

NATIONAL WEATHER SERVICE INSTRUCTION 60-702

December 21, 2009

Information Technology

**INFORMATION TECHNOLOGY SECURITY POLICY 60-7
MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS**

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

OPR: W/CIO (J. England-Gordon)

Certified by: W/CIO(A. Gardner)

Type of Issuance: Revised

SUMMARY OF REVISIONS: Supersedes NWS Instructions dated November 14, 2003, as follows: 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 As a result, NWSI 60-703 and NWSI 60-704 are hereby rescinded.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 (ITSP), 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.

(signed)

12/07/2009

Adrian R. Gardner

Date

Director, Office of the Chief Information Officer

INFORMATION TECHNOLOGY SECURITY POLICY 60-702

Table of Contents	Page
1. Introduction.....	5
1.1 Background.....	5
1.2 System Security Categorization Considerations.....	5
1.3 System Owner Responsibilities	6
1.4 Control Precedence.....	6
1.5 Expected Control Baseline Standards.....	7
1.6 Documentation.....	7
2. Access Control.....	8
AC-7 Unsuccessful Login Attempts.....	9
AC-10 Concurrent Session Control	9
AC-11 Session Lock.....	9
AC-14 Permitted Actions Without Identification or Authentication.....	9
AC-19 Access Control for Mobile Devices.....	9
AC-22 Publicly Accessible Content	10
3. Awareness and Training.....	10
4. Audit and Accountability.....	11
AU-5 Response to Audit Processing Failures.....	11
AU-6 Audit Review, Analysis, and Reporting.....	11
AU-7 Audit Reduction and Report Generation	12
AU-8 Time Stamps	12
AU-10 Non-Repudiation.....	12
AU-12 Audit Generation	12
5. Security Assessment and Authorization.....	12
CA-1 Security Assessment and Authorization Policies and Procedures	13
CA-4 Security Certifications	13
CA-6 Security Authorization.....	13
CA-7 Continuous Monitoring.....	13
6.0 Configuration Management.....	14
CM-3 Configuration Change Control.....	14
CM-5 Access Restrictions for Change.....	14
CM-8 Information System Component Inventory.....	14
7.0 Contingency Planning.....	15
CP-1 Contingency Planning Policy and Procedures.....	15
CP-2 Contingency Plan.....	15
CP-3 Contingency Training.....	16
CP-4 Contingency Plan Testing and Exercises.....	16
CP-7 Alternate Processing Sites	16
CP-8 Telecommunications Services.....	16
CP-9 Information System Backup.....	16
CP-10 Information System Recovery and Reconstitution.....	16
8. Identification and Authentication.....	17
IA-1 Identification and Authentication Policy and Procedures	17
IA-7 Cryptographic Module Authentication.....	17

9. Incident Response.....	18
IR-1 Incident Response Policy and Procedures.....	18
10. Maintenance.....	19
MA-1 System Maintenance Policy and Procedures.....	19
MA-3 Maintenance Tools.....	19
MA-4 Non-Local Maintenance.....	19
MA-5 Maintenance Personnel.....	19
MA-6 Timely Maintenance.....	20
11. Media Protection.....	20
MP-3 Media Marking.....	20
MP-4 Media Storage.....	20
MP-5 Media Transport.....	20
MP-6 Media Sanitization.....	21
12. Physical and Environmental Protection.....	21
PE-4 Access Control for Transmission Medium.....	22
PE-5 Access Control for Output Devices.....	22
PE-10 Emergency Shutoff.....	22
PE-11 Emergency Power.....	22
PE-12 Emergency Lighting.....	22
PE-13 Fire Protection.....	22
PE-14 Temperature and Humidity Controls.....	22
PE-15 Water Damage Protection.....	22
PE-16 Delivery and Removal.....	22
PE-17 Alternate work Site.....	22
PE-18 Location of Information System Components.....	22
13. Planning.....	23
PL-4 Rules of Behavior.....	23
PL-5 Privacy Impact Assessment.....	23
PL-6 Security-Related Activity Planning.....	23
14. Personnel Security.....	24
PS-4 Personnel Termination.....	24
PS-5 Personnel Transfer.....	24
PS-6 Access Agreements.....	24
15. Risk Assessment.....	25
RA-5 Vulnerability Scanning.....	25
16. System and Services Acquisition.....	26
SA-5 Information System Documentation.....	26
SA-9 External Information System Services.....	27
SA-11 Developer Security Testing.....	27
SA-12 Supply Chain Protection.....	27
SA-13 Trustworthiness.....	27
17. System and Communications Protection.....	28
SC-3 Security Function Isolation.....	29
SC-4 Information in Shared Resources.....	29
SC-5 Denial of Service Protection.....	30
SC-8 Transmission Integrity.....	30
SC-9 Transmission Confidentiality.....	31

SC-12 Cryptographic Key Establishment and Management31
 SC-13 Use of Cryptography31
 SC-14 Public Access Protections.....31
 SC-15 Collaborative Computing Devices.....31
 SC-17 Public Key Infrastructure Certificates31
 SC-18 Mobile Code32
 SC-20 Secure Name/Address Resolution Service (Authoritative Source)32
 SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver).....32
 SC-22 Architecture and Provisioning for Name/Address Resolution Service32
 SC-23 Session Authenticity32
 SC-24 Fail in Known State32
 SC-26 Honeypots32
 SC-28 Protection of Information at Rest33
 SC-30 Virtualization Techniques.....33
 SC-32 Information System Partitioning33
 18. System and Information Integrity34
 SI-4 Information System Monitoring34
 SI-5 Security Alerts, Advisories and Directives34
 SI-7 Software and Information Integrity35
 SI-10 Information Input Validation35
 SI-11 Error Handling35

List of Tables:

Table 1: Assessment Expectations..... 6
 Table 2: Access Controls 8
 Table 3: Awareness and Training Controls 10
 Table 4: Audit and Accountability Controls..... 11
 Table 5: Security Assessment and Authorization Controls 12
 Table 6: Configuration Management Controls 14
 Table 7: Contingency Planning Controls..... 15
 Table 8: Identification and Authentication Controls 17
 Table 9: Incident Response Controls 18
 Table 10: Maintenance Controls..... 19
 Table 11: Media Protection Controls..... 20
 Table 12: Physical and Environmental Protection Controls 21
 Table 13: Planning Controls 23
 Table 14: Personnel Security Controls 24
 Table 15: Risk Assessment Controls 25
 Table 16: System and Services Acquisition Controls..... 26
 Table 17: System and Communications Protection Controls 29
 Table 18: System and Information Integrity Controls 34

1. **Introduction.**

1.1 Background. NWS IT systems provide data and information across the nation and the world. Security 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.

To assist all Federal Departments and agencies with that process, the Federal Information Security Management Act of 2002 (FISMA) instructs the National Institute of Standards and Technology (NIST) to prepare guidance and Federal Information Processing Standards (FIPS) that collectively set the statutory and regulatory standards that must be implemented by Federal officials responsible for assuring the uninterrupted operation and safe interconnection with and among Federal IT systems.

1.2 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 the August 2008 NIST 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 operational 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.

For example, NIST SP 800-60 Revision 1 Vol. II Section D.4.1., "Disaster Monitoring and Prediction Information Type," may apply to NWS operational systems that contribute to hydrometeorological 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.

The FIPS 199 security categorization of non-operational NWS information systems potentially could 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."

1.3 System Owner Responsibilities. FISMA and its implementing FIPS and NIST guidance establish the statutory level of responsibility and accountability that NWS IT System Owners must document in addressing DOC, NIST, 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 local conditions. For example, as set out in Table 1: Assessment Expectations, NIST illustrates conditions under which higher levels of security controls are justified and necessary. These conditions would be met when there are reasonable grounds to believe that a system has been compromised by unauthorized actions and/or threat agents against an operational system.

Assessment Expectations	Information System Impact Level		
	Low	Moderate	High
Security Controls are in place with no obvious errors	X	X	X
Increased grounds for confidence that the security controls are implemented correctly and operating as intended	No	X	X
Further increased grounds for confidence that the security controls are implemented correctly and operating as intended on an ongoing basis and that there is support for continuous improvement in the effectiveness of the control	No	No	X
Grounds for a high degree of confidence that the security controls are complete, consistent, and correct (beyond the minimum recommendations of NIST Special Publication 800-53A)	For environments with specific, credible threat information indicating sophisticated, well-resourced threat agents and possible attacks against high-value targets		

Table 1: Assessment Expectations

NIST guidance also allows System Owners to use a waiver process to change the level of protection of, or even eliminate, a recommended security control when necessitated by compelling operational reasons AND when compensating controls are implemented that achieve substantially the same outcome.

1.4 Control Precedence. This NWSI describes and clarifies NWS Control Baseline Standards and Enhancements that supplement the applicable Department of Commerce (DOC) and NOAA policies already in place. Minimum IT security controls must be implemented on all NWS IT systems as articulated in NIST Special Publication (SP) 800-53, Revision 3 of August 2009, 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 3 standard applies.

1.5 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 3 and its Annexes. DOC further defines the implementation expectations of these Control Baseline Standards in its Information Technology Security Program Policy of January 2009 and related Commerce Information Technology Requirements (CITR). These are located at:

http://home.commerce.gov/CIO/ITSITnew/IT_Security_Program_Documentation.html

In addition, NOAA has set out Control Baseline Standards enhancements in the NOAA Information Technology Security Manual of 2008 set out in NAO 212-1300, located at:

<https://www.csp.noaa.gov/policies/>

Beginning with Section 2.0 below are NWS control baseline enhancements, if any, or clarifying language that supplement 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 ITSO along with 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.

1.6 Documentation. To satisfy requirements of the Office of the Inspector General, documentation of the status of IT security controls must be maintained for the current Assessment and Authorization period. 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 on the schedule set out by NOAA for Continuous Monitoring or more often if separately advised.

In other instances 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 are extremely valuable for the improvement of the collective NWS control posture.

2. Access Control.

Access Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination (Withdrawn)	N/A	N/A	N/A
AC-13	Supervision and Review—Access Control (Withdrawn)	N/A	N/A	N/A
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking (Withdrawn)	N/A	N/A	N/A
AC-16	Security Attributes	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4) (5) (7) (8)	AC-17 (1) (2) (3) (4) (5) (7) (8)
AC-18	Wireless Access	AC-18	AC-18 (1)	AC-18 (1) (2) (4) (5)
AC-19	Access Control for Mobile Devices	AC-19	AC-19 (1) (2) (3)	AC-19 (1) (2) (3)
AC-20	Use of External Information Systems	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	User-Based Collaboration and Information Sharing	Not Selected	Not Selected	Not Selected
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22

Table 2: Access Controls

AC-7 Unsuccessful Login Attempts

NWS requires that the documentation of the periodic test validation of the effectiveness of the controls that detect and record unsuccessful login attempts should be retained for the life cycle of the use of the control(s).

AC-10 Concurrent Session Control

NWS requires that no more than 1 (one) active session be allowed for a single user at a time for an account. If a System Owner has a reason why a single user should be allowed to have more than one active session at the same time, a request for waiver should be provided to the Authorizing Official with a copy to the NWS IT Security Officer (ITSO).

AC-11 Session Lock

DOC policy requires all operating units to implement the Federal Desktop Core Configuration, which includes 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, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

However, since many NWS systems are operational systems that require immediate access to time-sensitive resources related to the protection of 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 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 must 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 3 and its Annexes.

AC-14 Permitted Actions Without Identification or Authentication

NWS requires System Owners to ensure that all actions taken on NWS systems are attributable to a specifically identified and authenticated user. This requirement does not pertain to external persons accessing publicly-available NWS web sites.

AC-19 Access Control for Mobile Devices

The NWS OCIO circulates new requirements for DOC and NOAA controls upon receipt.

AC-22 Publicly Accessible Content

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

3. Awareness and Training.

Awareness and Training				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	Not Selected	Not Selected	Not Selected

Table 3: Awareness and Training Controls

There are no NWS enhancements for Awareness and Training.

4. Audit and Accountability.

Audit and Accountability				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (3) (4)	AU-2 (3) (4)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	AU-6	AU-6	AU-6 (1)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-10	Non-repudiation	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12	AU-12 (1)
AU-13	Monitoring for Information Disclosure	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	Not Selected	Not Selected	Not Selected

Table 4: Audit and Accountability Controls

AU-5 Response to Audit Processing Failures

NWS OCIO requires that documentation of audit process failures be retained throughout the life cycle of the system.

AU-6 Audit Review, Analysis, and Reporting

NWS requires that monitoring and analysis of audit logs be conducted at least weekly. System Owners should document the frequency for analysis, the dates performed, and results, and maintain the information throughout the life cycle of the system.

AU-7 Audit Reduction and Report Generation

Because of the federated nature of the NWS IT enterprise, there is no centralized automated log reduction and reporting tool. System Owners should maintain descriptive information regarding the tool(s) they select for this control and the results of automated log reduction demonstrating variance from established norms should be retained throughout the life cycle of the system.

AU-8 Time Stamps

To maintain consistency throughout the enterprise, NWS requires use of UTC timestamps.

AU-10 Non-Repudiation

When System Owners believe Non-Repudiation capabilities to be a mandatory requirement, such as documenting the validity of a Watch or Warning notification, it is recommended that the PIV Common Access Card Public Key Infrastructure (PKI) capabilities be utilized for generating digital signatures. System Owners should document their decisions regarding the use of Non-Repudiation capabilities.

AU-12 Audit Generation

Because of the federated nature of the NWS IT enterprise, only System Owners know the information system components utilized in their systems. To comply with NIST SP 800-53 Rev. 3 requirements, System Owners should define the information system components to be covered by this control.

5. Security Assessment and Authorization.

Security Assessment and Authorization				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification (Withdrawn)	N/A	N/A	N/A
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7

Table 5: Security Assessment and Authorization Controls

CA-1 Security Assessment and Authorization Policies and Procedures

The NOAA Assistant Administrator for Weather Services has delegated the role of Authorizing Official (AO) to Directors of NWS Headquarters Offices and NWS Regions. AOs and System Owners should comply with the minimum DOC Certification and Accreditation (C&A) artifacts as stated in CITR-004, which specifies requirements for the DOC C&A process (now called the Assessment and Authorization process by NIST).

CA-4 Security Certifications

DOC requires the OUs to employ an independent CA or Certification Team to conduct an assessment of the security controls in the information system. Funding for this requirement is not provided centrally. However, the NWS has procurement vehicles in place should the System Owner desire to use them.

CA-6 Security Authorization

As set out in NWSI 60-701, all NWS AOs are Directors of NWS Headquarters Offices and NWS Regions.

CA-7 Continuous Monitoring

AOs and System Owners should comply with the DOC Continuous Monitoring Plan as stated in CITR-003.

6.0 Configuration Management.

Configuration Management				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1) (3) (4)	CM-2 (1) (2) (3) (5) (6)
CM-3	Configuration Change Control	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings	CM-6	CM-6 (3)	CM-6 (1) (2) (3)
CM-7	Least Functionality	CM-7	CM-7 (1)	CM-7 (1) (2)
CM-8	Information System Component Inventory	CM-8	CM-8 (1) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	Not Selected	CM-9	CM-9

Table 6: Configuration Management Controls

CM-3 Configuration Change Control

The organization-defined configuration change control element for NWS is the Operations and Service Improvement Process (OSIP).

CM-5 Access Restrictions for Change

Because of the federated nature of the NWS enterprise, the NWS OCIO does not have a test environment in which to test software, hardware, or firmware. System Owners should document the controls utilized in their system(s) for review to determine if any unauthorized changes have occurred.

CM-8 Information System Component Inventory

NOAA/NWS inventory management policies are outside the control of the NWS OCIO and therefore are not repeated here. Each System Owner should maintain a current Information System Component Inventory that accurately reflects the state of the system.

7.0 Contingency Planning.

Contingency Planning				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2)(3)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	CP-4	CP-4 (1)	CP-4 (1) (2) (4)
CP-5	Contingency Plan Update (Withdrawn)	N/A	N/A	N/A
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3) (4) (5)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2)(3)	CP-10 (2) (3) (4)

Table 7: Contingency Planning Controls

CP-1 Contingency Planning Policy and Procedures

Within NWS, additional requirements are set out in NWSD 10-22 and NWSI 10-2201 regarding backup operations for failover between NWS components.

CP-2 Contingency Plan

Because of the federated nature of the NWS enterprise, no one set of control enhancements will fit all needs. However, at a minimum, all NWS elements should distribute their contingency plans to all personnel responsible for execution of the plan, the next higher headquarters, and maintain contingency plans on the NOAA Vital Records Server and/or on a local equivalent with access rights to personnel within the organization and at the next higher headquarters. The review and update schedule set out in CP-1 above should be maintained. System Owners should document the controls utilized in their system and retain the documentation for the life cycle of the system.

CP-3 Contingency Training

NWS requires that such training be conducted and that after-action reports be documented.

CP-4 Contingency Plan Testing and Exercises

NWS requires that such testing and exercises are conducted and that after-action reports be documented.

CP-7 Alternate Processing Sites

Because of the federated nature of the NWS enterprise, no single set of controls will be universally applicable. However, at a minimum, each NWS organization, as part of the Business Impact Analysis (BIA) conducted for each system must determine the recovery time objectives (maximum allowable down time) for each system based on the business processes the system supports. That BIA determination will set the recovery time objective for each system. System Owners should document the demonstrated results exercises and the extent to which recovery time objectives were achieved.

CP-8 Telecommunications Services

Because of the federated nature of the NWS enterprise, no single set of controls will be universally applicable. However, at a minimum, each NWS organization, as part of the Business Impact Analysis (BIA) conducted for each system must determine the recovery time objectives (maximum allowable downtime) for each system based on the business processes the system supports. That BIA determination will set the recovery time objective for telecommunications services. System Owners should document the demonstrated results exercises and the extent to which recovery time objectives were achieved.

To achieve communications recovery time objectives, System Owners may wish to consider “last mile” alternative routing (in other words, multiple communication pathways such as terrestrial fiber optic cable supplemented by 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 NOAAnet.

CP-9 Information System Backup

NWS supplements this control by requiring at least weekly full backup and daily incremental backup. System Owners should 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.

CP-10 Information System Recovery and Reconstitution

NWS requires at least annual testing of the recovery and reconstitution controls, preparation of after action reports, documentation of the viable life of the backup media, and retention of records of control testing, etc., be maintained for the entire life cycle of the system.

8. Identification and Authentication.

Identification and Authentication				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1)	IA-2 (1) (2) (3) (8)	IA-2 (1) (2) (3) (4) (8) (9)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5 (1)	IA-5 (1) (2) (3)	IA-5 (1) (2) (3)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8	IA-8	IA-8

Table 8: Identification and Authentication Controls

IA-1 Identification and Authentication Policy and Procedures

NOAA augments this control with its Policy for Identification, Authentication and Password Management. System Owners should be alert to the fact that NOAA’s instructions for this control also contains instructions that apply to subsequent items in this control family that are not being repeated herein.

IA-7 Cryptographic Module Authentication

NWS recommends transition to the 2 factor authentication process enabled by the new PIV Common Access Cards as the most cost effective method of implementing and documenting this control.

9. Incident Response.

Incident Response				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8

Table 9: Incident Response Controls

IR-1 Incident Response Policy and Procedures

For all security incidents, the NWS OCIO must provide an initial IT security incident report in accordance with NOAA guidance at <https://www.csp.noaa.gov>. All electronic communication regarding incidents must be encrypted using the NOAA Incident Reporting Form (NOAA Form 47-43) and encrypted electronic mail. NOAA does not authorize the use of electronic communications using standard “clear text” electronic mail.

To date, NOAA has not set an encryption standard. NWS recommends utilization of the Common Access Card PKI encryption system to both standardize encryption utilization across NWS and to prevent additional costs incurred by disparate encryption systems.

10. Maintenance.

Maintenance				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Non-Local Maintenance	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6

Table 10: Maintenance Controls

MA-1 System Maintenance Policy and Procedures

Only System Owners are in a position to establish the system maintenance policies and procedures for their unique environment. NWS OCIO requires that the review and update of such policies and procedures be documented at least annually and whenever substantive changes in the technical environment take place or there are changes in key personnel responsibilities. These policies and procedures should be maintained iteratively throughout the life cycle of the system.

MA-3 Maintenance Tools

Other than NOAA-provided scanning tools, NWS has no other independent enterprise maintenance tools. System Owners should document what control(s) is/are in place and when/how such tools are implemented and retain documentation throughout the system life cycle.

MA-4 Non-Local Maintenance

Only System Owners are in a position to establish the system maintenance policies and procedures for their unique environment. NOAA does not supplement this control and NWS does not utilize non-local maintenance tools. If System Owners utilize such controls they should document what control(s) is/are utilized and how they are implemented. Such documentation should be retained throughout the system life cycle.

MA-5 Maintenance Personnel

Only System Owners are in a position to establish the system maintenance policies and procedures for their unique environment. In the event external personnel are utilized for system maintenance, System Owners should document Service Level Agreements and PS-6 Access Agreements. These should be maintained at least three years beyond the completion/termination of the external services contract.

MA-6 Timely Maintenance

Because of the federated nature of the NWS computing enterprise, on the basis of local knowledge and Business Impact Analyses, System Owners must create their own listing of security-critical information system components and acceptable outage periods. Documentation should be retained throughout the system life cycle.

11. Media Protection.

Media Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Marking	Not Selected	MP-3	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (2) (4)	MP-5 (2) (3) (4)
MP-6	Media Sanitization	MP-6	MP-6	MP-6 (1) (2) (3)

Table 11: Media Protection Controls

MP-3 Media Marking

Given the federated nature of the NWS IT enterprise, only System Owners are in a position to list and mark media types or components used in their system environments, as well as the controlled areas within which their systems operate.

MP-4 Media Storage

To date, NOAA has not selected a common encryption mechanism or tool that should be used for all media that should be restricted in some manner - privileged medical, contract-sensitive, proprietary, personally identifiable information, special access programs/compartments. NWS recommends utilization of the Common Access Card PKI encryption system to both standardize encryption utilization across NWS and to prevent additional costs incurred by disparate encryption approaches. At a minimum, System Owners should comply with controls required under CP-9.

MP-5 Media Transport

System Owners are responsible for establishing local controls over the transportation of any media that should be restricted in some manner, i.e., containing personally identifiable information (PII), and such controls should comport with DOC requirements for full disk encryption of PII. Such controls should be documented and reviewed annually.

MP-6 Media Sanitization

System Owners and the IT staff supporting the system must certify that media sanitization has taken place prior to disposal of any media. The date and nature of such sanitization procedures should be recorded.

12. Physical and Environmental Protection.

Physical and Environmental Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected

Table 12: Physical and Environmental Protection Controls

PE-4 Access Control for Transmission Medium

The physical access to transmission lines can only be controlled at the System Owner level. The requirement for such access controls and any compliance procedures should be documented.

PE-5 Access Control for Output Devices

Physical access to output devices, such as printers, monitors, and audio devices, can only be controlled at the System Owner level. The requirement for such access controls and any compliance procedures should be documented.

PE-10 Emergency Shutoff

System Owners and local network operations staff should document locations and procedures for this control. A record of any deviations from expected results should be maintained throughout the system life cycle.

PE-11 Emergency Power

System Owners and local facilities staff should document the manner in which this control is implemented and dates the control(s) is/are tested.

PE-12 Emergency Lighting

System Owners and local facilities staff should document the manner in which this control is implemented and dates the control(s) is/are tested.

PE-13 Fire Protection

System Owners and local facilities staff should document the manner in which this control is implemented and dates the control(s) is/are tested.

PE-14 Temperature and Humidity Controls

System Owners and local facilities staff should document the manner in which this control is implemented and dates the control(s) is/are tested.

PE-15 Water Damage Protection

System Owners and local facilities staff should document the manner in which this control is implemented and dates the control(s) is/are tested.

PE-16 Delivery and Removal

System Owners and local facilities staff should document the manner in which this control is implemented and dates the control(s) is/are tested.

PE-17 Alternate work Site

System Owners and local facilities staff should document the manner in which this control is implemented and dates the control(s) is/are tested.

PE-18 Location of Information System Components

System Owners and local facilities staff should document the manner in which this control is implemented and dates the control(s) is/are tested.

13. Planning.

Planning				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update (Withdrawn)	N/A	N/A	N/A
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	Not Selected	PL-6	PL-6

Table 13: Planning Controls

PL-4 Rules of Behavior

System Owners may develop Rules of Behavior that enhance NOAA rules as the System Owner deems appropriate for their environment. Such rules should be provided to the NWS OCIO for review.

PL-5 Privacy Impact Assessment

NWS requires such assessments to be conducted at least every three years or more often if significant changes to the IT system occur.

PL-6 Security-Related Activity Planning

NWS supplementary guidance requires documentation of the implementation of this control be maintained at least until the next Assessment and Authorization review of the system.

14. Personnel Security.

Personnel Security				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8

Table 14: Personnel Security Controls*PS-4 Personnel Termination*

NWS requires all IT system access to be terminated on the final duty day of the terminated employee, as well as the return of all IT equipment and access devices, such as PIV cards and building access badges.

PS-5 Personnel Transfer

For permanent personnel transfers (as opposed to Temporary Duty assignments) outside NWS, all network access to NWS systems should be canceled on the final duty day and appropriate password changes made at the same time as necessary. The departing personnel should also return all IT equipment and access devices, such as PIV cards and building access badges.

PS-6 Access Agreements

NWS notes that access agreements need only be re-signed if there is a break in service.

15. **Risk Assessment.**

Risk Assessment				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update (Withdrawn)	N/A	N/A	N/A
RA-5	Vulnerability Scanning	RA-5	RA-5 (1)	RA-5 (1) (2) (3) (4) (5) (7)

Table 15: Risk Assessment Controls

RA-5 Vulnerability Scanning

NOAA has selected a NOAA Standard Vulnerability Scanning tool for meeting this requirement. The use of other tools and/or additional tools to perform vulnerability scanning requires an approved waiver from the NOAA IT Security Office.

16. System and Services Acquisition.

System and Services Acquisition				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1) (4)	SA-4 (1) (2) (4)
SA-5	Information System Documentation	SA-5	SA-5 (1) (3)	SA-5 (1) (2) (3)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	Not Selected	Not Selected	SA-13
SA-14	Critical Information System Components	Not Selected	Not Selected	Not Selected

Table 16: System and Services Acquisition Controls*SA-5 Information System Documentation*

At a minimum, all NWS elements should distribute their information system documentation to all personnel responsible for disaster recovery activities, the next higher headquarters, and maintain such documentation on the NOAA Vital Records Server and/or on a local equivalent with access rights to personnel within the organization and at the next higher headquarters.

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 Service Level Agreements and compliance with FISMA should be maintained at least three years beyond the completion/termination of the external services contract.

SA-11 Developer Security Testing

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

SA-12 Supply Chain Protection

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

SA-13 Trustworthiness

NWS requires that System Owners developing new systems, including research systems, maintain documentation of their compliance with these controls through procurement of goods solely through an approved Federal Acquisition Contract, utilization of software that is compliant with the Federal Desktop Core Configuration, and compliance with FISMA, FIPS and NIST standards that assure the availability, accuracy, and timely production of NWS services and products.

17. System and Communications Protection.

System and Communications Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3) (4) (5) (7)	SC-7 (1) (2) (3) (4) (5) (6) (7) (8)
SC-8	Transmission Integrity	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9 (1)	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12	SC-12 (1)
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing Devices	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	SC-20 (1)	SC-20 (1)	SC-20 (1)
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21

System and Communications Protection				
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	Not Selected	Not Selected	SC-24
SC-25	Thin Nodes	Not Selected	Not Selected	Not Selected
SC-26	Honey Pots	Not Selected	Not Selected	Not Selected
SC-27	Operating System-Independent Applications	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	Not Selected	Not Selected	Not Selected
SC-30	Virtualization Techniques	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	Not Selected	SC-32	SC-32
SC-33	Transmission Preparation Integrity	Not Selected	Not Selected	Not Selected
SC-34	Non-Modifiable Executable Programs	Not Selected	Not Selected	Not Selected

Table 17: System and Communications Protection Controls

SC-3 Security Function Isolation

NWS requires that System Administrators follow the NIST guidance to separate and protect security functions from other applications, functions, and normal user software, through use of partitions, domains, screened subnets, or other similar means. Because each NWS IT environment is different, each System Owner should document their approach, the dates when control testing and validation are conducted and the results thereof.

SC-4 Information in Shared Resources

From the perspective of the NWS OCIO, this control clearly applies to PII, which should be protected through the DOC requirement for full disk encryption. If System Owners believe that additional information may apply, the NWS OCIO is prepared to discuss the issue with them and collaborate on an acceptable technical approach to achieve the desired outcome. Any controls implemented by the System Owner should be documented and retained throughout the system's life cycle.

SC-5 Denial of Service Protection

Because of the federated nature of the NWS enterprise, no single solution set will adequately address every potential denial of service protection need. In considering the proper security controls for local systems, the System Owner should at a minimum consider whether their systems may be vulnerable to one or more of the following prevalent denial of services attacks. If so, System Owners should consider implementing countermeasures such as:

1. Disable direct broadcast functionality at border routers to make sure NWS networks are not used as an amplifier for attacks on other networks.
2. Configure perimeter routers to reject as incoming messages any packets that contain internal source IP addresses since such packets are spoofed.
3. Allow only the necessary ICMP traffic into and out of an environment.
4. Employ network-based IDS to watch for suspicious activity.
5. Apply appropriate patches in a timely fashion, usually not more than 45-days following release.
6. Allow only the necessary UDP packets into and out of the environment.
7. Use perimeter routers to restrict unnecessary ICMP and UDP traffic.
8. Decrease the connection-established time out period.
9. Increase the size of the connection queue in the IP stack.
10. Configure firewalls to watch for common attack types, such as synflood, and alert the administrator or cut the connection.
11. Disallow malformed packets to enter the environment.
12. Use a router that combines all fragments into a full packet prior to routing to the destination system.
13. Disable unused subsystems and services on computers.
14. Other controls as the System Owner deems appropriate for their unique operational environment.

Whatever controls the System Owner chooses to implement should be documented and retained across the life cycle of the system.

SC-8 Transmission Integrity

NWS envisions a common control being part of NOAA net when completed and fully operational. Until then, System Owners should 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 180-3 of October 2008 provides additional information. In the interim, System Owners should document whatever control they choose to implement and maintain records at least across the life cycle of the product.

SC-9 Transmission Confidentiality

NOAA does not supplement this control and neither NOAA nor NWS have a common control. NWS envisions a common control being part of NOAAnet when completed and fully operational. In the interim, NWS recommends use of the PKI encryption solution in PIV Common Access Cards as the most economical approach to this control. System Owners should document whatever control they choose to implement and maintain records at least across the life cycle of the product.

SC-12 Cryptographic Key Establishment and Management

NOAA does not supplement this control and neither NOAA nor NWS have a common control. NWS envisions a common control being part of NOAAnet when completed and fully operational. In the interim, NWS recommends use of the PKI encryption solution in PIV Common Access Cards as the most economical approach to this control. In the interim, System Owners should document whatever control they choose to implement and maintain records at least across the life cycle of the product.

SC-13 Use of Cryptography

NWS envisions a common cryptographic control being part of NOAAnet when completed and fully operational. In the interim, NWS recommends use of the PKI encryption solution in PIV Common Access Cards as the most economical approach to this control. When System Owners determine that cryptography is necessary, they should document whatever control they choose to implement and maintain records at least across the life cycle of the product.

SC-14 Public Access Protections

NWS provides controls supporting integrity and availability of web content managed by the NWS Web Farm family of services. Should System Owners choose to provide public access to NWS information through another forum, such as social media, consultation with the NWS OCIO is required for the process of security controls selection to protect the NWS network and NWS information availability and integrity. Whatever solution(s) System Owners choose to implement should be documented records retained at least across the life cycle of the product.

SC-15 Collaborative Computing Devices

Because of the federated nature of the NWS computing environment, this control cannot be implanted in a common fashion. Each individual System Owner bears the responsibility and accountability for addressing this requirement for their system. System Owners should document whatever control(s) they choose to implement and maintain a record of those controls.

SC-17 Public Key Infrastructure Certificates

NWS OCIO requires that all System Owners whose systems use PKI certificates should, as a matter of confidentiality and integrity, adhere to the requirement that certificates be certified with the Federal Bridge Certification Authority. Documentation of that certification should be provided to the NWS OCIO and updated should any certificate changes take place. Documentation should be retained for review across the life cycle of the certificate(s).

SC-18 Mobile Code

System Owners should document whatever controls they adopt regarding mobile code and retain the documentation.

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

NOAA does not supplement this control and neither NOAA nor NWS have implemented a common control. System Owners whose systems include control of Domain Name Servers (DNS) must comply with the provisions of OMB Memorandum M-08-23 regarding DNS Security (DNSSEC).

SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

Given the federated nature of the NWS enterprise, NWS cannot centrally implement this control. Whatever control(s) is/are implemented should be documented and retained across the life cycle of the system.

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

Given the federated nature of the NWS enterprise, NWS cannot centrally implement this control. Whatever control(s) is/are implemented should be documented and retained across the life cycle of the system.

SC-23 Session Authenticity

NOAA does not supplement this control and neither NOAA nor NWS provide common controls. NOAAnet, when fully implemented and operational, envisions incorporation of a common control for Session Authentication. In the interim, System Owners should consider using 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. Whatever control(s) is/are implemented should be documented and retained across the life cycle of the control.

SC-24 Fail in Known State

Given the federated nature of the NWS enterprise, neither NOAA nor NWS can provide common controls. NWS OCIO is available for collaboration with any 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/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. Whatever control(s) is/are implemented should be documented and retained across the life cycle of the system.

SC-26 Honeypots

Should a System Owner wish to proceed with this control, coordination with NWS OCIO is required so that NOAA Legal Counsel can review the proposed solution, which could have serious legal implications.

SC-28 Protection of Information at Rest

Given the federated nature of the NWS enterprise, neither NOAA nor NWS can provide a common control for this issue. System Owners should implement controls that assure that configuration of databases, firewall rules and configurations, gateways, Intrusion Detection System/Intrusion Prevention System (IDS/IPS), filtering routers, and access and authorization controls within their system architecture are adequate to achieve the level of protection required by this control. Documentation of controls should be maintained across the life cycle of the system.

SC-30 Virtualization Techniques

If a System Owner wishes to proceed with a virtualization initiative, such as server virtualization, NWS OCIO requires that it be kept informed of the progress and architecture being employed.

SC-32 Information System Partitioning

Given the federated nature of the NWS enterprise, neither NOAA nor NWS can provide a common control for this issue. System Owners should implement controls that assure the partitioning of information system components and domains if disparities in the security categorization of system components and the size and volume of transactions at the disparate security levels would be better served by such partitioning. Since NWS systems rarely require “High” confidentiality requirements, it does not seem likely that System Owners will determine that control is necessary. However, if such controls do seem to be appropriate, System Owners may wish to consider running at a “system high” state as a compensating control instead of partitioning.

18. System and Information Integrity.

System and Information Integrity				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2) (3)	SI-3 (1) (2) (3)
SI-4	Information System Monitoring	Not Selected	SI-4 (2) (4) (5) (6)	SI-4 (2) (4) (5) (6)
SI-5	Security Alerts, Advisories, and Directives	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	Not Selected	Not Selected	SI-6
SI-7	Software and Information Integrity	Not Selected	SI-7 (1)	SI-7 (1) (2)
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Input Validation	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	Not Selected	Not Selected	Not Selected

Table 18: System and Information Integrity Controls

SI-4 Information System Monitoring

While there is no NWS capability to conduct system monitoring, the transition to NOAAnet and the Federal Trusted Internet Connection will for the first time enable NWS-wide monitoring of backbone communications for malware and known attack vectors. In the interim, controls implemented by System Owners should be tested to be sure the controls are properly installed, operating as intended, and providing the desired protections.

SI-5 Security Alerts, Advisories and Directives

As NWS OCIO becomes aware of security alerts, advisories, and/or directives, they are disseminated to the ISSO community.

SI-7 Software and Information Integrity

NWS does not provide the necessary tools to implement this control. Should any such tools presently be in place at a system level, System Owners should set the frequency of use and document results across the life cycle of the system.

SI-10 Information Input Validation

Because of the federated nature of the NWS IT environment, System Owners are in the best position to know the extent to which their systems require tools to assure that these controls are properly installed, operating as intended, and providing the desired functionality.

SI-11 Error Handling

NOAA does not supplement this control or provide guidance on what sensitive or potentially harmful information must be concealed in error logs. However, such information is generally considered to be PII. System Owners should document any other controls they utilize and maintain records across the life cycle of the system.