once the system enters the implementation phase, the other designated contacts section of the SSP must be fully documented and approved by the AO/AODR.

8.7 Assignment of Security Responsibility

This section of the SSP identifies persons with security responsibility. The SO must provide the contact information for the officially-appointed ISSO in this section of the SSP. In addition, if the SO has formally designated an alternate ISSO or key security personnel in writing, their contact information must also reside in this section.

During the initiation phase, the SO must identify the ISSO and document their contact information in this section of the SSP. It is possible this information is not yet finalized and person not yet identified. The SO should attempt to document this position early in the process; however it is possible this position will change over time. The SO is responsible for updating the SSP to document the current personnel assigned to the key roles. Once the system enters the implementation phase, this section of the SSP must be fully documented and approved by the AO.

For NESDIS system in development, the development organization may identify the ISSO. The SO, both development and operational SO if applicable, must agree with the ISSO assignment. It is critical for the development organization to work closely with the operational organization to ensure the requirements of both organizations are included in the design and development.

8.8 Operational Status

The system owner must fully document the operational status at all phases of the SDLC. The operational status can be identified as:

- In Development, Not Operational
- Operational under Authorization to Operate (ATO)
- Operational under Interim Authority to Operate (IATO)
- Decommissioned, Not Operational

Information systems under development and connected to another information system or data source for testing only should be identified as “In Development, Not Operational” with an additional note stating the level of connection or data processing for testing purposes only. Also, the SO must document the approval to connect or process information for testing purposes only. Under no circumstance may the information system perform its primary mission without AO approval. Once the AO has approved operations, the SO must change the SSP to reflect the system’s operational status as one of the operational states. The Operational Status section of the SSP must be current and fully documented during each phase of the SDLC. AO approval is required to transition the system from development to operational.

8.9 Information System Type

The information system type must be defined early in the SDLC. Valid data types in this section of the SSP are “General Support System” and “Major Application”. For common controls, the information system type may be identified as “General Support System, Common Controls.” The SO must fully document one of these system types in the SSP during the initiation phase.

The AO must approve the system type at the start of the Development/ Acquisition phase of the SDLC.

8.10 General System Description / Purpose

This section of the SSP describes the information system, including the mission of the system and the user community of the system. System owners are required to include the following information in this section of the SSP:

- Succinct narrative describing what the system is, what it does, the population it serves, and how it fulfills the mission.
- Reference to all associated/related budget account codes used in Exhibits 300 and 53.
- A detailed topology narrative and graphic that clearly depict the system boundaries, system interconnections, and key¹¹ devices within the boundary.

¹¹ Key devices include perimeter security devices, firewalls, routers, switches, and file/print/application servers. End user workstations must also be depicted; however the system diagram is not required to depict each user

workstation. The diagram can depict a representative grouping of the workstations. System diagrams should depict workstations in all segments of the network as well as all facilities where they are located.

- All system diagrams provided must be fully and logically (sequenced) described in the text, including primary data flows and processing flow of the application from system input to system output.
- A description of the primary computing platform(s) used (e.g., mainframe, desktop, LAN or Wide Area Network (WAN)). Include a general description of the principal system components, including hardware, software, and communications resources.
- System Inventory Provide a complete listing of all hardware and software (system software and application software) components, including make/OEM, model, version, and service packs. Indicate if software is customized or COTS/GOTS. Indicate if hardware and software are government-owned or contractor-provided. (May be in the inventory)
- Describe how and when remote access is permitted and for what reason.
- Identify and describe the DMZ (if applicable), including each network component and host in the DMZ. Address the data flow of information into and out of the DMZ.
- Provide for each web server (internal and external) description of the User population, Access Controls that apply, and the data that is resident on the server.
- Discuss in detail each service accessible outside of the system boundary (FTP, SMTP, SSH, other).

During the initiation phase of the SDLC, the SO is likely not to have the required detailed information for each area within this section of the SSP. However, the SO should have limited information about the mission of the system and interconnections. The SO must document all information as it becomes available during the development process.

As the system enters into the Development/ Acquisition phase, the SO must document the refined description information. Sufficient information must exist for the SO to begin development or the acquisition activities. Any requirements information must be fully documented in the SSP during the Development/ Acquisition phase.

Once the system enters into the implementation phase, the system description must be fully documented. The AO/AODR must approve the description before implementation is completed. The SO is encouraged to have frequent conversations with the ITSO, AODR, and the AO to ensure that the system design and implementation does not expose NESDIS to unacceptable risk.

During the Operational/Maintenance phase of the SDLC, the SO must maintain currency of the information in the SSP. The system description must be kept up to date based on the approved changes¹². In the disposal phase, the SO must document the disposition of the information system, location of archived data, software, and hardware.

8.10- System Environment

This section of the SSP describes:

- the physical environment(s) where the information system resides,
- a description of the communications lines connecting the information system to other systems,
- technical that raise special security concerns (wireless; mobile devices; such as Blackberries, PDAs, and smart phones; and others),
- public access to the information system (physical and logical),
- major and minor applications supported by the information system,
- list of other systems that this information system interfaces with (e.g., ESPC interfaces with GOES and POES), and
- (for General Support Systems) list the number of users and list the user organizations (internal and external) that are supported by the system.

During the initiation phase of the SDLC, the SO is likely not to have the required detailed information for each area within this section of the SSP. However, the SO should have preliminary information for most topics. The SO must document all information as it becomes available during the development process.

As the system enters into the Development/ Acquisition phase, the SO must document the refined environmental information. Sufficient information must exist for the SO to begin development or the acquisition activities. Any requirements information must be fully documented in the SSP during the Development/ Acquisition phase.

Once the system enters into the implementation phase, the environmental description must be fully documented. The AODR must approve the description before implementation is completed. The SO is encouraged to have frequent conversations with the ITSO, AODR, and the AO to ensure that the system design and implementation does not expose NESDIS to unacceptable risk.

During the Operational/Maintenance phase of the SDLC, the SO must maintain currency of the information in the SSP. The system environment information must be kept up to date based on the approved changes¹³. In the disposal phase, the SO must document the disposition of the information system, location of archived data, software, and hardware.

8.11- System Inter-connections / Information Sharing

The interconnections/information sharing section of the SSP documents the physical interconnections and the logical interconnections. The SSP is required to document the physical interconnections, including leased lines, connections to other NOAA information systems for connectivity and data sharing, remote access via dial-up, and Internet connectivity. These interconnections require detailed information about the system connected to, including points of contact, FIPS categorizations, 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 concerns¹⁴ for sharing that information.

¹³ See *NESDIS Configuration Management Policy and Procedure* for more detailed requirements on implementing an acceptable configuration management program.

¹⁴ Security concerns revolve around the confidentiality, availability or the integrity of the information shared.

During the initiation phase of the SDLC, the details of all interconnections are likely not defined. However, based on the anticipated location of the information system and mission, some interconnections can be anticipated. For instance, information systems located in NSOF requiring Internet connectivity will likely have an interconnection to the NOAA MAN for that connectivity. Also, new satellite ground systems that collect environmental data will likely need to pass that data to ESPC for processing and possibly CLASS for archive. These initial interconnections should be documented to indicate the likely connections to these systems.

As the system design progresses into the Development/ Acquisition phase, additional details will emerge. The SP is required to update the SSP to reflect these design decisions. Systems in the implementation phases and beyond require all interconnections and data sharing to be fully documented, independently tested¹⁵, and AO approved.

During the Operation/Maintenance phase, the interconnections may change due to risk assessments, changes in requirements, or architectural changes. If these changes occur, the interconnections section must be updated to reflect the accurate connectivity and data sharing agreements. All changes to the interconnections require AO approval before the change is implemented.

8.12 Related Laws / Regulations / Policies

During the initiation phase of the SDLC, the SO must ensure all applicable laws, regulations, and policies are identified that impact the process or development activities. NESDIS provides a list of applicable laws, regulations, and policies in the SSP template. The SO should review these default laws, regulations, and policies and determine if they are applicable to the information system. In the initiation phase, the system is not fully designed. Therefore, the laws, regulations, and policies cannot be finalized. As the system design changes, the laws, regulations, and policies may change. In addition, the SO must add in any unique laws, regulations, and policies based on the system specific implementation or mission.

Once the system moves into the development and acquisition phase, all applicable laws, regulations, and policies must be fully documented, ITSO reviewed and AO/AODR approved. Throughout the remainder of the SDLC, the laws, regulations, and policies must be fully documented, AO/AODR approved and kept up to date as they change or new revisions are released. As a part of continuous monitoring, the SO is required to annually review and update the SSP. During this review and update, the SO must determine if all the documented laws, regulations, and policies remain applicable. New revisions¹⁶ of the documentation must be included in this section of the SSP and fully integrated into the information system. Also, throughout the operations and maintenance phase, if a change request introduces new or removes the need for any law, regulation, or policy, the SO must take the appropriate action to update the laws, regulations, and policies section as well as integrate the new requirement into the all aspects of the information system, including the SSP.

¹⁵ For FIPS 199 Moderate and High impact systems.

¹⁶ New revisions of NIST guidance are not required unless mandated by DOC, NOAA, or NESDIS. System owners may choose to follow new NIST guidance if it is more appropriate to their information system. NESDIS does not mandate Draft NIST guidance.

8.13 System Security Plan Completion Date

The System Security Plan Completion date section of the SSP identifies the date the SSP was last updated. The purpose of this is to maintain version control as well as identify the age of the document. During the initiation phase of the SDLC, the SO will frequently update the SSP. This date should reflect the completion date of the significant versions of the SSP. It is not necessary to update this date daily; however, when the SSP is released for review, the date must be updated to reflect the date of the last revision. This date will change frequently through the initiation and development phases of the SDLC.

Once the system enters the implementation phase, the system should be fully documented and the SSP completion date must be identified. During Operations, the SO must update the date to reflect the AO/AODR approved SSP completion date. Since the SSP is a living document, the SO will continue to modify this date field for each SSP update. The SO also must update the SSP Completion Date when performing an annual review and update of the SSP.

In the SSP SDLC Initiation and Development/ Acquisition phases, the system owner needs to provide a refined content update anticipating this date. At the start of the Implementation/ Assessment phase of the SSP SDLC, the system owner needs to fully document this anticipated date and then contact the NESDIS OCIO for guidance on implementing contracts anticipating the start of the Authorization process in a reasonable timeframe (several months in advance of the anticipated SSP completion date). The section's content will change at least yearly during the entire Implementation/ Assessment, Operations / Maintenance, and Disposal phases of the SSP system life cycle.

8.14 System Security Plan Approval Date

The SSP Approval date is the date that the AO (or AODR) approved and signed the SSP. Include a reference to the SSP version approved by the AO/AODR. The AO/AODR must approve the SSP once the system enters the implementation phase of the SDLC. Prior to that phase, the SSP is not finalized and not available for full AO/AODR approval.

Changes implemented during the operation/maintenance phase of the SDLC will require updates to the SSP. The AO/AODR approval date and the SSP completion date may not always be consistent due to these changes. However, when significant changes¹⁷ occur, the SO must request AO (or AODR) written approval of the SSP.

8.15 Rules of Behavior

NOAA has defined a common set of Rules of Behavior (RoB) that all systems must follow. These are references in the NOAA IT Security Manual 212-1302. All system SSPs must refer to the NOAA RoB. In addition, systems may supplement the NOAA RoB with system specific RoB. This section of the SSP must document the reference to the NOAA RoB as well as provide details on the system specific RoB if applicable. NESDIS does not supplement the NOAA RoB.

During the initiation phase of the SDLC, the SO must begin the process of defining if system specific RoBs are required and if so, begin the process of defining them. As the system moves

into the Development/ Acquisition phase, the system-specific RoB must be fully documented. AO approval is required for the implementation phase and beyond.

The SO may reference the RoB in this section of the SSP and provide the details in an appendix.

8.16 Minimum Security Controls

The Minimum Security Controls section of the SSP documents the implementation details and plans for implementation of the security controls required by the FIPS 200.

During the initiation phase of the SDLC, the SO will begin developing the concept/mission of the information system and the initial design. The minimum security controls section of the SSP during this phase will contain very limited information about the implementation (or plans for implementing) the security controls. The SO should have preliminarily identified the FIPS 199, which will define the initial baseline of security controls. Also, the SO should identify any NOAA and NESDIS common controls that will likely apply. This section of the SSP must contain the preliminary information as it becomes available to the SO and the development team.

During the Development/ Acquisition phase, the SO will have completed the FIPS 200 control selection process. All of the security controls and their associated control tailoring must be documented in this section of the SSP, and the AO-approved FIPS 200 analysis included in Appendix N. All of the implementation details may not be fully defined. Initial implementation details and general implementation strategy should be documented.

During the implementation phase, the SO must fully document the implementation of each required security control. The AO/AODR must approve the SSP, including the control descriptions. Also, towards the end of the implementation phase, the Certifier will oversee independent assessment of the security controls. The SO must ensure the SSP is revised to reflect the results of the independent testing. The SO must document deficiencies found during testing, including documenting the detailed POA&Ms to correct the deficiency.

During the operations/maintenance phase, the SO must ensure the security control implementation details are kept current and accurately reflect the implementation of the information system. The SO must update the SSP based on POA&M closures and change requests. Also, during the continuous monitoring activities, the SO must ensure the implementation documentation reflects the testing results.

8.17 SSP Appendix A: FIPS 199 Categorization

The FIPS 199 security categorization drives the security requirements and risk impact ratings with the information system. Creating the correct FIPS 199 categorization is critical to successfully managing the certification and accreditation process.¹⁸ The SO must have an initial draft of the FIPS 199 very early in the initiation phase of the SDLC. Shortly afterwards, the SO needs to refine the FIPS 199 and obtain ITSO concurrence with the proposed categorization. At the start of the Development/ Acquisition phase, the SO must finalize, fully document, and receive AO approval of the FIPS 199. Over the remainder of the SDLC, the FIPS 199 will not change unless the system, mission, or sensitivity of the information significantly changes. The

¹⁸ See the NESDIS *Federal Information Processing Standards Publication (FIPS) 199 Policy and Procedures* for more information.

FIPS 199 appendix of the SSP must include the full calculation of the security categorization, including all data types and rationale for their associated security impact. Any deviation from NIST SP 800-60 must be fully documented to capture the decision-making process. The AO-approved FIPS 199 analysis must be filed in CSAM.

8.18 SSP Appendix B: Line Office & NOAA/NNN Personnel Lists

The personnel list provides role and contact information for personnel who have significant roles in the system operation. Any person in a specific role discussed in the SSP should be included in the personnel list, such as system and network administrators, continuity of operations personnel, physical security personnel, etc. The list should also include anyone who receives specific role-based security training, as described in AT-3 Security Training. The list must be maintained throughout the implementation and operational phase of the system lifecycle.

8.19 SSP Appendix C: System Description

The description provided in this appendix is a more detailed discussion than that provided in SSP Section 9 – General System Description/Purpose. See Section 8.9 of this document for the discussion of content required for this appendix.

8.20 SSP Appendix D: Environment Description/System Inventory

The description provided in this appendix is a more detailed discussion than that provided in SSP Section 10 – System Environment. See Section 8.10 of this document for the discussion of content required for this appendix. Refer to the *NESDIS IT Systems Inventory Management Policy and Procedures* for requirements in documenting the system component inventory.

8.21 SSP Appendix E: Related Laws/Regulations/Policies

This appendix provides a list of federal laws, policies, and implementation guidance that apply to the system. DOC specific, NOAA, NESDIS, and local office policies and implementation guidance should be addressed in the SSP, Section 12 – Related Laws/Regulations/Policies. See Section 8.12 of this document for a detailed discussion of content required for this appendix. List DOC, NOAA, and NESDIS-specific policies and procedures in Section 12, and list here federal regulations and public laws.

8.22 SSP Appendix F: Rules of Behavior (RoB)

This appendix provides detailed system specific RoB. See Section 8.15 of this document for a detailed discussion of content required for this appendix.

8.23 SSP Appendix G: Privacy Threshold Analysis (PTA)/ Privacy Impact Assessment (PIA)

This appendix contains a copy of the SO and NOAA Privacy Coordinator approval page of the PTA. The complete PTA and PIA documents must be filed in CSAM. The PTA/PIA must be completed and approved prior to the completion of the initiation life cycle phase.

8.24 SSP Appendix H: Continuous Monitoring Plan

This appendix contains the system Continuous Monitoring Plan. 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:

- a) Quarterly vulnerability scanning (RA-5), including required scanning for unauthorized wireless access points for AC-18(2) as required by DOC ITSP.
- b) Semi-annual account reviews (AC-2).
- c) Monthly Plan of Actions and Milestones (POA&M) updates (CA-5).
- d) System maintenance (MA-2), including routine patching schedules (SI-2)
- e) 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).
- f) Annual contingency plan (CP), business impact analysis (BIA), and CP test plan and results (CPTPR) updates; CP training, CP testing, and backup and recovery testing (CP-2, CP-3, CP-4, and CP-9/CP-10).
- g) Annual physical access record reviews (PE-2) and monthly visitor access record reviews (PE-8).
- h) Semi-annual update of FISMA Inventory information in CSAM (PL-1).
- i) Annual reviews of access agreements (PS-6 -- see DOC ITSP, 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).
- j) Annual risk assessment update (RA-3), which would at a minimum coincide with scheduling of the annual independent security controls assessment for CA-2.
- k) Semi-annual SI-7 integrity scans required by DOC ITSP.
- l) 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 CTR-006.
- m) Annual incident response training (IR-2, IR-3).

8.25 SSP Appendix I: Service Level Agreement

This appendix contains copies of connectivity, data sharing, and service agreements that document agreed upon standards between the system and the external entity, including Interconnection Security Agreements, SLAs, and Memoranda of Agreement/Understanding. The SO should begin drafting the agreements as early in the development and implementation phases as the need for the arrangement is identified and must be finalized and approved by both entities prior to certification activities.

8.26 SSP J Appendix: Contingency Plan

This appendix contains a copy of the SO and AO/AODR approval page for the Contingency Plan after it has passed NESDIS ITSO Compliance Review. The CPTPR Compliance Review

Checklist used by the ITSO is available on the NESDIS IT Security Handbook website. The complete plan must be filed in CSAM.

8.27 SSP Appendix K: Contingency Test Plan and Results

This appendix contains a copy of the approval page for the Contingency Test Plan and Results (CPTPR) document after it has passed NESDIS ITSO Compliance Review. The CPTPR Compliance Review Checklist used by the ITSO is available on the NESDIS IT Security Handbook website. The complete test plan and results must be filed in CSAM.

8.28 SSP Appendix L: Risk Assessment

This appendix contains a copy of the cover page for the Risk Assessment Report. The complete report must be provided in the system's CSAM record.

8.29 SSP Appendix M: Designation Letters

This appendix contains a copy of designation letters for critical IT Security roles in the system. At a minimum, a copy of the ISSO and SO appointment letters must be included.

8.30 SSP Appendix N: FIPS 200 Approval Memo

This appendix contains a copy of the AO approval page for the FIPS 200 analysis. The complete FIPS 200 analysis document must be provided in the system's CSAM record.

Appendix A – SSP Acceptable Content

The SSP is required to document the security of the information system. In order for the security to be verifiable, the system and its environment must be adequately documented to support a full understanding of the risks related to operational use. NIST provides guidance for the development of the SSP in NIST SP 800-18; however, it does not provide detailed acceptance criteria for the content. This SSP Acceptable Content Appendix provides additional guidance to assist the SO with SSP development and maintenance activities compliant with NESDIS/NOAA/DOC's requirements.

A.1 System Diagram Requirements

The System Description section of the SSP requires the SO to provide detailed system diagram(s) depicting the information system, its interconnections, its components, and internal connectivity. The purpose of the diagrams is to visually document the information system and provide details into the architecture of the information system. NESDIS requires the system diagrams meet the following criteria:

A.1.1 System Diagrams May Be Identified as Multiple Diagrams

Some NESDIS information systems are large and complex architectures. For these systems, the SO is encouraged to create multiple logical diagrams with increasing level of detail to describe the system. The diagrams should move from the high level diagram showing the system boundary and interconnections with the information system identified as a cloud or multiple clouds to the lower level diagrams showing more detailed logical system diagrams. Each lower level diagram should expand out a cloud identified on the higher level diagram until each system component is identified and documented. If sub-diagrams are implemented, a clear understanding must be depicted to ensure the reader understands what sub-section of the information system is shown.

A.1.2 System Diagrams Must Clearly Identify the System Boundary

System diagrams must ensure the reader can easily identify a component as within or external to the information system. The diagram must have a clear solid line identified with a "System Boundary" label. Expanded cloud sub-diagrams, where all components in the diagram are within the boundary, must be depicted or described in the legend as being completely within the security boundary. SOs may also depict this by drawing the security boundary around all components in the diagram.

Some information systems have components in multiple sites that are disconnected or contain gaps of control between the two segments. These system diagrams must show multiple boxes surrounding the components within the control of the information system.

A.1.3 System Diagrams Must Identify All Physical and Logical Interconnections

At the highest level diagram, the SO must ensure all interconnections are properly identified and documented. The physical interconnections must visually cross the system boundary. All interconnections documented in the "Interconnections" section of the SSP must be identified in the diagrams.

A.1.4 System Diagrams Must Identify All Components Listed in the Hardware Inventory

The SO must ensure that all information system components are clearly identified in the system diagram using the unique identifier from the system inventory. Each identifier must include the system name and the associated IP address (if applicable). For example, an information system contains two Cisco PIX 535 firewalls. The system diagram must identify each firewall individually to ensure the correct hardware is associated with the diagram icon. One firewall is named “FW1” and the other is “FW2”. The diagram must identify each firewall icon as “FW1, 192.168.1.10” and “FW2, 192.168.1.11”.

A.1.5 System Diagrams Must be Logical Diagrams

The system diagram must show the logical connections and location of the components. Rack and wiring diagrams are useful, however, they are difficult to use for describing the information system. Components with multiple logical connections must be identified as having multiple connections. Additional icons can be used to depict the logical locations of components; however, the diagram must identify a component as having multiple connections through alternate color or shading of the icon. For extremely complex networks, additional diagrams may be required to fully document the logical network connections.

A.1.6 System Description Must Fully Document the Diagram

The system description must include verbiage describing the system diagram. Every component in the diagram must have a corresponding text description with identical identifiers for tracking. There should be a description of the processing flow of the application from system input to system output.

A.2 Security Control Documentation Requirements

Each NIST SP 800-53 control requires detailed description of the implementation. Sufficient information is required to facilitate testing of the control. Below is a list of NESDIS requirements for documenting the security controls within the SSP.

A.2.1 All NIST SP 800-53 Controls Must be Included in the SSP

If the control is not required or has been tailored out of the baseline through the FIPS 200 process, the SO must document the control is not required or not applicable. A short description of why the control is not required or not applicable must be documented in the control implementation description section. If the security control is modified from the NIST SP 800-53 definition, the SSP must include the original NIST 800-53 control description and the description of the AO approved modified control.

A.2.2 Control Description Must Match the Control

The SO must carefully read the control requirements and address all parts of the control requirement. If the control was tailored or compensated in the FIPS 200, the SO must document the tailored or compensated control.

A.2.2 Control Description Must Include Complete Implementation Details

Control descriptions must be provided for each operating system environment, configuration item, with location specific details.

A.2.3 Security Controls Identified as Common Controls Must Include the Common Control Description

NESDIS encourages the use of common controls. When documenting the common controls in the SSP, the SO should paraphrase the common control implementation description and refer the reader to the original common control security plan for complete implementation and testing details. System owners are responsible for implementing the security requirements as defined in the AO approved FIPS 200.

In the event the SO implements a control via common control inheritance, the SO must ensure the implementation of the common control meets the requirements of the information system. If the control is not fully implemented by the Common Control Provider (CCP), the SO must supplement the CCP's implementation with system specific implementation or identify a POA&M to fully implement the control¹⁹.

A.2.4 Control Description Must Include All Applicable Parameters

NIST identifies organization-defined control parameters for certain controls in the SP 800-53 control catalog. The SO is responsible for documenting the control parameters for these security controls. Also, DOC/NOAA/NESDIS publish policy that may dictate the minimum configuration for certain controls. The SO must adopt the DOC/NOAA/NESDIS published configuration at a minimum. SO may strengthen the configuration as they feel is necessary for their information system.

A.2.5 Security Controls with Deficiencies Must Include Detailed Plan of Action and Milestones (POA&Ms)

Security controls with identified deficiencies must include a POA&M to address the deficiency identified. The detailed corrective action plan must be documented in the SSP as a part of the security control description. The plan must include details of the plan to correct the deficiency, the responsible person for completion of the POA&M, the planned start and finish dates for the deficiency correction, CSAM POA&M identifier, and details of the funding for the POA&M. Refer to the NESDIS Plan of Action and Milestones (POA&M) Management Handbook for further information on how to complete the POA&M process.

Appendix B - System Boundary Architecture Diagram

Below is an example of a compliant system boundary architecture diagram which presents a very basic and NESDIS compliant picture of a fictional NOAAAnnnn IT system with just five (5) hardware and software components. It shows the accreditation boundary with all the hardware inventory components included in the diagram and it shows all of the connecting devices that may affect the potential data flow for the system's security. The hardware noted on the diagram can be mapped to the software inventory.

In the body of SSP text the system owner would likely mention in the description of the system boundary architecture diagram that *“The Sierra component functions as a database server, which uses the MySQL database under a Linux OS. The Foxtrot component functions as a web application server for this specific IT system and is running an Apache Tomcat web application under the Windows 2003 OS. The Bravo component functions as an intrusion detection appliance server and runs the Snort IDS application under the Windows XP OS. The Delta component functions as a network monitoring server and runs a Nagios application under the Windows XP OS. The Alfa component functions as the IT system network switch and firewall appliance; it runs a firewall application under a CISCO IOS.”* This system diagram depicts a LAN component from another related environment outside the security accreditation boundary line that connects to the system referenced within the SSP example. It is not part of the system accreditation boundary or of the inventory of the system covered within the diagram. However, it is important for the SO to visually show the potential data interconnections that may affect the security within the accreditation boundary.

Note the system accreditation boundary is clearly marked with a solid line and labeled to identify internal and external components. The Alfa, Bravo, Delta, Foxtrot, and Sierra components are inside the boundary while the Tango and NSOF Intranet are outside the accreditation boundary. These are shown for a complete understanding to the reader of the interconnections and data flow of the system.

The system boundary architecture diagram within the SSP must reflect all components within the Configuration Management Baseline (CM-2) as required by the DOC ITSP.

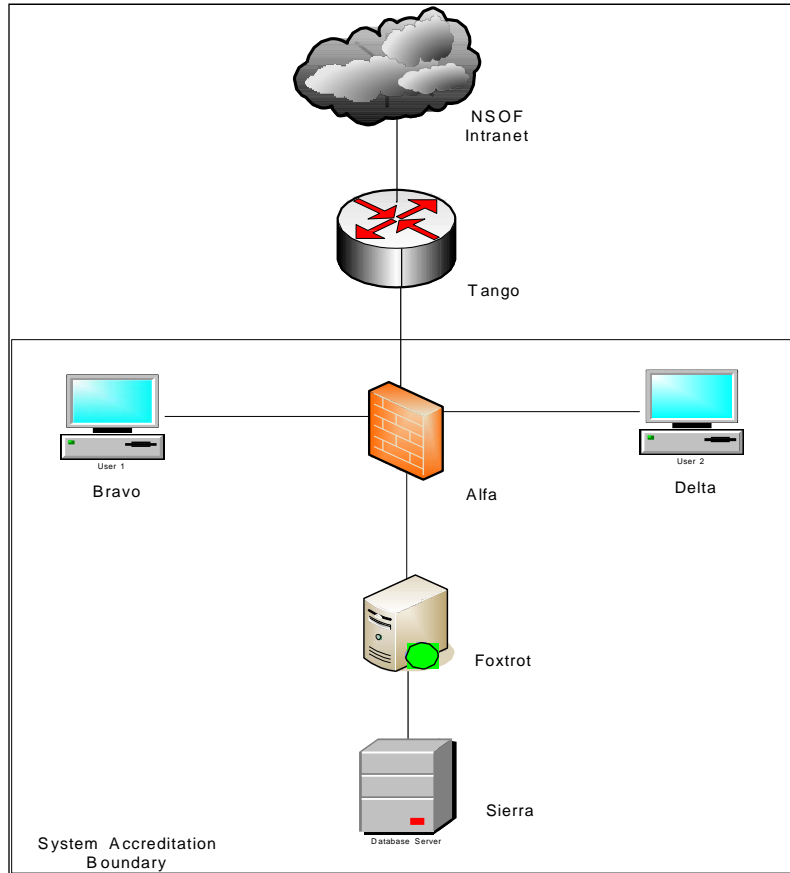
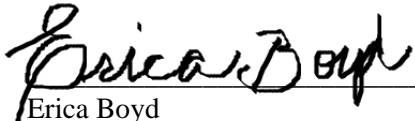


FIGURE 2 - SYSTEM BOUNDARY ARCHITECTURE DIAGRAM EXAMPLE

Approval Page


Document Number: NQP-3415, Revision 2.1	
Document Title Block: System Security Plan Development and Maintenance Policy and Procedures	
Process Owner: NESDIS Chief Information Division	Document Release Date: September 1, 2011

Prepared by:


Erica Boyd
Ambit- Associate Consultant
NESDIS Chief Information Office

3/26/15
Date:

Approved by:


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-3415