NOAA/NESDIS

Federal Information Processing Standards Publication 199 Security Categorization Policy and Procedures

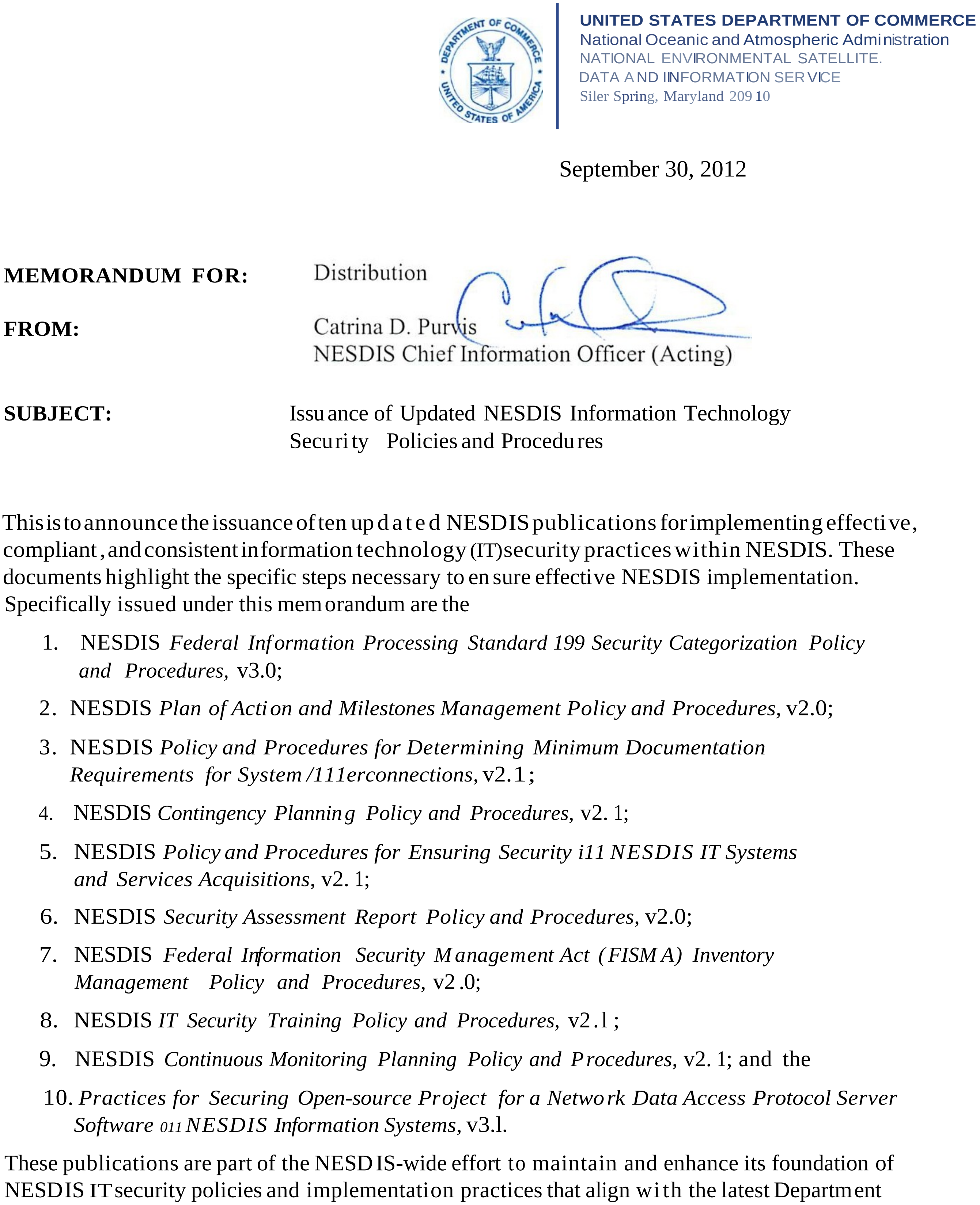
September 1, 2012

Prepared by:

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

Table of Contents

Record of Changes/Revisions 5
2.0 Scope 6
3.0 Roles and Responsibilities 6
4.0 Management Commitment 6
5.0 Compliance 7
6.0 NESDIS FIPS 199 Policy 7
7.0 Procedures 8
1. System Overview 1
2. Purpose and Methodology 4
3. FIPS 199 Analysis for NOAA50xx 6



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

September 30, 2012

MEMORANDUM FOR: Distribution

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

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

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

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

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

NESDIS FIPS 199 SECURITY CATEGORIZATION POLICY AND PROCEDURES

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
Draft 1.0	6/19/2009	All	Noblis	Draft
Draft 2.0	6/22/2009	All	ITSO	Initial Review
Draft 3.0	6/22/2009	All	Noblis	Incorporation of ITSO Revisions
Draft 3.1	8/19/2009	All	ITSO	Incorporation of NESDIS ISSO comments
Pre-final Draft 3.2	9/15/2009	3.1, 7.0, 7.1.4.1	ITSO	Incorporate NESDIS-wide comments and issued pre-final draft for final comments
Final v1.0	9/30/2009	Date	ITSO	Finalize
Draft v1.1	8/15/2011	Headers, footers, Appendix B, terminology	ITSO	FY2011 review and update
2.0 final	9/01/2011	All	ITSO	Removed Draft markings and finalized
3.0	9/01/2012	7.1.3, 7.1.4.2	ITSO	FY2012 review and update

1.0 Background and Purpose

The Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541, *et seq.*, directed the promulgation of federal standards for the security categorization of federal information and information systems based on objectives of providing the appropriate levels of information security according to a range of risk levels. The Federal Information Processing Standards (FIPS) Publication 199, entitled *Standards for Security Categorization of Federal Information and Information Systems,* establishes those federal standards.[1]

The purpose of this document is to provide NESDIS-specific policies and procedures for implementing FIPS 199.

2.0 Scope

The scope of this document is limited to NESDIS-specific procedures for 1) determining, 2) documenting, 3) obtaining Information Technology Security Officer (ITSO) review and Authorization Official (AO) approval of, and 4) complying with FIPS 199 security categorization requirements.

3.0 Roles and Responsibilities

3.1 Authorizing Official (AO)

The AO is responsible for approving the FIPS 199 security categorization.

3.2 Information System Owner (SO)

The SO is responsible for preparing, updating, and meeting all NESDIS FIPS 199 security categorization requirements identified in this document. The SO may however; delegate FIPS 199 activities to the Information System Security Officer (ISSO).

3.3 Information Owner (IO)

The IO is the agency official with statutory and/or operational authority for protecting specified information. The IO is responsible for informing the SO of all information types for which they are responsible and identifying any unique requirements for the protection of that information, including the controls for its generation, collection, processing, dissemination, and disposal.

3.4 Information Technology Security Officer (ITSO)

The ITSO is responsible for performing quality reviews of all FIPS 199 documents and artifacts prior to submission for AO approval.

3.5 Information System Security Officer (ISSO)

The ISSO is responsible for maintaining the appropriate security posture of the system in accordance with the approved FIPS 199. The ISSO is also responsible for performing additional FIPS 199 activities, as delegated by the SO.

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 Chief

Information Division

(CID) demonstrates its commitment to implementing a cost effective IT Security program with a standard approach to implementing the FIPS 199 security categorization process. This issuance also demonstrates CID commitment to ensuring that FIPS 199 documentation and artifacts submitted to any NESDIS AO for approval provide sufficient basis for a fully informed risk acceptance decision.

5.0 Compliance

The NESDIS ITSO monitors – through periodic quality reviews and monthly performance metrics – implementation of the Assessment and Authorization (A&A) process within NESDIS to ensure compliance with applicable laws, directives, policies, and guidance. The ITSO reports to the AA monthly, and to the CIO and Office Directors as necessary regarding compliance. The AA, Chief Information Officer, 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.

5.1 References

- DOC *Information Technology Security Program Policy* (ITSPP), section 4.14.2 (January 2009)
- NIST Special Publication (SP) 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: Volume I and Volume II* (August 2008)

6.0 NESDIS FIPS 199 Policy

As required by DOC ITSPP section 4.14.2, the NESDIS-specific FIPS 199 process and procedures shall align with the FIPS 199 and NIST SP 800-60 prescribed practices for the determining the security categorization of systems. This document provides NESDIS-specific procedures for implementing FIPS 199 and NIST SP 800-60 and should be used as companion document for implementation within NESDIS and not as a replacement document.

6.1 Policy Maintenance

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

6.2 Policy Feedback Process

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

6.3 Policy Effective Date

This policy is effective upon issuance.

7.0 Procedures

Implementing the FIPS 199 security categorization of information and information systems is a critical first step of the NESDIS risk assessment process. Performing the FIPS 199 as a part of the risk assessment enables security to be planned, acquired, built in, and deployed as an integral part of a system early and throughout the system development life cycle (SDLC).

The procedures below provide step-by-step instructions for implementing FIPS 199 using the NESDIS required FIPS 199 template provided at Appendix A of this document (current versions of templates used in NESDIS can be found on the NESDIS IT Security Handbook website at: https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php).

7.1 Determining FIPS 199 Information and Information System Security Categories

7.1.1 Required Input

The SO must identify the following prior to performing the FIPS 199 part of the risk assessment.

- A high level system description, including the purpose of the system. The SO may reference the System Security Plan description of the system environment and the Business Impact Analysis for additional information regarding the importance/criticality of the system to the overall mission and the logical and physical partitioning of service enclaves within the environment.
- A general characterization of the information which will be stored, processed, or transmitted by the system. The SO may reference interconnection agreements and requirements documents to ensure all information types shared/exchanged are identified.
- Information security and data protection requirements that are unique for a specific information type, as dictated by the IO, if applicable. In a service-oriented architecture, the system environment may be partitioned into several enclaves with different security categorizations or with the same categorizations but different function. These differences and the services supported by the partition may affect the determination of the security controls requirements baseline and tailoring.

7.1.2 Documenting Information Types

The SO must meet with all IOs in the selection of information types defined in the NIST SP 800-60, Volume II, Appendices C and D,[2] and select on the FIPS 199 all of the information types which will be stored, processed, or transmitted by the system. The "Impact Level Assessment Table" provided in the NESDIS FIPS 199 template lists all NIST SP 800-60 identified information types. The SO must place a checkmark (i.e., X) in the left column of the "Impact Level Assessment Table" next to each selected information type.

7.1.3 Documenting Impact Level Assessments

The SO must review the provisional impact level assignments provided in NIST SP 800-60 for each selected information type. These provisional impact level assignments are also identified in the NESDIS FIPS 199 template for SO convenience. Compliant with NIST SP 800-60 guidance on existence of exceptions to provisional impact level assignments, the SO must use the "Assessment of Impact" columns of the "Impact Level Assessment Table" to document the system-specific impact level assessment (High, Moderate, or Low) for the Confidentiality, Integrity, and Availability of each selected information type.

Note, however, that the rationale for all deviations from the NIST provisional impact level assignments must be documented in the "Summary Analysis" section of the NESDIS FIPS 199 template described in section 7.1.4.2 of this document.

Review other documents including Interconnection Security Agreements, Business Impact Analysis, interface requirements documents, and critical infrastructure system interdependencies to understand and align with the sensitivity of the system's information types from the perspective of customers and other users of the information.

Figure 1.0 below depicts an excerpt of the "Impact Level Assessment Table" provided in the NESDIS FIPS 199 template to be completed.

		NIST 800-60 Categorization of Information				**<NOAA50xx> Assessment of Impact**		
		Information Types for this System / Application(s):	**C-Impact**	**I-Impact**	**A-Impact**	**C-Impact**	**I-Impact**	**A-Impact**
X		**MISSION-BASED INFORMATION**				**Confidentiality (H/M/L)**	**Integrity (H/M/L)**	**Availability (H/M/L)**
	D.8	***ENVIRONMENTAL MANAGEMENT***						
	D.8.1	Environmental Monitoring/Forecasting	Low	Moderate	Low			
	D.8.2	Environmental Remediation	Moderate	Low	Low			
	D.8.3	Pollution Prevention And Control	Low	Low	Low			
	D.19	***GENERAL SCIENCE & INNOVATION***						
	D.19.1	Scientific and Tech Research and Innovation	Low	Moderate	Low			
	D.19.2	Space Exploration and Innovation	Low	Moderate	Low			
		MANAGEMENT & SUPPORT INFORMATION						
	C.3.2	***FINANCIAL MANAGEMENT***						
	C.3.2.1	Asset and Liability Management	Low	Low	Low			
	C.3.2.2	Reporting and Information	Low	Moderate	Low			
	C.3.2.3	Budget and Finance	Moderate	Moderate	Low			
	C.3.3	***HUMAN RESOURCES***						
	C.3.3.4	Resource Training and Development	Low	Low	Low			
	C.3.3.5	Security Clearance Management	Low	Moderate	Low			
	C.3.3.6	Staff Recruitment and Employment	Low	Low	Low			
	C.3.5	***INFORMATION & TECHNOLOGY MANAGEMENT***						
	C.3.5.1	System Development	Low	Moderate	Low			
	C.3.5.2	Lifecycle / Change Management	Low	Moderate	Low			
	C.3.5.3	System Maintenance	Low	Moderate	Low			
	C.3.5.4	IT Infrastructure Maintenance	Low	Moderate	Low			
	C.3.5.5	IT Security	Low	Moderate	Low			

Figure 1— Impact Assessment Table Excerpt

7.1.4 Required Output

The SO must document and complete the remaining sections of the NESDIS FIPS 199 template as follows:

7.1.4.1 Designated Contacts

The SO must provide contact information for the following roles in the NESDIS FIPS 199 template:

- Authorization Official (AO) or co-AOs
- Information System Owner (SO)
- Information Owner (IO)
- Information Technology Security Officer (ITSO)
- Information System Security Officer (ISSO)

The information depicted below in Figure 2 must be provided for each role identified above.

Name	
Role	
Title	
Agency	
Address	
Email address	
Phone number	

Figure 2 – Required FIPS 199 Contact Information

7.1.4.2 FIPS 199 Analysis

The SO must complete the Summary Analysis section of the NESDIS FIPS 199 template in the format identified below in Figure 3. If the system environment contains partitions of different security categorizations, then document the partitioning in separate sections of the FIPS 199 analysis.

FIPS 199 Analysis for <NOAA50xx>

[Provide the breakout of the information and mission types identified in the checklist in the format identified below.]

The <NOAA50xx> system contains the following Security Categorization of Service Delivery Support Information (NIST SP 800-60, Revision 1, Volume II, Appendix C) and/or Mission Information (NIST SP 800-60, Revision 1, Volume II, Appendix D). The default security impacts were selected for all NIST SP 800-60 information and mission types.

SC $_{\text{C..2.1.3 Program Monitoring}}$ *= {(confidentiality,* ***Low****), (integrity,* ***Low****), (availability,* ***Low)****}.*

SC $_{\text{D.4.1 Disaster Monitoring}}$*= {(confidentiality,* ***Low****), (integrity,* ***High****), (availability,* ***High****)}.*

Therefore, the overall security impact of the <NOAAnnnn> system is:

*SC <****NOAAnnnn*** *>= {(confidentiality,* ***Low****), (integrity,* ***High****), (availability,* ***High****)}*

The high watermark security impact for the system overall is ***High****.*

<u>Disaster Monitoring Service Enclave</u>

The high watermark security impact for consideration in the FIPS 200 evaluation of the Disaster Monitoring Service enclave is ***High****. The Disaster Monitoring Service enclave data supports DOC Primary Mission Essential Functions (PMEFs) and loss of integrity or availability could jeopardize lives and property. Also, the integrity of the disaster program performance measurement data must be maintained to create reliable statistics for oversight committee and public information regarding program performance effectiveness.*

<u>Program Monitoring Service Enclave</u>

The high watermark security impact for consideration in the FIPS 200 evaluation of the Program Monitoring Service enclave is ***Low****. The Program Monitoring Service enclave consists of publicly-available websites containing statistical information derived from program performance measurement data. The statistics can be readily recreated from the input data stored in the Disaster Monitoring Service enclave. The enclave provides a data dissemination service to the public via web portal.*

Figure 3 –Required Summary FIPS 199 Analysis Information Example

7.2 Obtaining ITSO Review and AO Approval

The SO must complete and document the FIPS 199 using the NESDIS required FIPS 199 template and submit it securely via PGP-encrypted email or hand-deliver to the

ITSO for compliance review. The ITSO will review and provide compliance assessment results to the SO within five (5) business days of receipt. If the FIPS 199 is determined compliant by the ITSO, the ITSO will assist the SO in obtaining AO approval by helping to coordinate routing among stakeholders for concurrence and providing the AO with their recommendation for approval. If the FIPS 199 is determined non-compliant, the ITSO will provide revision recommendations which must be completed by the SO and resubmitted to the ITSO within 5 business days of their receipt of the comments from the ITSO.

In no case shall the SO submit the FIPS 199 to the AO without obtaining ITSO concurrence. In the event that the SO and ITSO cannot agree on the FIPS 199 security category, they will meet together with the AO to discuss the differences in their assessments.

In all cases, the AO will make the final determination and approval decision. The AO approval must be documented using the FIPS 199 AO Signature Page Template at Appendix B of this document.

7.3 Complying with FIPS 199 Continuous Monitoring Requirements

The system's overall FIPS 199 security category, which is derived from the security impact highest watermark, will provide a basis for the FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, analysis. See NESDIS *FIPS 200 Security Control Selection and Tailoring Policy and Procedures* for detailed instructions on how to conduct a FIPS 200 analysis.

NESDIS requires annual SO review, and update if necessary, of the FIPS 199 as part of the annual review of System Security Plans and Risk Assessments. The annual SO review of the FIPS 199 must include a repeat of the procedures identified in section 7.1 and, if necessary, section 7.2 of this document. The SO must also update the FIPS 199 whenever a new information type is added to or removed from the system during the system configuration management process (e.g., addition or change in use of an information collection component to the system environment such as a database or file server).

All FIPS 199 changes require written approval from the AO. The FIPS 199 must, at a minimum, be re-authorized in writing by the AO at least every 3 years as part of the *Monitor Security Controls* Step of the system's assessment and authorization process.

The SO must maintain the FIPS 199 Record of Changes to record the initial issuance and subsequent annual reviews and updates.

Appendix A - NESDIS FIPS 199 Template

FOR OFFICIAL USE ONLY

Federal Information Processing Standards (FIPS) 199 Analysis for System Name (System Acronym) NOAA50xx

Prepared by:
<enter preparer's name and contact information>

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

<Date>

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) 199 ANALYSIS FOR NOAA50XX

Record of Changes/Revisions

Version	Date	Section	Author	Change Description

1. System Overview

a. Information System Name/Title

System Name: Enter full name and do not use acronyms
System ID: NOAA50xx
Data National Security Classification: Unclassified

b. System Description

[Provide a SHORT (1-3 paragraph) description of the information system's purpose/mission(s) from the System Security Plan]

c. Points of Contact

Primary Authorizing Official (AO)

Name	
Role	
Title	
Agency/LO	
Address	
Email address	
Phone number	

co-Authorizing Official (co-AO) *(if applicable)*

Name	
Role	
Title	
Agency/LO	
Address	
Email address	
Phone number	

AO's Designated Representative (AODR)

Name	
Role	
Title	
Agency/LO	
Address	
Email address	
Phone number	

Information System Owner (SO)

Name	
Role	
Title	
Agency/LO	
Address	
Email address	
Phone number	

Information Owner 1 (IO)

Name	
Role	
Title	
Agency/LO	
Address	
Email address	
Phone number	
Information Type(s) Owned	

Information Owner 2 (IO) *[add more IOs as needed]*

Name	
Role	
Title	
Agency/LO	
Address	
Email address	
Phone number	
Information Type(s) Owned	

Information Technology Security Officer (ITSO)

Name	
Role	
Title	
Agency/LO	
Address	
Email address	
Phone number	

Information System Security Officer (ISSO)

Name	
Role	
Title	
Agency/LO	
Address	
Email address	
Phone number	

2. Purpose and Methodology

The purpose of this *Federal Information Processing Standard (FIPS) 199 Analysis* is to document the security categorization for <SYTEM NAME or ID> in accordance with the Federal Information Security Management Act of 2002 (FISMA). FISMA requires that federal agencies utilize the standards and guidelines issued by the National Institute of Standards and Technology (NIST) to categorize information systems and the information types collected or maintained by or on behalf of each agency. These standards and guidelines are based on the objectives of providing appropriate levels of information security according to a range of risk levels and of recommending the types of information and information systems to be included in each category.

The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, and maintain its day-to-day functions. The system owner must complete the FIPS 199 categorization using NIST Special Publication (SP) 800-60 guidance to categorize the confidentiality, integrity, and availability security objectives for the system's information types. These categorizations are used to establish the high watermark categorization for each security objective that in turn are used to establish the system's overall categorization and the FIPS 200 associated controls baseline. Upon completion of the FIPS 199 table, the system owner must first obtain AO approval, then use this result to establish the high watermark needed to determine the minimum security controls FIPS 200 baseline.

The table in Section 4 provides a checklist for recording the system's information types and selected categorizations for confidentiality, integrity, and availability for each information type. It includes the categorizations as recommended by NIST SP 800-60 as well as the selection or tailoring of the recommended categorization as appropriate for the data and mission types collected or maintained by <SYSTEM NAME or ID>. In addition, the security categorization was determined using the Homeland Security Presidential Directive 7 (HSPD-7), the Patriot Act, and the criteria contained in FIPS 199, which;

"[E]stablishes security categories for both information, and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization."[3]

- References
  - HSPD-7, *Homeland Security Presidential Directive*, December 17, 2003
  - HR 3162 RDS, *USA Patriot Act*, October 24, 2001

[3] FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems,*

February 2004.

3. FIPS 199 Analysis for NOAA50xx

[Provide the breakout of the information and mission types identified in the checklist in the format identified below.]

The *NOAA50xx* system contains the following Security Categorization of Service Delivery Support Information (NIST SP 800-60 Revision 1 Volume 2, Appendix C) and/or Mission Information (NIST SP 800-60 Revision 1 Volume 2, Appendix D). The default security impacts were selected for all NIST SP 800-60 information and mission types.

[List ALL information types checked in the table in Section 4]

SC C.1.2.3 Information Type 1= {(confidentiality, *high/moderate/low*), (integrity, *high/moderate/low*), (availability, *high/moderate/low*)}.

SC D.1.2 Information Type 2 = {(confidentiality, *high/moderate/low*), (integrity, *high/moderate/low*), (availability, *high/moderate/low*)}.

Therefore, the overall security impact of the ***NOAA0xx*** system is:

SC *NOAA50xx* = {(confidentiality, *high/moderate/low*), (integrity, *high/moderate/low*), (availability, *high/moderate/low*)}

The high watermark security impact for consideration in the FIPS 200 evaluation is [**High, Moderate, or Low**].

4. Information Type Selection Table

“X” if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
MISSION-BASED INFORMATION								
	D.1	***DEFENSE & NATIONAL SECURITY***	Nat’l Security	Nat’l Security	Nat’l Security			
	D.2	***HOMELAND SECURITY***						
	D.2.1	Border Control and Transportation Security	Moderate	Moderate	Moderate			
	D.2.2	Key Asset and Critical Infrastructure Protection	High	High	High			
	D.2.3	Catastrophic Defense	High	High	High			
	D.2.4	Executive Functions of the EOP	High	Moderate	High			
	D.3	***INTELLIGENCE OPERATIONS***	High	High	High			
	D.4	***DISASTER MANAGEMENT***						
	D.4.1	Disaster Monitoring and Prediction	Low	High	High			
	D.4.2	Disaster Preparedness and Planning	Low	Low	Low			
	D.4.3	Disaster Repair and Restoration	Low	Low	Low			
	D.4.4	Emergency Response	Low	High	High			
	D.5	***INTERNATIONAL AFFAIRS & COMMERCE***						
	D.5.1	Foreign Relations	High	High	Moderate			
	D.5.2	International Development and Humanitarian Aid	Moderate	Low	Low			
	D.5.3	Global Trade	High	High	High			
	D.6	***NATURAL RESOURCES***						

"X" if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	D.6.1	Water Resource Management	Low	Low	Low			
	D.6.2	Conservation, Marine, and Land Management	Low	Low	Low			
	D.6.3	Recreational Resource Management and Tourism	Low	Low	Low			
	D.6.4	Agricultural Innovation and Services	Low	Low	Low			
	D.7	***ENERGY***						
	D.7.1	Energy Supply	Low	Moderate	Moderate			
	D.7.2	Energy Conservation and Preparedness	Low	Low	Low			
	D.7.3	Energy Resource Management	Moderate	Low	Low			
	D.7.4	Energy Production	Low	Low	Low			
	D.8	***ENVIRONMENTAL MANAGEMENT***						
	D.8.1	Environmental Monitoring/Forecasting	Low	Moderate	Low			
	D.8.2	Environmental Remediation	Moderate	Low	Low			
	D.8.3	Pollution Prevention And Control	Low	Low	Low			
	D.9	***ECONOMIC DEVELOPMENT***						
	D.9.1	Business and Industry Development	Low	Low	Low			
	D.9.2	Intellectual Property Protection	Low	Low	Low			
	D.9.3	Financial Sector Oversight	Moderate	Low	Low			
	D.9.4	Industry Sector Income Stabilization	Moderate	Low	Low			
	D.10	***COMMUNITY & SOCIAL SERVICES***						

"X" if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	D.10.1	Homeownership Promotion	Low	Low	Low			
	D.10.2	Community and Regional Development	Low	Low	Low			
	D.10.3	Social Services	Low	Low	Low			
	D.10.4	Postal Services	Low	Moderate	Moderate			
	D.11	***TRANSPORTATION***						
	D.11.1	Ground Transportation	Low	Low	Low			
	D.11.2	Water Transportation	Low	Low	Low			
	D.11.3	Air Transportation	Low	Low	Low			
	D.11.4	Space Operations	Low	High	High			
	D.12	***EDUCATION***						
	D.12.1	Elementary, Secondary, & Vocational Education	Low	Low	Low			
	D.12.2	Higher Education	Low	Low	Low			
	D.12.3	Cultural & Historic Preservation	Low	Low	Low			
	D.12.4	Cultural & Historic Exhibition	Low	Low	Low			
	D.13	***WORKFORCE MANAGEMENT***						
	D.13.1	Training and Employment	Low	Low	Low			
	D.13.2	Labor Rights Management	Low	Low	Low			
	D.13.3	Worker Safety	Low	Low	Low			
	D.14	***HEALTH***						

"X" if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	D.14.1	Access to Care	Low	Moderate	Low			
	D.14.2	Population Health Management and Consumer Safety	Low	Moderate	Low			
	D.14.3	Health Care Administration	Low	Moderate	Low			
	D.14.4	Health Care Delivery Services	Low	High	Low			
	D.14.5	Health Care Research and Practitioner Education	Low	Moderate	Low			
	D.15	***INCOME SECURITY***						
	D.15.1	General Retirement and Disability	Moderate	Moderate	Moderate			
	D.15.2	Unemployment Compensation	Low	Low	Low			
	D.15.3	Housing Assistance	Low	Low	Low			
	D.15.4	Food and Nutrition Assistance	Low	Low	Low			
	D.15.5	Survivor Compensation	Low	Low	Low			
	D.16	***LAW ENFORCEMENT***						
	D.16.1	Criminal Apprehension	Low	Low	Moderate			
	D.16.2	Criminal Investigation and Surveillance	Moderate	Moderate	Moderate			
	D.16.3	Citizen Protection	Moderate	Moderate	Moderate			
	D.16.4	Leadership Protection	Moderate	Low	Low			
	D.16.5	Property Protection	Low	Low	Low			
	D.16.6	Substance Control	Moderate	Moderate	Moderate			

"X" if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	D.16.7	Crime Prevention	Low	Low	Low			
	D.16.8	Trade Law Enforcement	Moderate	Moderate	Moderate			
	D.17	***LITIGATION & JUDICIAL ACTIVITIES***						
	D.17.1	Judicial Hearings	Moderate	Low	Low			
	D.17.2	Legal Defense	Moderate	High	Low			
	D.17.3	Legal Investigation	Moderate	Moderate	Moderate			
	D.17.4	Legal Prosecution and Litigation	Low	Moderate	Low			
	D.17.5	Resolution Facilitation	Moderate	Low	Low			
	D.18	***FEDERAL CORRECTIONAL ACTIVITIES***						
	D.18.1	Criminal Incarceration	Low	Moderate	Low			
	D.18.2	Criminal Rehabilitation	Low	Low	Low			
	D.19	***GENERAL SCIENCE & INNOVATION***						
	D.19.1	Scientific and Technological Research and Innovation	Low	Moderate	Low			
	D.19.2	Space Exploration and Innovation	Low	Moderate	Low			
	D.20	***KNOWLEDGE CREATION & MANAGEMENT***						
	D.20.1	Research and Development	Low	Moderate	Low			
	D.20.2	General Purpose Data and Statistics	Low	Low	Low			
	D.20.3	Advising and Consulting	Low	Low	Low			

“X” if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	D.20.4	Knowledge Dissemination	Low	Low	Low			
	D.21	***REGULATORY COMPLIANCE & ENFORCEMENT***						
	D.21.1	Inspections and Auditing	Moderate	Moderate	Low			
	D.21.2	Standards Setting / Reporting Guideline Development	Low	Low	Low			
	D.21.3	Permits and Licensing	Low	Low	Low			
	D.22	***PUBLIC GOODS CREATION & MANAGEMENT***						
	D.22.1	Manufacturing	Low	Low	Low			
	D.22.2	Construction	Low	Low	Low			
	D.22.3	Public Resources, Facility, and Infrastructure Management	Low	Low	Low			
	D.22.4	Information Infrastructure Management	Low	Low	Low			
	D.23	***FEDERAL FINANCIAL ASSISTANCE***						
	D.23.1	Federal Grants (Non-State)	Low	Low	Low			
	D.23.2	Direct Transfers to Individuals	Low	Low	Low			
	D.23.3	Subsidies	Low	Low	Low			
	D.23.4	Tax Credits	Moderate	Low	Low			
	D.24	***CREDITS & INSURANCE***						
	D.24.1	Direct Loans	Low	Low	Low			
	D.24.2	Loan Guarantees	Low	Low	Low			

“X” if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	D.24.3	General Insurance	Low	Low	Low			
	D.25	***TRANSFERS TO STATE / LOCAL GOVERNMENTS***						
	D.25.1	Formula Grants	Low	Low	Low			
	D.25.2	Project / Competitive Grants	Low	Low	Low			
	D.25.3	Earmarked Grants	Low	Low	Low			
	D.25.4	State Loans	Low	Low	Low			
	D.26	***Direct Services for Citizens***						
	D.26.1	Military Operations	N/A	N/A	N/A			
	D.26.2	Civilian Operations	N/A	N/A	N/A			
MANAGEMENT & SUPPORT INFORMATION								
Services Delivery Support Information								
	C.2.1	***CONTROLS & OVERSIGHT***						
	C.2.1.1	Corrective Action (policy/regulation)	Low	Low	Low			
	C.2.1.2	Program Evaluation	Low	Low	Low			
	C.2.1.3	Program Monitoring	Low	Low	Low			
	C.2.2	***REGULATORY DEVELOPMENT***						
	C.2.2.1	Policy and Guidance Development	Low	Low	Low			
	C.2.2.2	Public Comment Tracking	Low	Low	Low			

“X” if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	C.2.2.3	Regulatory Creation	Low	Low	Low			
	C.2.2.4	Rule Publication	Low	Low	Low			
	C.2.3	***PLANNING & Budgeting***						
	C.2.3.1	Budget Formulation	Low	Low	Low			
	C.2.3.2	Capital Planning	Low	Low	Low			
	C.2.3.3	Enterprise Architecture	Low	Low	Low			
	C.2.3.4	Strategic Planning	Low	Low	Low			
	C.2.3.5	Budget Execution	Low	Low	Low			
	C.2.3.6	Workforce Planning	Low	Low	Low			
	C.2.3.7	Management Improvement	Low	Low	Low			
	C.2.3.8	Budgeting & Performance Integration	Low	Low	Low			
	C.2.3.9	Tax and Fiscal Policy	Low	Low	Low			
	C.2.4	***INTERNAL RISK MANAGEMENT & MITIGATION***						
	C.2.4.1	Contingency Planning	Moderate	Moderate	Moderate			
	C.2.4.2	Continuity of Operations	Moderate	Moderate	Moderate			
	C.2.4.3	Service Recovery	Low	Low	Low			
	C.2.5	***REVENUE COLLECTION***						
	C.2.5.1	Debt Collection	Moderate	Low	Low			
	C.2.5.2	User Fee Collection	Low	Low	Moderate			

"X" if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	C.2.5.3	Federal Asset Sales	Low	Moderate	Low			
	C.2.6	***PUBLIC AFFAIRS***						
	C.2.6.1	Customer Services	Low	Low	Low			
	C.2.6.2	Official Information Dissemination	Low	Low	Low			
	C.2.6.3	Product Outreach	Low	Low	Low			
	C.2.6.4	Public Relations	Low	Low	Low			
	C.2.7	***LEGISLATIVE RELATIONS***						
	C.2.7.1	Legislative Tracking	Low	Low	Low			
	C.2.7.2	Legislation Testimony	Low	Low	Low			
	C.2.7.3	Proposal Development	Moderate	Low	Low			
	C.2.7.4	Congressional Liaison Operations	Moderate	Low	Low			
	C.2.8	***CENTRAL GOVERNMENT***						
	C.2.8.1	Central Fiscal Operations	Moderate	Low	Low			
	C.2.8.2	Legislative Functions	Low	Low	Low			
	C.2.8.3	Executive Functions	Low	Low	Low			
	C.2.8.4	Central Property Management	Low	Low	Low			
	C.2.8.5	Central Personnel Management	Low	Low	Low			
	C.2.8.6	Taxation Management	Moderate	Low	Low			
	C.2.8.7	Central Records and Statistics Management	Moderate	Low	Low			

"X" if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	C.2.8.8	Income Information	Moderate	Moderate	Moderate			
	C.2.8.9	Personal Identity and Authentication	Moderate	Moderate	Moderate			
	C.2.8.10	Entitlement Event Information	Moderate	Moderate	Moderate			
	C.2.8.11	Representative Payee Information	Moderate	Moderate	Moderate			
	C.2.8.12	General Information	Low	Low	Low			
Government Resource Management Information								
	C.3.1	***ADMINISTRATIVE MANAGEMENT***						
	C.3.1.1	Facilities, Fleet, and Equipment Management	Low	Low	Low			
	C.3.1.2	Help Desk Services	Low	Low	Low			
	C.3.1.3	Security Management	Moderate	Moderate	Low			
	C.3.1.4	Travel	Low	Low	Low			
	C.3.1.5	Workplace Policy Development and Management	Low	Low	Low			
	C.3.2	***FINANCIAL MANAGEMENT***						
	C.3.2.1	Asset and Liability Management	Low	Low	Low			
	C.3.2.2	Reporting and Information	Low	Moderate	Low			
	C.3.2.3	Funds Control	Moderate	Moderate	Low			
	C.3.2.4	Accounting	Low	Moderate	Low			
	C.3.2.5	Payments	Low	Moderate	Low			
	C.3.2.6	Collections and Receivables	Low	Moderate	Low			

“X” if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	C.3.2.7	Cost Accounting/Performance Measurement	Low	Moderate	Low			
	C.3.3	***HUMAN RESOURCE MANAGEMENT***						
	C.3.3.1	HR Strategy	Low	Low	Low			
	C.3.3.2	Staff Acquisition	Low	Low	Low			
	C.3.3.3	Organization and Position Management	Low	Low	Low			
	C.3.3.4	Compensation Management	Low	Low	Low			
	C.3.3.5	Benefits Management	Low	Low	Low			
	C.3.3.6	Employee Performance Management	Low	Low	Low			
	C.3.3.7	Employee Relations	Low	Low	Low			
	C.3.3.8	Labor Relations	Low	Low	Low			
	C.3.3.9	Separation Management	Low	Low	Low			
	C.3.3.10	Human Resources Development	Low	Low	Low			
	C.3.4	***SUPPLY CHAIN MANAGEMENT***						
	C.3.4.1	Goods Acquisition	Low	Low	Low			
	C.3.4.2	Inventory Control	Low	Low	Low			
	C.3.4.3	Logistics Management	Low	Low	Low			
	C.3.4.4	Services Acquisition	Low	Low	Low			
	C.3.5	***INFORMATION & TECHNOLOGY MANAGEMENT***						
	C.3.5.1	System Development	Low	Moderate	Low			

“X” if type applies	SP 800-60 section reference	NIST 800-60 Categorization of Information	Level Recommended by NIST SP 800-60			<SYSTEM NAME or ID> Assessment of Impact		
		Information Types this System / Application:	Confidentiality	Integrity	Availability	Confidentiality - (H/M/L)	Integrity - (H/M/L)	Availability - (H/M/L)
	C.3.5.2	Lifecycle / Change Management	Low	Moderate	Low			
	C.3.5.3	System Maintenance	Low	Moderate	Low			
	C.3.5.4	IT Infrastructure Maintenance*	Low*	Low	Low			
	C.3.5.5	Information System Security	Low	Moderate	Low			
	C.3.5.6	Record Retention	Low	Low	Low			
	C.3.5.7	Information Management*	Low*	Moderate	Low			
	C.3.5.8	System and Network Monitoring	Moderate	Moderate	Low			
	C.3.5.9	Information Sharing	N/A	N/A	N/A			

* The confidentiality impact assigned to the IT Infrastructure Maintenance (C.3.5.4) and Information Management (C.3.5.7) Information Types may necessitate the highest confidentiality impact of the information types processed by the system

Appendix B - NESDIS FIPS 199 AO Signature Page Template

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

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

FROM: <AO Name>
Authorizing Official /or/ co-Authorizing Official
<Office>

<co-AO Name (for Moderate systems only)>
co-Authorizing Official and
Title

SUBJECT: Approval of the Federal Information Processing Standard 199
Security Categorization for <system long name>

I/We have reviewed the Federal Information Processing Standard (FIPS) 199 Security Categorization, version x.x dated Month day, 20xx, for <system long name>, System ID NOAA50xx (attached). I/We approve the designation of the system's overall security categorization as <High, Moderate, or Low>. This categorization is based on categorization of the individual security objectives as Confidentiality—<High, Moderate, or Low>, Integrity—<High, Moderate, or Low>, and Availability—<High, Moderate, or Low>.

You are directed to submit for my/our approval, within 30 days of the date of this approval, the security controls baseline for the system prepared in accordance with FIPS 200. The FIPS 200 determination must reflect the cost-effective control requirements that adequately protect the system to this level of security categorization.

You are required to review the FIPS 199, and update it as necessary, at least annually as part of the System Security Plan and risk assessment annual review, as well as whenever a significant event occurs, such as adding a new information type to, or removing an information type from, the system during the ongoing system configuration management process. Also, you must update the FIPS 199 Record of Changes for each review and update performed. All FIPS 199 changes require my/our written approval, and at a minimum, you must re-submit it for my/our written approval at least every 3 years as part of the system assessment and authorization process, even if there has been no change to the FIPS 199.

You must retain this approval memo as part of the system's security authorization package documentation.

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

FOR OFFICIAL USE ONLY

Approval Page

Document Number: NQP-3403, Revision 3.1	
Document Title Block: **Federal Information Processing Standards Publication 199 Security Categorization Policy and Procedures**	
Process Owner: NESDIS Chief Information Office	Document Release Date: September 1,2012

Prepared by:

Erica Boyd

Erica Boyd
Ambit- Associate Consultant
NESDIS Chief Information Office

3/25/15
Date:

Approved by:

Irene Parker

Irene Parker
Assistant Chief Information Officer - Satellites

3/25/15
Date:

FOR OFFICIAL USE ONLY

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
3.1	**March 25, 2015**	**----**	**ALL**	**Baseline NQP-3403**