NATIONAL WEATHER SERVICE INSTRUCTION 60-702

JUNE 23, 2023

Information Technology

Information Technology Security Policy, NWSPD 60-7

SECURITY AND PRIVACY CONTROLS

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: W/ACIO (O. Omotoso) **Certified by:** W/ACIO (B. Koonge)

Type of Issuance: Routine

SUMMARY OF REVISIONS: This directive supersedes NWS Instruction 60-702, *Security and Privacy Controls*, dated May 30, 2019. Changes include:

a. Quadrennial review and editorial changes to ensure policies are clear and concise, and improve readability.

b. Fixed broken hyperlinks (URLs), and replaced them throughout the document.

c. Updated reference information on continuous monitoring (Appendix A & B); list of acronyms (Appendix C); and expanded summary of revisions (Appendix D).

KOONGE.BECKIE.A.1408306880 Digitally signed by KOONGE.BECKIE.A.1408306880 Date: 2023.06.09 13:03:22 -04'00'

Beckie Koonge
Assistant Chief Information Officer (ACIO) for Weather

Date

Security and Privacy Controls

Table of Contents

1. Introduction

National Weather Service (NWS) Information Technology (IT) systems provide data and information across the nation and the world. Security and privacy controls are necessary to assure that NWS products and services are readily available, accurate, timely, and protected from threats that could disrupt, damage, alter, or destroy the contents of NWS systems. Assuring that IT systems are maintained commensurate with these requirements is a complex task.

The NWS Security and Privacy Controls policy is established to ensure that all NWS FISMA systems adhere to the following security objectives:

Confidentiality – Confidentiality ensures that NWS information are protected from unauthorized disclosure.

Integrity – Integrity ensures that NWS information is protected from unauthorized, unanticipated, or unintentional modification.

Availability – Availability ensures that NWS information has timely and reliable access to (and consumption of) information.

2. Purpose

The purpose of this policy is to define requirements necessary for all NWS systems to meet the fundamental security objectives and ensure adequate security posture. This policy complies with the implementation of the Federal Information Security Modernization Act (FISMA) of 2014 (as amended) and other department requirements.

To assist all Federal Departments and agencies with that process, the National Institute of Standards and Technology (NIST) is instructed to prepare guidance and issue Federal Information Processing Standards (FIPS) that collectively set the statutory and regulatory standards to be implemented by Federal officials responsible for assuring the uninterrupted operation and safe interconnection with and among Federal IT systems.

3. Risk Management Framework

Federal agencies are required to adopt the NIST Risk Management Framework (RMF) as part of their FISMA implementation. This framework provides a structured and repeatable process integrating security and risk management activity into the system development life cycle (SDLC). The RMF's six steps are:

Step 1: Categorize
Step 2: Select
Step 3: Implement
Step 4: Assess
Step 5: Authorize
Step 6: Monitor

Figure 1 Security Life Cycle

Source: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

4. System Security Categorization Considerations

FIPS 199 summarizes the standards for security categorization of Federal information systems. FIPS 199 is extensively supplemented by detailed examples in NIST Special Publication (SP) 800-60 Revision 1 Volume II, "Guide for Mapping Types of Information and Information Systems to Security Categories." The standards set by these two documents suggest that NWS operations systems will most often be captured in examples provided by NIST SP 800-60 Vol. II Annex D, Section D.4., "Disaster Management." The standards and definitions of these two documents also suggest that the security categorization of research and non-operational systems will often be best captured in other NIST SP 800-60 Vol. II appendixes and sections as demonstrated in examples below.

Operations example: NIST SP 800-60 Revision 1 Vol. II Section D.4.1., "Disaster Monitoring and Prediction Information Type," may apply to NWS operations systems that contribute to hydro meteorological and/or space weather forecasts, watches, and/or warnings. Section D.4.1 includes IT operations undertaken to "predict when and where a disaster may take place and communicate that information to affected parties." Depending on the circumstances, the FIPS 199 Confidentiality level of such information could be "Low," "Moderate," or "High," while the recommended Integrity and Availability impacts are both "High." Sections D.4.2 to D.4.4 may also apply to NWS operational systems, with FIPS 199 Integrity and Availability categorization often at the "High" levels.

Non-Operations example: The FIPS 199 security categorization of NWS non-operations systems could potentially fall into a number of examples in NIST SP 800-60 Vol. II Appendix C, "Management and Support Information and Information Systems Impact Levels," or in Appendix E, "Legislative and Executive Sources Establishing Sensitivity/Criticality." Research information systems are defined in SP 800-60 Revision 1 Vol. II Appendix D, "Impact Determination for Mission-based Information and Information Services."

Considerations for System Security Categorization shall be documented and updated annually using the NWS FIPS 199 document template available from the following location: https://sites.google.com/a/noaa.gov/acio/it-security-services-branch-itssb/nws-it-security-information-portal/nws-rmf-templates

5. Information System Owner (System Owner) Responsibilities

FISMA and NIST guidance establish the statutory level of responsibility and accountability that NWS IT System Owners document in addressing Department of Commerce (DOC), NIST, National Oceanic and Atmospheric Administration (NOAA) and NWS security control requirements. However, System Owners have the authority to go beyond the minimum requirements when necessary to establish adequate security controls based on reasonable grounds that a system has been compromised by unauthorized actions and/or threat agents against an operational system.

6. Control Precedence

This NWSI describes and clarifies NWS Control Baseline Standards and Enhancements that supplement the applicable DOC and NOAA policies already in place. Minimum IT security controls should be implemented on all NWS IT systems as stated in NIST SP 800-53, Revision 5, and applicable DOC, NOAA, and NWS policies.

If a conflict exists among DOC, NOAA and NWS Control Baseline Standards, the DOC standard takes precedence unless the NOAA or NWS Control Baseline Standard sets a more stringent requirement. Where no DOC, NOAA, or NWS enhancement is specified, the NIST SP 800-53 Revision 5 standard applies.

7. Expected Control Baseline Standards

Control Baseline Standards derive from a combination of FIPS 199 System Categorization (as further defined in NIST SP 800-60 Revision 1) and NIST SP 800-53 Revision 5 and its appendices. DOC further defines the implementation expectations of these Control Baseline Standards in its Information Technology Security Baseline Policy (ITSBP), dated June 2019. This can be located at: https://connection.commerce.gov/policy/20220928/enterprise-cybersecurity-policy-program

In addition, NOAA's tailored Control Baseline Standards are documented in the NOAA Information Technology Security Manual (ITSM) version 7.2, dated March 2022 located at: https://sites.google.com/a/noaa.gov/ocio-itso/home/itsm-itsbp

NWS control baseline enhancements listings begin with section 9 below. Each contains clarifying language that supplements DOC and NOAA expectations. If the System Owner believes that local conditions require a different Control Baseline Standard, be it higher or lower, they should forward that recommendation to the NWS Chief Information Security Officer (CISO) along with a strong business justification, the means by which their proposed control(s) will be monitored, and the period for which the documentation of the effectiveness of the control(s) will be retained.

8. Security Documentation

To satisfy requirements of the Office of the Inspector General (OIG), documentation of the status of IT security controls will be maintained from previous Assessment and Authorization (A&A) periods. Because that is a standing DOC requirement, it will not be reiterated in comments below regarding NWS control enhancements. All artifacts, excluding Security Assessment Testing evidence, should be uploaded into Cyber Security Assessment and Management (CSAM) or equivalent Governance, Risk Management, Compliance (GRC) tool on the schedule set out by NOAA for Continuous Monitoring or more often if separately advised.

In other instances cited below, NWS control enhancements are being specified regarding retention of selected documentation of the effectiveness of certain controls. Through liaison with the United States Intelligence Community, NWS gains access to classified national security information regarding advanced and persistent threats and exploits being utilized to attack U.S. Government information systems. Having the ability to look back over time for selected controls is extremely valuable in determining whether newly-understood exploits have successfully been utilized in the past to circumvent NWS system security controls. Having such records also helps understand why control failures took place, and are extremely valuable for the improvement of the collective NWS control posture.

9. Access Control (AC)

Table 1 Access Control

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1)(2)(3)(4)	AC-2 (1)(2)(3)(4)(5) (11)(12)(13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1)(2)(5) (9)(10)	AC-6 (1)(2)(3) (5)(9)(10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1)(2)(3)(4)	AC-17 (1)(2)(3)(4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1)(4)(5)

AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1)(2)	AC-20 (1)(2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

9.1 AC-7 Unsuccessful Login Attempts

Privileged accounts shall remain locked until System Administrator/Help Desk personnel unlocks the account.

9.2 AC-10 Concurrent Session Control

No more than one (1) active session is permitted for each individual user account. If deviation from policy is dictated by a mission critical need, the information system owner shall notify the NWS CISO, and the acceptance of risk will be documented in the system's FIPS 200 Security Control Baseline Tailoring document, and in the System Security Plan.

9.3 AC-11 Session Lock

NOAA requires that information systems prevent further access to the system by initiating a session lock after fifteen (15) minutes of inactivity. The session lock shall remain in effect until the user re-establishes access using appropriate identification and authentication procedures.

However, since many NWS systems supporting operations require immediate access to time-sensitive resources related to the protection to life and property, the AC-11 control can place lives and property at risk. Fortunately, NIST SP 800-53 allows such controls to be tailored. As a result, NWS delegates to the Authorizing Officials (AOs) the authority to accept the risk caused by the elimination of the 15-minute AC-11 Session Lock Control for specifically identified, time-sensitive IT systems if compensating controls achieve essentially the same outcome. At a minimum, compensating controls should include:

1. Physical security measures that control access to the space in which access can be gained to such time-sensitive IT systems;
2. Personnel security controls that assure all persons who access controlled space have undergone appropriate suitability background checks; AND
3. Visitors or guests in such space who do not meet personnel security control requirements are under the continuous personal supervision of NWS personnel authorized to be in the controlled workspace.

Applicable control standards for the three examples given above are contained in the Access Control, Physical and Environmental Protection, and Personnel Security Control Families in NIST SP 800-53 Revision 5 and its Appendices.

9.4 AC-22 Publicly Accessible Content

NWS requires System Owners to document approvals for those individuals authorized to post information on publicly accessible information systems.

10. Awareness and Training (AT)

Table 2 Awareness and Training Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---

10.1 AT-3 Role-Based Security Training

NWS ACIO provides role-based security training material and tracks the completion for Authorizing Officials and System Owners. For Information System Security Officers (ISSO), NWS ACIO only tracks the completion of security certifications as listed in the DOC Information Technology Security Baseline Policy (ITSBP) v1.0, Annex C-1, Appendix A. NWS System Owners must ensure that other security roles and personnel are adequately trained and tracked.

11. Audit and Accountability (AU)

Table 3 Audit and Accountability Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1)(2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1)(2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1)(3)	AU-6 (1)(3)(5)(6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2)(3)(4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1)(3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected

11.1 AU-6 Audit Review, Analysis, and Reporting

NWS requires that monitoring and analysis of audit logs be conducted at least weekly. Information System Owners shall document the frequency for analysis, the dates performed, and results. Audit logs are to be securely stored, retained, and accessible only to authorized personnel.

11.2 AU-7 Audit Reduction and Report Generation

Information System Owners shall maintain descriptive information regarding the tool(s) they select for this control, and the results of automated log reduction demonstrating variance from established norms.

11.3 AU-8 Time Stamps

To maintain consistency throughout the enterprise, NWS requires the use of Coordinated Universal Time (UTC) timestamps.

11.4 AU-10 Non-Repudiation

Common Access Card Public Key Infrastructure (PKI) capabilities shall be utilized for generating digital signatures. Information System Owners shall document their decisions regarding the use of Non-Repudiation capabilities.

12. Security Assessment and Authorization (CA)

Table 4 Security Assessment and Authorization Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1)(2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	**Withdrawn**	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9

12.1 CA-2 Security Assessments

Every year the Chief Information Security Officer (CISO) shall develop an assessment schedule for every system in NWS. This schedule includes dates for on-site assessments, document deliverables, and ATO schedules. The IT Security Services Branch (ITSSB) will serve as the independent 3rd party assessors for all systems categorized as high or moderate. Independent security control assessors will develop a Security Assessment Plan (SAP) for each system. The SAP shall describe the scope of the assessment including:

- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and

- Assessment environment, assessment team, and assessment roles and responsibilities;

All NWS FISMA systems shall assess the security controls in the information system and its environment of operation annually in accordance with DOC requirements. Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Security control assessors develop a Security Control Assessment (SCA) and a Security Assessment Report (SAR) for each system documenting the results of the assessment and distribute these documents to the AO, ISO and ISSO.

12.2 CA-2(1) Independent Assessors

The Assistant Chief Information Officer (ACIO) for Weather employs assessment and compliance teams within the NWS ACIO office to conduct security control assessments.

12.3 CA-2(2) Specialized Assessments

NWS includes as part of security control assessments, announced, in-depth monitoring; vulnerability scanning at least annually. Penetration testing is conducted when applicable.

12.4 CA-3 System Interconnections

All NWS operational units shall document all external system interconnections using the NOAA Interconnection Security Agreement (ISA) templates (or equivalent). All system interconnections must be reviewed annually (or as otherwise stipulated in the ISA) or when there is a significant change. ISA Agreements between two NOAA systems are not required, but highly recommended especially if there are differences in the impact level of the two systems. Additionally, interconnections between two NOAA systems shall be documented in CSAM or equivalent GRC tool. Information system owners are required to maintain all valid and signed ISAs in CSAM or equivalent GRC tool.

12.5 CA-3(5) Restrictions on External System Connections

All NWS FISMA systems shall employ a deny-all, permit-by-exception policy for allowing any connections to external information systems. Information system owners are required to document this policy in all valid and signed ISAs in CSAM or equivalent GRC tool.

12.6 CA-5 Plan of Actions and Milestones

All NWS FISMA systems shall follow the NOAA POA&M Management process located at: https://sites.google.com/a/noaa.gov/ocio-itso/home/procedures-processes

12.7 CA-6 Security Authorization

All NWS FISMA systems shall renew their security authorization at least every 365 days with the AOs ensuring all of the security controls are assessed at least once every three years, and/or when triggered by a significant event.

12.8 CA-7 Continuous Monitoring

All NWS AOs and ISOs will comply with the DOC Continuous Monitoring requirements, with the NOAA

ITSM, and with all security controls and/or enhancements addressing continuous monitoring. NOAA common controls, as defined by the NOAA ITSM (as amended), will not be assessed by the Assessment Team as part of the annual assessment except under special circumstances.

12.9 CA-8 Penetration Testing

Annual penetration testing for all NWS High-impact systems is required by NWS ACIO. Moderate and low systems may request penetration testing from the NWS ACIO if resources are available. In addition, NWS ACIO may initiate – with System Owner and system personnel – penetration testing on any NWS system when necessary.

13. Configuration Management (CM)

Table 5 Configuration Management Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1)(3)(7)	CM-2 (1)(2)(3)(7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1)(2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1)(2)(3)
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1)(2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1)(2)(5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1)(3)(5)	CM-8 (1)(2)(3)(4)(5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11

13.1 CM-3 Configuration Change Control

NWS FISMA systems shall retain records of configuration changes throughout the lifecycle of the information system.

13.2 CM-5 Access Restrictions for Change

Information system owners shall document the physical and logical access restrictions utilized in their system(s) for review to determine if any unauthorized changes have occurred.

13.3 CM-8 Information System Component Inventory

Information system owners shall maintain a current Information System Component Inventory that accurately reflects the state of the system, and that is in compliance with DOC ITSBP Annex B-5: Configuration Management (CM) ITSBP Requirements.

14. Contingency Planning (CP)

Table 6 Contingency Planning Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1)(3)(8)	CP-2 (1)(2)(3)(4)(5)(8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1)(2)
CP-5	**Withdrawn**	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1)(3)	CP-6 (1)(2)(3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1)(2)(3)	CP-7 (1)(2)(3)(4)
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1)(2)	CP-8 (1)(2)(3)(4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1)(2)(3)(5)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)	CP-10 (2)(4)
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected

14.1 CP-1 Contingency Planning Policy and Procedures

Within NWS, additional requirements are set out in NWSD 10-22 (as amended) and NWSI 10-2201 (as amended) regarding backup operations for failover between NWS components. These are located at: https://www.nws.noaa.gov/directives/010/010.php

14.2 CP-2 Contingency Plan

At a minimum, all NWS FISMA systems must distribute their contingency plans to all personnel responsible for execution of the plan. The review and update schedule set out in CP-1 above should be maintained.

14.3 CP-3 Contingency Training

NWS requires that such training be conducted at a minimum annually, and that after-action reports be documented.

14.4 CP-4 Contingency Plan Testing

NWS requires that such testing and exercises are conducted at a minimum annually, and that after-action reports be documented.

14.5 CP-7 Alternate Processing Sites

At a minimum, each NWS system shall determine the recovery time objectives (maximum allowable downtime) based on the business processes the system supports, and document them in the Business Impact Analysis (BIA) document. Information system owners will document the results of the exercises and the

extent to which recovery time objectives were achieved.

14.6 CP-8 Telecommunications Services

At a minimum, each NWS system shall determine the recovery time objectives (maximum tolerable downtime) based on the business processes the system supports, and document them in the BIA report. Information system owners shall document the results of the exercises and the extent to which recovery time objectives were achieved.

To achieve communications recovery time objectives, information system owners may wish to consider "last mile" alternative routing (in other words, multiple communication pathways such as terrestrial fiber optic cable supplemented by Very Small Aperture Terminal (VSAT) and diverse routing (in other words, using such techniques as routing traffic through split cable facilities or duplicating cable facilities).

The NWS OCIO and NWS Homeland Security Activities Office are available for consultation regarding communications options, to include OneNWSNet.

14.7 CP-9 Information System Backup

NWS supplements this control by requiring at least weekly full backup and daily incremental backup. Information system owners shall document how this control is implemented, and review and update the process at least annually (or more often if significant technology changes have taken place with the system).

15. Identification and Authentication (IA)

Table 7 Identification and Authentication Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1)(2)(3)(8) (11)(12)	IA-2 (1)(2)(3)(4)(8)(9) (11)(12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1)(11)	IA-5 (1)(2)(3)(11)	IA-5 (1)(2)(3)(11)
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1)(2)(3)(4)	IA-8 (1)(2)(3)(4)	IA-8 (1)(2)(3)(4)
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected

15.1 IA-2 Identification and Authentication (Organizational Users)

All NWS FISMA systems shall comply with requirements in the Homeland Security Presidential Directive

(HSPD) 12; however, if an information system cannot meet this requirement, the information system owner will document any exceptions (i.e., service accounts, network devices, social media accounts, etc.) in the FIPS 200, and seek AO approval.

16. Incident Response (IR)

Table 8 Incident Response Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Incident Response					
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1)(2)
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1)(4)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	P2	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	P0	Not Selected	Not Selected	Not Selected
IR-10	Integrated Information Security Analysis Team	P0	Not Selected	Not Selected	Not Selected

16.1 IR-1 Incident Response Policy and Procedures

For all security incidents, NWS FISMA systems shall provide an initial IT security incident report in accordance with NOAA guidance at https://sites.google.com/noaa.gov/noaacybersecuritycenter/report-an-incident. All electronic communication regarding incidents will be encrypted using the NOAA Incident Response Reporting Application (NIRRA) and encrypted electronic mail. NOAA does not authorize the use of electronic communications using standard "clear text" electronic mail. The NOAA Incident Response Plan can be located on the NOAA Cyber Security Division Procedures and Processes site.

17. Maintenance (MA)

Table 9 Maintenance Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Maintenance					
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	P2	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	P3	Not Selected	MA-3 (1)(2)	MA-3 (1)(2)(3)
MA-4	Nonlocal Maintenance	P2	MA-4	MA-4 (2)	MA-4 (2)(3)
MA-5	Maintenance Personnel	P2	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	P2	Not Selected	MA-6	MA-6

17.1 MA-5 Maintenance Personnel

In the event external personnel are utilized for system maintenance, information system owners must document Service Level Agreements and PS-6 Access Agreements. These should be maintained for at least three years beyond the completion/termination of the external services contract.

18. Media Protection (MP)

Table 10 Media Protection Controls CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Media Protection					
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	MP-1
MP-2	Media Access	P1	MP-2	MP-2	MP-2
MP-3	Media Marking	P2	Not Selected	MP-3	MP-3
MP-4	Media Storage	P1	Not Selected	MP-4	MP-4
MP-5	Media Transport	P1	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	P1	MP-6	MP-6	MP-6 (1)(2)(3)
MP-7	Media Use	P1	MP-7	MP-7 (1)	MP-7 (1)
MP-8	Media Downgrading	P0	Not Selected	Not Selected	Not Selected

18.1 MP-3 Media Marking

Information system owners shall identify media types or hardware components in use in their environments, and document exempt media (if any) that will remain in system-defined controlled environments.

18.2 MP-4 Media Storage

NWS FISMA systems shall physically control and securely store information not for public consumption on all diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, digital video disks, paper and microfilm, and mobile devices with information storage containing backed up data, archives, and other information as defined in MP-3 Media Marking and within containers or facilities which have restricted access to authorized personnel only.

18.3 MP-5 Media Transport

Information system owners are responsible for establishing local controls over the transportation of all media under their control that will be protected in some manner, i.e., containing personally identifiable information (PII), and such controls will conform with DOC requirements for full disk encryption. These controls shall be documented and reviewed annually.

18.4 MP-6 Media Sanitization

Information system owners and the IT staff supporting the FISMA system shall certify that media sanitization has taken place prior to disposal of any media. The date and nature of the sanitization procedures shall be recorded.

19. Physical and Environmental Protection (PE)

Table 11 Physical and Environmental Protection Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2	PE-2	PE-2
PE-3	Physical Access Control	P1	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	P2	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1)(4)
PE-7	**Withdrawn**	---	---	---	---
PE-8	Visitor Access Records	P3	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	P1	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	P1	Not Selected	PE-10	PE-10
PE-11	Emergency Power	P1	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	P1	PE-12	PE-12	PE-12
PE-13	Fire Protection	P1	PE-13	PE-13 (3)	PE-13 (1)(2) (3)
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	P1	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	P2	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	Not Selected	Not Selected	Not Selected

For the entire PE control family, the information system owner is responsible for selecting all applicable controls within the PE family and documenting them, at a minimum, in the SSP and FIPS 200 Security Control Baseline Tailoring document even if the information system is not responsible for implementing them.

20. Planning (PL)

Table 12 Planning Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Planning					
PL-1	Security Planning Policy and Procedures	P1	PL-1	PL-1	PL-1
PL-2	System Security Plan	P1	PL-2	PL-2 (3)	PL-2 (3)
PL-3	**Withdrawn**	---	---	---	---
PL-4	Rules of Behavior	P2	PL-4	PL-4 (1)	PL-4 (1)
PL-5	**Withdrawn**	---	---	---	---
PL-6	**Withdrawn**	---	---	---	---
PL-7	Security Concept of Operations	P0	Not Selected	Not Selected	Not Selected
PL-8	Information Security Architecture	P1	Not Selected	PL-8	PL-8
PL-9	Central Management	P0	Not Selected	Not Selected	Not Selected

20.1 PL-4 Rules of Behavior

Although this is a NOAA common control, NWS information system owners may develop Rules of Behavior as deemed necessary for their environment. A copy of the system-specific rules, if they exist, shall be provided to the NWS ITSOs for review. The NOAA Rules of Behavior can be located here.

21. Personnel Security (PS)

Table 13 Personnel Security Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Personnel Security					
PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	P1	PS-2	PS-2	PS-2
PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
PS-4	Personnel Termination	P1	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	P2	PS-5	PS-5	PS-5
PS-6	Access Agreements	P3	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	P1	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	P3	PS-8	PS-8	PS-8

21.1 PS-4 Personnel Termination

NWS FISMA systems shall revoke all information system access and all Government Furnished Equipment (GFE) or related property (i.e., CAC, Alt-Token) within 24 hours of notification of termination/transfer, or as determined by the information system owner.

21.2 PS-5 Personnel Transfer

NWS FISMA systems must review and adjust information system access within 24 hours of transfer or as

determined by the information system owner depending on the nature of the transfer (e.g., within NWS or NOAA).

22. Risk Assessment (RA)

Table 14 Risk Assessment Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	**Withdrawn**	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1)(2)(5)	RA-5 (1)(2)(4)(5)
RA-6	Technical Surveillance Countermeasures Survey	P0	Not Selected	Not Selected	Not Selected

22.1 RA-5 Vulnerability Scanning

All NWS FISMA systems shall follow the NWS Instruction 60-703, Vulnerability Management, for direction and guidance.

23. System and Services Acquisition (SA)

Table 15 System and Services Acquisition Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
System and Services Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	P1	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	P1	SA-3	SA-3	SA-3
SA-4	Acquisition Process	P1	SA-4 (10)	SA-4 (1)(2)(9)(10)	SA-4 (1)(2)(9)(10)
SA-5	Information System Documentation	P2	SA-5	SA-5	SA-5
SA-6	**Withdrawn**	---	---	---	---
SA-7	**Withdrawn**	---	---	---	---
SA-8	Security Engineering Principles	P1	Not Selected	SA-8	SA-8
SA-9	External Information System Services	P1	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	Not Selected

SA-14	Criticality Analysis	P0	Not Selected	Not Selected	Not Selected
SA-15	Development Process, Standards, and Tools	P2	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	P2	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	P1	Not Selected	Not Selected	SA-17
SA-18	Tamper Resistance and Detection	P0	Not Selected	Not Selected	Not Selected
SA-19	Component Authenticity	P0	Not Selected	Not Selected	Not Selected
SA-20	Customized Development of Critical Components	P0	Not Selected	Not Selected	Not Selected
SA-21	Developer Screening	P0	Not Selected	Not Selected	Not Selected
SA-22	Unsupported System Components	P0	Not Selected	Not Selected	Not Selected

23.1 SA-9 External Information System Services

NWS requires that external information system service providers comply with FISMA and NIST standards, and be subject to the same rules as Federal systems for the Assessment and Authorization process. Documentation of both the Service Level Agreements (SLAs) and the required compliance with FISMA should be maintained at least three years beyond the completion/termination of the external services contract in CSAM or equivalent GRC tool.

23.2 SA-11 Developer Security Training

NWS requires information system owners to include the NIST requirements in all developer contracts as part of the Service Level Agreement, and maintain documentation of developer compliance for at least three years beyond the completion/termination of the developer contract.

23.3 SA-12 Supply Chain Protection

NWS requires that supply chain protection be maintained through procurement of goods solely through an approved Federal Acquisition Contract. Information system owners shall maintain records beyond the next Assessment and Authorization cycle if the warranty period still applies. To proactively address this security control requirement, information system owners need to articulate their supply chain requirement as part of the process of bringing new systems on line.

24. System and Communications Protection (SC)

Table 16 System and Communications Protection Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected

SC-7	Boundary Protection	P1	SC-7	SC-7 (3)(4)(5)(7)	SC-7 (3)(4)(5)(7)(8)(18)(21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	**Withdrawn**	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Concealment and Misdirection	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P0	Not Selected	Not Selected	Not Selected
SC-33	**Withdrawn**	---	---	---	---
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
SC-35	Honeyclients	P0	Not Selected	Not Selected	Not Selected
SC-36	Distributed Processing and Storage	P0	Not Selected	Not Selected	Not Selected
SC-37	Out-of-Band Channels	P0	Not Selected	Not Selected	Not Selected
SC-38	Operations Security	P0	Not Selected	Not Selected	Not Selected
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39
SC-40	Wireless Link Protection	P0	Not Selected	Not Selected	Not Selected
SC-41	Port and I/O Device Access	P0	Not Selected	Not Selected	Not Selected
SC-42	Sensor Capability and Data	P0	Not Selected	Not Selected	Not Selected
SC-43	Usage Restrictions	P0	Not Selected	Not Selected	Not Selected
SC-44	Detonation Chambers	P0	Not Selected	Not Selected	Not Selected

24.1 SC-8 Transmission Confidentiality and Integrity

Information system owners shall utilize a secure message digest (hash) application to assure that any alteration of messages during transmission can be detected. NIST recommends the use of the Secure Hash Algorithm-2 (SHA-2) family of hash functions (SHA-224, SHA-256, SHA-384, and SHA-512). MD-5 has been compromised and is no longer considered a reliable integrity checker. FIPS 180-4 of August 2015 provides additional information.

24.2 SC-13 Cryptographic Protection

Information system owners shall determine if and when cryptography is necessary, and document cryptographic protection, at a minimum, in the system security plan.

24.3 SC-17 Public Key Infrastructure Certificates

Commercial encryption certificates, that is, certificates signed by commercial Certificate Authorities (CAs), shall be installed on Internet-facing systems accepting connections requiring (and capable of) encryption. For internal-facing systems accepting internal connections requiring (and capable of) encryption, DoD certificates shall be installed. PKI certificates issued by NOAA8850 - EMES are also acceptable on NWS FISMA systems subscribing to NOAA8850 Certificate Services for internal connections requiring (and capable of) encryption. PKI certificates issued by system-maintained CAs are acceptable within the system boundary for internal system connections provided system-maintained CA servers meet minimum requirements for key sizes, encryption algorithm strength, etc. Refer to NWS Guide: Public Key Infrastructure and Self-Signed Certificate; and NOAA ICAM Certificate Request site for additional guidance.

24.4 SC-18 Mobile Code

Use of mobile code technology (e.g., java, JavaScript, ActiveX, etc.) shall be based on the system's needs. Decisions regarding the use of mobile code should be assessed based on the potential for the code to cause harm to NWS systems if used maliciously.

24.5 SC-20 Secure Name/Address Resolution Service (Authoritative Source)

NWS FISMA systems can fully inherit this control from NOAA0201 Web Operations Center (WOC). Information system owners are required to document this in CSAM or equivalent GRC tool.

24.6 SC-22 Architecture and Provisioning for Name / Address Resolution Service

NWS FISMA systems can fully inherit this control from NOAA0201 Web Operations Center (WOC). Information system owners are required to document this in CSAM or equivalent GRC tool.

24.7 SC-23 Session Authenticity

Information system owners are required to use PKI certificates and one of the SHA-2 family of message digest software (discussed in SC-8) for positive session authentication and assurance that transmitted information has not been altered.

24.8 SC-24 Fail in Known State

NWS ACIO is available for collaboration with any information system owner requiring assistance for implementation of this control. A potential compensating control may be to maintain a mirror or shadow system as part of the Disaster Recovery (DR)/Continuity of Operations (COOP) plan for the system so that, upon failure of the primary system, the mirror/shadow system can assume the primary role while the failed system is repaired or replaced.

25. System and Information Integrity (SI)

Table 17 System and Information Integrity Controls

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1)(2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1)(2)	SI-3 (1)(2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2)(4)(5)	SI-4 (2)(4)(5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1)(7)	SI-7 (1)(2)(5) (7)(14)
SI-8	Spam Protection	P2	Not Selected	SI-8 (1)(2)	SI-8 (1)(2)
SI-9	**Withdrawn**	---	---	---	---
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
SI-14	Non-Persistence	P0	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	P0	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	P1	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	P0	Not Selected	Not Selected	Not Selected

25.1 SI-4 Information System Monitoring

The controls implemented by information system owners shall be tested to ensure the controls are properly installed, operating as intended, and providing the desired protections.

Appendix A: NWS Assessment Control Families Distribution Years 1, 2, and 3

Year 1	Year 2	Year 3
All Privacy Controls (AP, AR, DI, DM, IP, SE, TR, UL)		
AC – Access Control	AT – Awareness and Training	AU – Audit and Accountability
IA – Identification and Authentication	CA – Security Assessment and Authorization	SA – System and Services Acquisition
MA – Maintenance	CM – Configuration Management	SC – System and Communications Protection
MP – Media Protection	CP – Contingency Planning	SI – System and Information Integrity
PS – Personnel Security	IR – Incident Response	
	PE – Physical and Environmental Protection	
	PL – Planning	
	RA – Risk Assessment	

Appendix B: Annual Compliance Document Review

Control	Compliance Document	Template	Low	Moderate	High
RA-2	FIPS-199 Categorization	NWS	X	X	X
PL2(a)(7)	FIPS-200 Minimum Security Requirements and Acceptance of Risk	NWS	X	X	X
PL-2	System Security Plan	CSAM	X	X	X
PL-2(a)(2)	Authorization Boundary for the System	None	X	X	X
AC-20 CA-3 CA-9 SA-9	Interconnection Agreements (ISAs, MOA/Us, SLAs)	NOAA	X	X	X
CM-9	Configuration Management Plan (CMP)	NOAA	X	X	X
CP-2	Business Impact Analysis (BIA)	NOAA	X	(3)(8)	(3)(4)(5)(8)
CP-2	Contingency Plan (CP)	NOAA	X	X	X
CP-4	Contingency Plan Test and Results	NOAA	X	X	X
IR-8	Incident Response Plan (IRP)	NOAA	X	X	X
CA-7	Continuous Monitoring Plan	NWS	X	X	X
RA-3(b)	Risk Assessment Report (RAR)	NOAA	X	X	X
AR-2	Privacy Threshold Assessment (PTA)	NOAA	X	X	X
AR-2	Privacy Impact Assessment (PIA)	NOAA	Only if PTA warrants a PIA		
CA-2(a)	Security Assessment Plan (SAP)	NWS	X	X	X
CM-8	Information System Component Inventory	None	X	X	X
RA-5	Discovery Scan	TSC	X	X	X
RA-5	Internal Vulnerability Scan	TSC	X	X	X
RA-5(4)	External Vulnerability Scan	[redacted]			X
CA-8	Rules of Engagement for Pen Testing	NWS	*X	*X	X

*CA-8: Low and Moderate impact systems are not mandated to perform annual penetration testing, instead, they are selected at the discretion of the NWS CISO.

Appendix C: Acronyms

A&A	Assessment and Authorization
AO	Authorizing Official
AOR	Acceptance of Risk
ACIO	Assistant Chief Information Officer
ATO	Authority to Operate
BIA	Business Impact Analysis
CAC	Common Access Card
CISO	Chief Information Security Officer
CMP	Configuration Management Plan
COOP	Continuity of Operations
CSAM	Cyber Security Assessment and Management
DNSSEC	Domain Name System Security Extensions
DOC	Department of Commerce
DoD	Department of Defense
DR	Disaster Recovery
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GFE	Government Furnished Equipment
GRC	Governance Risk Management Compliance
HSPD	Homeland Security Presidential Directive
ICMP	Internet Control Message Protocol
ID	Identification
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITSM	Information Technology Security Manual
ITSSB	Information Technology Security Services Branch
ITSO	Informational Technology Security Officer
ITSBP	Information Technology Security Baseline Policy
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIRRA	NOAA Incident Response Reporting Application
NIST	National Institute of standards and Technology
NOAA	National Oceanic Atmospheric Administration
NWSI	National Weather Service Instruction
OIG	Office of Inspector General
OPPSD	Office of Planning and Programming for Service Delivery
OPR	Office of Primary Responsibility
OSIP	Operations and Service Improvement Process
PIA	Privacy Impact Assessment

PII	Personal Identifiable Information
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
RAR	Risk Assessment Report
RMF	Risk Management Framework
SAP	Security Assessment Plan
SAR	Security Assessment Report
SCA	Security Control Assessment
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SP	Special Publication
SSP	System Security Plan
UTC	Coordinated Universal Time
WOC	Web Operations Center

Appendix D: Summary of Revisions

Date	Change Description	Author (s)
December 21, 2009	NWSI 60-702, Management Controls; NWSI 60-703, Operational Controls; and NWSI 60-704, Technical Controls, and Directive 60-7, Information Technology Policy, dated August 28, 2003. This new NWSI incorporates only NWS mandates within all of the Control Families of the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3. As a result, NWSI 60-703 and NWSI 60-704 are hereby rescinded. Directives from the Department of Commerce (DOC) can be found in the Information Technology Security Program Policy (ITSPP), January 2009. Directives from the National Oceanic and Atmospheric Administration (NOAA) can be found in the Information Technology Security Manual (ITSM) 212-1302, May 15, 2008.	J. England-Gordon
December 10, 2018	Updated to NIST 800-53 Rev.4, editorial changes to ensure the policy is clear and concise. This update is the first phase of a two phase approach to keep this policy document current, increase applicability, and reduce ambiguity. This version incorporates all reasonable requests from key stakeholders (i.e., ISSOs, ISOs, etc.) from a review that took place from April 2018 to November 2018. The following controls have been incorporated in this policy document as a result of applicability and/or modifications to NIST SP 800-53, DOC ITSP, and NOAA ITSM: AT-3, CA-2, CA-2(1), CA-2 (2), CA-3, CA-3(5), CA-5, CA-8, IA-2, PL-5, PL-6 The following controls have been withdrawn from this policy document as a result of inapplicability and/ or modifications to NIST SP 800-53, DOC ITSP, and NOAA ITSM: AU-12, CA-1, CA-4, IA-1, MA-6, PE-4, PE-5, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-17, PE-18, PS-6, SA-13, SC-9, SC-14, SC-15, SC-26, SC-30, SC-32, SI-5, SI-7, SI-10, SI-11	ITSSB

April 19, 2019	Minor edits per General Counsel (use of "must," "should," "will") throughout the document.	ITSSB
June 1, 2023	- Minor edits throughout the document addressing grammar, broken hyperlinks (URLs), policy reference updates	ITSSB