

NATIONAL WEATHER SERVICE CENTRAL REGION SUPPLEMENT 02-2010

APPLICABLE TO NWSI 60-702

April 18, 2012

Information Technology

INFORMATION TECHNOLOGY SECURITY POLICY, NWSPD 60-7

MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS, NWSI 60-702

IT SECURITY POLICIES & PROCEDURES

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

OPR: W/CR41x5 (A. Van Meter)

Certified by: W/CR4 (R. Brauch)

Type of Issuance: Routine

SUMMARY OF REVISIONS: The changes to this supplement reflect the changes between NIST 800-53 revision 2 and NIST 800-53 revision 3. The affected security controls are as followings: RA-1, RA-3, RA-4, SA-6, SA-12, SA-13, SA-14, CA, CA-4, CA-7, PS-8, PE-2, PE-4, PE-5, CP-4, CP-5, CP-10, CM-2, CM-4, CM-7, CM-7, CM-9, MA-2, MA-4, SI-4, SI-5, SI-6, SI-10, SI-13, MP-1, MP-2, MP-3, MP-6, IR-3, IR-7, IR-8, IA-2, IA-4, IA-8, AC-2, AC-9, AC-12, AC-13, AC-15, AC-16, AC-19, AC-20, AC-21, AC-22, AU-5, AU-6, AU-12, AU-13, AU-14, SC-4, SC-15, SC-24 through SC-34, and PM-1 through PM-11. Appendix B – added new Certification of PDA and Cell Phone Destruction Form and updated the CR Computer/Hard Drive Sanitization Validation Form. A sample Restricted Area sign was placed in Appendix F, and the new Annual Privileged Accounts Verification Form was placed in Appendix H.

_____/signed/
Lynn P. Maximuk
Regional Director

April 4, 2012
Date

IT SECURITY POLICIES & PROCEDURES

<u>Table of Contents:</u>	<u>Page</u>
1. Purpose and Introduction.....	3
2. Scope.....	3
3. Roles and Responsibilities	3
4. Document Structure and Content.....	4
5. Management Controls	4
5.1. Risk Assessment (RA):.....	4
5.2 Planning (PL):.....	6
5.3 System and Services Acquisition (SA).....	7
5.4 Security Assessment and Authorization (CA):.....	10
6. Operational Controls	12
6.1 Personnel Security (PS)	12
6.2 Physical and Environmental Protection (PE).....	14
6.3 Contingency Planning (CP)	18
6.4 Configuration Management (CM)	21
6.5 System Maintenance (MA).....	24
6.6 System and Information Integrity (SI).....	27
6.7 Media Protection (MP)	30
6.8 Incident Response (IR)	33
6.9 Awareness and Training (AT)	35
7. Technical Controls	36
7.1 Identification and Authentication (IA).....	36
7.2 Access Control (AC).....	38
7.3 Audit and Accountability (AU)	43
7.4 System and Communications Protection (SC).....	46
8. Information Security Program Management Controls.....	51
8.1 Program Management (PM)	51

APPENDICES

APPENDIX A Abbreviations and Acronyms.....	A-1
APPENDIX B NOAA Sanitization Validation and Destruction Worksheet.....	B-1
APPENDIX C Sample Central Region Risk Analysis Worksheet	C-1
APPENDIX D WFO/RFC Local Security Related Planning Activities Example.....	D-1
APPENDIX E IT System Interconnection Agreement Templates	E-1
APPENDIX F Restricted/Controlled Area Sign – Sample	F-1
APPENDIX G HAM Usage Guideline Example.....	G-1
APPENDIX H Annual Privileged Accounts Verification Form.....	H-1
APPENDIX I EMRS Report Auditing A-26 Sample	I-1

1. Purpose and Introduction. This supplement defines and establishes the regional policy and procedures for implementing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3 requirements for the security controls in the NOAA8881 system boundary. The main objective is to control the risk and magnitude of harm that could result from the loss, misuse, disclosure, or modification of the system. These procedures are based on Federal Information Processing Standards (FIPS), Department of Commerce (DOC), National Oceanic and Atmospheric Administration (NOAA), and National Weather Service (NWS) security documents and reflect higher organization requirements and established IT security practices. Applicable DOC and NOAA policies will be implemented as written unless otherwise stated in this document. It also provides clarification to the above mentioned documents and establishes the regional control criteria for those controls that DOC and NOAA policy has assigned to the System Owner.

2. Scope. The policy and procedures specifically focus on the people, equipment, network, and software components of the Information Technology (IT) systems within the NOAA8881 network boundary. It applies to all National Weather Service (NWS) systems within the Central Region, including contractor's systems that manage, store, and/or process data on behalf of Central Region. Individual local offices are encouraged to develop their own office-specific operating control guidance for their operating environment, providing that their local guidance meets and exceeds this policy guidance and other higher level security policy and procedures.

3. Roles and Responsibilities. The following roles are defined for the system:

1. **Authorizing Official (AO):** The principal person who has the authority to formally assume responsibility for operating an information system at an acceptable level of risk. The Regional Director (RD) is assigned this role.
2. **System Owner (SO):** The principal person responsible for the management and operations of all IT systems within the NOAA8881 system boundary. The Systems and Facility Division (SFD) Chief is assigned this role.
3. **Security Manager (SM):** The principal person with statutory or operational authority who oversees the local programming and IT support of their Local Area Network (LAN). They have overall responsibility for ensuring the security controls are implemented for their LAN. The CRH IT Branch Chief, the Meteorologist-In-Charge (MIC) and the Hydrologist-In-Charge (HIC) are assigned this role.
4. **Information System Security Officer (ISSO):** The primary person responsible for management of IT system and information security and in managing the FISMA requirements. The person designated as the CR ISSO has this role.
5. **System Administrator (SA):** A person in charge of maintaining and administering the implementation of the policy and procedures on the IT systems. The Electronic System Analyst (ESA) and/or the Information Technology Officer (ITO) are assigned SA duties and responsibilities. Other personnel who have the knowledge, training, and skill set to perform system administrator duties may be assigned SA duties by the SM.
6. **User:** The user is an approved NOAA employee, contractor, or visitor with an authorized user account for using the IT system to achieve the NOAA/NWS mission of the organization.
7. **Privileged User:** Users who have been granted the rights beyond that of a normal

- user to install software and/or to make computer setting changes similar to an SA.
4. Document Structure and Content. The document structure aligns with NIST Special Publication 800-53. The organization of controls is by control type (i.e. Management, Operational, and Technical) followed by control topic that follows the order within the System Security Plan (SSP).
 5. Management Controls. These are security controls for the information system that focus on the management of risk and the management of the information system security. Controls in this control class rely on management policy and procedures to set and enforce security safeguards and countermeasures to mitigate the risks.
- 5.1. Risk Assessment (RA): The NOAA8881 system RA process supports risk management in the evaluation of the system's risk to determine the overall security posture of CR WAN/LAN. The RA process has three phases: System documentation, Risk determination and safeguard determination.

Relevant Documents

- NIST SP 800 – 12 [An Introduction to Computer Security](#)
- NIST SP 800 – 30 [Risk Management Guide for Information Technology Systems](#)
- NIST SP 800 – 39 [Managing Information Security Risk: Organization, Mission, and Information System View](#)
- NIST SP 800 – 40 Ver. 2 [Creating a Patch and Vulnerability Management Program](#)
- NIST SP 800 – 60 Rev.1 [Guide for Mapping Types of Information and Information Systems to Security Categories: \(2 Volumes\) - Volume 1: Guide Volume 2: Appendices](#)
- NIST SP 800 – 70 Rev. 2 [National Checklist Program for IT Products: Guidelines for Checklist Users and Developers](#)
- NIST SP 800 – 100 [Information Security Handbook: A Guide for Managers](#)
- NIST SP 800 – 115 [Technical Guide to Information Security Testing and Assessment](#)
- DOC ITSP [Information Technology Security Program Policy](#)

5.1.1 Risk Assessment Policy and Procedures (RA-1): This is a fully implemented NOAA common control. The compliance with the DOC and NOAA policy and procedures according to the system categorization are tracked for each information system within NOAA and are part of an overall Assessment and Accreditation (A&A) plan. It is the System Owner's responsibility to properly categorize the system in accordance with FIPS 199.

5.1.2 Security Categorization (RA-2): NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories: Volume I and Volume II are used to determine the proper system categorization. The categorization of the NOAA8881 is the responsibility of the System Owner and the Central Region (CR) ISSO, but it requires input from local field offices. The NOAA8881 FIPS199 Security Categorization document contains the process, methodology, and supporting information to support the system's "Moderate" classification.

5.1.3 Risk Assessment (RA-3): NIST SP 800-53, Rev 3 sets the requirement for organizations to conduct assessments of risk and magnitude of harm to the system. Risk assessments are conducted locally, regionally, and from the DOC Office of Security on an annual basis or whenever there are significant changes within the IT system or whenever significant threats

occur within the environment of operations. For example, the deployment of Active Directory in the NOAA8881 IT infrastructure or the construction of a new nuclear facility near a CR office would constitute a significant event that would require an update. The overall risk assessment is documented in the current NOAA8881 Continuous Monitoring document and in the Risk Assessment Report produced by the CR ISSO and reviewed and accepted by the Regional Director and the Systems and Facilities Division Chief.

Local offices are responsible for conducting a local office risk assessment before seeking CRH approval to introduce new IT systems or technology into the NOAA8881 system. The local office risk assessment needs to address and document the following areas.

- Determine operational requirements
- Identify program inputs/outputs, protocols, services, etc.
- Identify known risks associated with hardware/software
- Identify controls that will mitigate known risks
- Evaluate the impact of IT System if software vulnerabilities are exploited
- Complete the CR Risk Analysis Worksheet as shown in Appendix C

5.1.4 Risk Assessment Update (RA-4): This security control has been withdrawn in NIST 800-53 revision 3 and incorporated in the RA-3 control.

5.1.5 Vulnerability Scanning (RA-5): Vulnerability scanning is a required process directed from DOC, NOAA and NWS. The following steps are required to be taken by all field offices in the Central Region:

- Entire system scans be performed systematically on a routine basis using the NOAA approved automated scan tool/s, with scan results available to the CR ISSO as stated in the released CR NOAA IT System Scan EMRS Technical Order. The CR ISSO will analyze the scan results and recommend mitigation actions to System Owner.
- Computers that have been out of the office and have been detected to have malicious code under the SI-3 control will need to be scanned by a vulnerability scanning tool to ensure that they are at the highest patch level and/or have sufficient countermeasures in place to mitigate any discovered weaknesses.
- Vulnerability scanning and assessments will be performed on all IT devices. Non-network devices or those network devices that the scanner tool cannot assess must be evaluated manually and placed on the quarterly Plan of Action and Milestone spreadsheet (POA&M). Waivers and exceptions will be granted by the System Owner on a case by case basis. National program systems such as AWIPS, CRS, etc. will normally not be scanned by local office due to their program level ownership and configuration management.
- Office regional routers will not enable SNMP to run the scanner tool as these are configuration managed devices and will be sample scanned from CRH.
- All HIGH and MEDIUM vulnerabilities will be mitigated within 25 days following the scheduled scan due date.

- Completed scan and rescan files will be automatically sent to the NOAA approved Tenable Security Center for review and compilation.
- Items listed in the POA&M will be remediated by the date stated in the POA&M.

In order to protect both the Government and the employee, all approved connections of personally-owned computer equipment under the AC-20 security control must be inspected by the local ESA or ITO before it is connected to the network. The local ESA or ITO will need to ensure that the computer equipment is scanned and meets the same level of security controls as Government-owned equipment. Scanning of approved personally-owned equipment which falls under the category of removable media is addressed under the SI-3 control. The only exception is personally-owned equipment used at the employee's home during telework status. The risks associated with that equipment is managed and mitigated through the telework management controls (i.e. checklists, telework agreement, etc.) and the Central Region VPN appliance end to end security technical controls.

5.2 Planning (PL): Security policies and procedures address the overall policy requirements for the system's confidentiality, integrity, and availability. NIST Special Publication 800-18 provides guidance on security planning while NIST Special Publication 800-12 provides guidance on security policies and procedures.

Relevant Documents

- NIST SP 800 – 12 [An Introduction to Computer Security](#)
- NIST SP 800 – 18 Rev.1 [Guide for Developing Security Plans for Federal Information Systems](#)
- NIST SP 800 – 100 [Information Security Handbook: A Guide for Managers](#)
- NOAA [Privacy Impact Assessment Guidance](#)

5.2.1 Security Planning Policy and Procedures (PL-1): This is a fully implemented NOAA common control. The NOAA 212-1302 IT Security Manual requires a System Security Plan (SSP) based on NIST SP 800-18 guidance for all IT Systems. The NOAA8881 CR WAN/LAN SSP document covers all IT systems and their components within the Central Region.

5.2.2 System Security Plan (PL-2): NOAA has established PL-2 as a hybrid control in which all system owners are required to develop and implement a SSP that is in accordance with NOAA and DOC policy and procedures. The SSP is the plan that implements and documents each system security control in place for the NOAA8881 information system, providing a system security requirement overview of the security controls compliance. The NOAA8881 Security Plan will be annually reviewed and updated, as necessary, as part of the Continuous Monitoring of the system plans and procedures. Each field office is responsible to review the plan and notify the CR ISSO with specific information to depict the uniqueness and differences from the core plan which details the basic operation of the office. The CR ISSO is the document owner who has the responsibility to review and update the plan for the System Owner who is the plan's approving official.

5.2.3 System Security Plan Update (PL-3): This security control has been withdrawn in NIST 800-53 revision 3 and incorporated in the PL-2 control.

5.2.4 Rules of Behavior (PL-4): NOAA has established PL-4 as a common control where users are required to accept the rules of behavior without exception before being allowed to access NOAA IT systems. The acceptance of the rules of behavior and security training course are annual requirements tracked by NOAA using the NOAA IT Security Awareness Course database. The NOAA8881 Rules-Of-Behavior document consolidates the DOC and NOAA rules into one single document and is part of the system's SSP package.

5.2.5 Privacy Impact Assessment (PIA) (PL-5): NOAA has established PL-5 as a hybrid control which requires the system owner to assess and determine the extent of privacy information that is stored or processed by the system. A PIA will be completed by the CR ISSO at least every three years or more often if it has been determined that a significant change has occurred in storing and/or processing privacy data by the system.

5.2.6 Security-Related Activity Planning (PL-6): NWSI 60-702 supplements this control by requiring offices to document required security-related planning activities. The CR ISSO will create and distribute a regional table annually. In addition to the regional table, each local office is to create a local table for their local security-related activities. See the sample PL-6 Table provided in Appendix D of this supplement.

5.3 System and Services Acquisition (SA): The System and Services Acquisition controls are designated as management controls that require management policy and procedures. The SA-1 is **fully** implemented at the NOAA level. See NOAA Common Controls, v4.1, April 7, 2010 document for a complete description of these controls. The following controls are supplemented by the NOAA8881 system.

Relevant Documents

- FIPS 140 – 2 [Security requirements for Cryptographic Modules](#)
- NIST SP 800 – 12 [An Introduction to Computer Security](#)
- NIST SP 800 – 18 Rev.1 [Guide for Developing Security Plans for Federal Information Systems](#)
- NIST SP 800 – 23 [Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products](#)
- NIST SP 800 – 35 [Guide to Information Technology Security Services](#)
- NIST SP 800 – 36 [Guide to Selecting Information Technology Security Products](#)
- NIST SP 800 – 100 [Information Security Handbook: A Guide for Managers](#)
- NIST SP 800 – 37 [Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)
- NIST SP 800 – 53 Rev. 3 [Recommended Security Controls for Federal Information Systems](#)
- NIST SP 800 – 64 Rev. 2 [Security Considerations in the System Development Life Cycle](#)
- NIST SP 800 – 65 [Integrating IT Security into the Capital Planning and Investment Control Process](#)
- NIST SP 800 – 70 [Rev. 2 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers](#)
- DOC ITSPP [Information Technology Security Program Policy](#)

5.3.1 System and Services Acquisition Policy and Procedures (SA-1): DOC has established an IT Security checklist for acquisitions of services and goods to ensure that data and information technology systems are adequately protected from outside threats throughout the acquisition life cycle. The completion and approval authority of the checklist is a CRH function and normally requires no field office actions other than complying with the security requirements in the solicitation.

5.3.2 Allocation of Resources (SA-2): The allocation of resources and the determination of security requirements are performed as part of the annual budget allocations for IT resources.

5.3.3 Life Cycle Support (SA-3): Central Region meets this control through the development and implementation of its IT Cyclical Replenishment Plan.

5.3.4 Acquisitions (SA-4): All system IT acquisitions (new or replacement) must meet the requirements of the CR IT Cyclical Replenishment Plan and the Enterprise Desktop Configuration plan for supporting hardware or software.

- All Linux software must be Redhat Enterprise or Fedora/CentOS supported software, with the version operational tested before released in the production environment.
- All Windows based operating system must be a current and supported release from Microsoft. Any new releases will be tested and approved before any upgrades are allowed.
- Application software shall be tested and approved by Security Manager or their designate before it is introduced to the CR system.

All micro IT acquisitions (less than \$3,000) need to be reviewed by an IT staff person (One of the following: CRH IT Branch Chief, CR SFD Chief, CR ISSO, local ESA or ITO). Purchases over the micro purchase limit must include the submission of an IT Acquisition Checklist to the CR ISSO for review and approval..

5.3.5 Information System Documentation (SA-5): Office information system documentation from CRH and from local offices needs adequate protection measures in place to safeguard the system's information from unauthorized users. Passwords, software license keys, and configuration checklists or files are some examples of system documentation that need protection. Besides documentation protection, the documentation needs to be available to authorized personnel who have a need for the information.

5.3.6 Software Usage Restrictions (SA-6): All system software (operating system or application) must meet all federal guidelines and policies from DOC, NOAA, and NWS. The following is required for all systems in the NOAA8881 system:

- Do not make any illegal copies of copyrighted software. Normally the license will allow a single copy to be made for archival purposes. If the license is for multiple users, do not exceed the authorized number of copies.
- Maintain records of software installed on each system and ensure that a license or other proof of government ownership is on file for each piece of software.

- Store licenses, software manuals, and procurement documentation in a secure location (e.g., closed file cabinet, etc.).
- Software shared from a server where there are a limited number of concurrent licenses, compensating controls (i.e. key license manager, local usage memorandum, usage audits, etc.) must be in place to ensure that concurrency limits are respected.
- Authorized use of peer-to-peer technology must be approved by NOAA.

5.3.7 User Installed Software (SA-7): With the use of Active Directory and group policies, no normal user (i.e. non-admin user) will be allowed to download, and install software on any CR IT system. Installation of software shall be completed by the local ESA/ ITO or his/her authorized backup. An SA may elevate the privileges of a normal user account, providing them the ability to download and install software to meet mission requirements when IT staff support is not available. Any installation of non-enterprise software shall be tested prior to its installation to determine the impact on current baselines and network performance. Security or hacker tools will not be installed on any IT system unless authorization is provided by the CR ISSO.

5.3.8 Security Engineering Principles (SA-8): Security Design Principles are essential to ensure that the security posture of the overall system remains the same or higher when new technologies, components and/or information data flows are implemented into the operational environment and continue throughout the System Development Life Cycle (SDLC). Below are some design principles that need to be considered:

- Driving ideas
 - o Clear and well-defined structure and interfaces
- Least Privilege
 - o an entity should be given only those privileges that it needs in order to accomplish its task
- Fail-Safe Defaults
 - o Default actions/access permission should be set to – none
- Economy of Mechanism
 - o Keep security mechanism simple
- Complete Mediation
 - o Input/Data Validation
- Open Design
 - o security of a mechanism should not depend on secrecy of its design or implementation
- Separation of Privilege
 - o Design a system which uses more than one verifiable condition in order to gain access
- Least Common Mechanism
 - o Do not share access mechanisms
- Psychological Acceptability
 - o Security mechanisms should not make the resource more difficult to access

5.3.9 External Information System Services (SA-9): An external information system service is a service that is implemented outside of the accreditation boundary of the organizational

information system (i.e., a service that is used by, but not a part of, the organizational information system). NWS requires that providers of these services conform and comply with FISMA and NIST standards. This is accomplished at the regional level as part of the acquisition for services. The documentation of the services and Service Level Agreements are maintained at least three years beyond contract termination date.

5.3.10 Developer Configuration Management (SA-10): System or software in-house development within the NOAA8881 system requires the developer to:

1. Create and implement a configuration management plan that controls changes to the system/software during development;
2. Test and document all code written prior to installing it in the operational environment;
3. Document software either in official documentation or fully displayed as remarks in the code;
4. Document the implementation of the project to include how to track security flaws and authorization of change.

5.3.11 Developer Security Testing (SA-11): Central Region requires that all system developers provide documentation that includes a security test procedures plan, an implementation plan, and a security test and evaluation results plan. This applies to external developer contracts and any internal development work within Central Region. The documentation is maintained at least three years beyond contract termination.

5.3.12 Supply Chain Protection (SA-12): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

5.3.13 Trustworthiness (SA-13): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

5.3.14 Critical Information System Components (SA-14): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

5.4 Security Assessment and Authorization (CA): The Security Assessment and Authorization controls are designated as management controls that require management policy and procedures. The CA-1 is fully implemented at the NOAA level. See NOAA Common Controls, v4.1, April 7, 2010 document for a complete description of these controls. The following controls are supplement by the NOAA8881 system.

Relevant Documents

- OMB [Circular A-130](#) and [Appendix III](#)
- FIPS 199 [Standards for Security Categorization of Federal Information and Information Systems](#)
- NIST SP 800 – 12 [An Introduction to Computer Security](#)
- NIST SP 800 – 37 [Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)
- NIST SP 800 – 47 [Security Guide for Interconnecting Information Technology Systems](#)
- NIST SP 800 – 53A [Guide for Assessing the Security Controls in Federal Information](#)

Systems

- NIST SP 800 – 100 [Information Security Handbook: A Guide for Managers](#)
- NIST SP 800 – 115 [Technical Guide to Information Security Testing and Assessment](#)
- DOC ITSPP [Information Technology Security Program Policy](#)
- DOC CTR-003 [Continuous Monitoring](#)
- DOC CTR-004 [Certification & Accreditation \(C&A\) Process](#)
- NOAA IT Security Manual [\(ITSM\) 212-1302 \(V4.2\)](#)
- NWSI 60-702 [Management, Operational, and Technical Controls](#)

5.4.1 Security Assessment and Authorization Policies and Procedures (CA-1): The development of these policies and procedures are established under the guidelines of NIST SP 800-37 and NIST SP 800-53. The NOAA8881 system AO and the SO are responsible to ensure the associated documents and artifacts comply with DOC, NOAA, and NWS policies.

5.4.2 Security Assessments (CA-2): NOAA has established CA-2 as a hybrid control which requires the system owner to assess and determine if the system security controls are in place, implemented correctly, operate as intended, and produce the desired outcome. The NOAA8881 system security controls will be reviewed in accordance with the Federal Information Security Management Act (FISMA), and DOC and NOAA policy guidance. An integral part of system security assessment and authorization is the on-going assessment and review of the system's security controls. Internal assessments of the controls are accomplished at all levels within the region. The following are the system security review and test assessment requirements:

- Each office will conduct an assessment of the security controls in the information system at least annually.
- Each office will conduct a self-assessment (per NIST SP 800-53, SP 800-26 and Central Region Supplement 05-2004) on an annual basis.
- The regional IT staff will visit field offices (WFO/RFCs) at least once every four years to perform an in-depth security audit and assessment, contingent on availability of funding.
- The CR ISSO will perform assessments under the CM-7 control.

The internal assessment tools used are:

- Continuous Monitoring Reporting – NOAA Security Assessment Report spreadsheet completed by the CR ISSO
- Central Region Oversight and Evaluation SFD Checklist – Completed by local offices and CRH IT visiting staff
- Central Region SFD IT Security Checklist - Completed by CRH IT visiting staff

External assessments are performed by outside agency assessors as part of the system Assessment and Accreditation documentation required every three years.

5.4.3 Information System Connections (CA-3): If other Government agencies to include NOAA/NWS line offices, government contractors, or private sector entities need access to the NOAA8881 system for the direct transfer of operational data or for contract work, an interconnection agreement must be signed by the SO and the other party official. The agreement contains inter-connected system names, descriptions, phone contacts, formal communication of

incidents, contingencies, configurations and personnel. Each agreement is reviewed every three (3) years or when a major change to the agreement takes place whichever is sooner. All signed agreements are kept with the CR ISSO on file. It is the responsibility of the local office to initiate the agreement using regional provided templates as shown in Appendix E.

5.4.4 Security Certification (CA-4): This security control has been withdrawn in NIST 800-53 revision 3 and incorporated in the CA-2 control.

5.4.5 Plan of Action and Milestones (CA-5): Plan of Action and Milestones (POA&M) documentation is completed to document and mitigate security weaknesses and vulnerabilities discovered during the assessments of IT system resources. The local office is required to complete and submit their local POA&M to the CR ISSO in accordance with instructions provided in the CR NOAA IT System Scan and Assessment EMRS Technical Orders.

Vulnerabilities and weaknesses that are discovered that cannot be immediately mitigated will be discussed with the System Owners and documented and tracked by the CR ISSO through the DOJ Cyber Security Assessment and Management (CSAM) web-based tool. Items in the CSAM POA&M database are reviewed monthly by the CR ISSO and appropriately updated to reflect the item status.

5.4.6 Security Accreditation (CA-6): The NOAA8881 system must go through accreditation every three years or when there is a significant change to the system as deemed by the Authorizing Official (AO).

5.4.7 Continuous Monitoring (CA-7): The CR ISSO has the responsibility to conduct continuous monitoring in accordance with the DOC Commerce Interim Technical Requirement – CITR-003. During the course of this monitoring, the CR ISSO may request security control artifacts from the local ESA and the ITO. Continuous monitoring reduces the level of effort required for the reauthorization of the IT system.

6. Operational Controls: Operational Controls are developed, implemented, and executed by people, as opposed to system technical controls, to improve the security of the system, and to ensure that the potential for significant negative impacts on the system are minimized. They describe the specific IT operations for controlling and managing processes and activates within the IT environment.

6.1 Personnel Security (PS): Personnel security controls are required to control the risk of individuals that could cause harm and disruption to IT systems. Background screening and identity verification processes are based on information access requirements and sensitivity levels established for positions.

Relevant Documents

- FIPS 201 [Personal Identity Verification \(PIV\) of Federal Employees and Contractors](#)
- NIST 800 – 35 [Guide to Information Technology Security Services](#)
- NIST 800 – 53A [Guide for Assessing the Security Controls in Federal Information Systems](#)
- NIST 800 – 73 Interfaces for Personal Identity Verification ([Part I](#), [Part II](#), [Part III](#), and

Part IV

– NIST 800 – 76 Biometric Data Specification for Personal Identity Verification

6.1.1 Personnel Security Policy and Procedures (PS-1): NOAA has established PS-1 as a Hybrid control. The compliance with DOC and NOAA personnel security policy and procedures according to the system categorization is tracked for each information system within NOAA and is part of the overall Assessment and Accreditation plan. Multiple NOAA offices provide comprehensive personnel security policies and procedures that apply to most NOAA systems. However, system owners are required to address any additional personnel security policies and procedures that go beyond the common policies and procedures to ensure protection that is equal to the risk of harm resulting from loss or damage to business or processes, if compromised. CR requires all IT system access to be terminated on the final duty day of the terminated employee and requires the return of all IT resources to include issued buildings access keys/badges and PIV cards.

6.1.2 Position Categorization (PS-2): The compliance with DOC and NOAA security policy and procedures according to position categorization is tracked for each information system within NOAA and is part of an overall Assessment and Accreditation plan. This control is designated as a NOAA common control.

6.1.3 Personnel Screening (PS-3): NOAA Workforce Force Management Office (WFMO) has implemented common personnel screening policy and procedures throughout NOAA for all personnel. This control is designated as a NOAA common control.

6.1.4 Personnel Termination (PS-4): Offices are to follow the CR Administrative Service Division (ASD) guidelines and complete the CD-126 Separation Clearance Certificate form. The office supervisors/managers will ensure that termination of employment results in:

- Local System Administrators need to deactivate all computer system accounts within 24 hours of notification of a change in user status, regardless of platform (including Active Directory, PC, network, mainframe, firewall, router, telephone, and other miscellaneous utility systems), when the account user:
 - Departs the agency voluntarily or involuntarily
 - Transfers to another operating unit within the agency
 - Is suspended or goes on long term detail
 - No longer has a legitimate business need for system access.
- E-mail notification sent to the regional email administrator, stating the termination of an employee so the account can be disabled.
- Collection of any mobile phones or other IT assets assigned to the employee.

6.1.5 Personnel Transfer (PS-5): Offices are to follow the ASD guidelines and complete the CD-126 Separation form. The office supervisors/managers will ensure that transfer of employment results in:

1. Within Central Region

- Disabling of all information system access by the local systems administrator.

- E-mail notification sent to the regional E-mail administrator stating the transfer of an employee so the account can be modified to reflect the new office information.
- Collection any mobile phones or other IT assets assigned to the employee by the local office.

2. To another region within the NWS

- Disabling of all information system access by the local systems administrator.
- E-mail notification sent to the regional E-mail administrator stating the transfer of an employee so the account can be transferred
- Collecting of any mobile phones or other IT assets assigned to the employee by CR.

6.1.6 Access Agreements (PS-6): These are individual access agreements which may include, for example, nondisclosure agreements, acceptable use agreements, and rules of behavior. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by higher authority. Re-signing an agreement is only required if there is a break in service, change in the agreement, or a higher level requirement.

6.1.7 Third-Party Personnel Security (PS-7): Third-Party providers who use and/or access NOAA IT resources are subject to all DOC, NOAA, and NWS IT security requirements.

6.1.8 Personnel Sanctions (PS-8): This is a fully implemented NOAA Common Control as formal sanctions for noncompliance is initiated by NOAA WFMO.

6.2 Physical and Environmental Protection (PE): NOAA has developed high-level Physical and Environmental Protection Policies and Procedures (PEPPP) that guide creation of locally tailored PEPPP to protect the facilities housing system resources, the system resources themselves, and the facilities used to support their operation, thus establishing PE-1 as a Hybrid control. See the latest NOAA Common Controls document for a complete description of this control.

Relevant Documents

- FIPS 199 [Standards for Security Categorization of Federal Information and Information Systems](#)
- FIPS 201 [Personal Identity Verification \(PIV\) of Federal Employees and Contractors](#)
- NIST 800 – 12 [An Introduction to Computer Security: The NIST Handbook](#)
- NIST 800 – 46 Rev 1 [Guide to Enterprise Telework and Remote Access Security](#)
- NIST 800 – 73 Interfaces for Personal Identity Verification ([Part I](#), [Part II](#), [Part III](#), and [Part IV](#))
- NIST 800-76 [Biometric Data Specification for Personal Identity Verification](#)
- NIST 800 – 78 – 3 [Cryptographic Algorithms and Key Sizes for Personal Identity Verification](#)
- NIST 800 – 100 [Information Security Handbook: A Guide for Managers](#)
- NWSI 30 – 2115 [Maintenance, Testing and Replacement of Valve-Regulated Lead Acid Batteries \(Vrla\) For Ups Applications](#)
- NOAA Common Controls
- NWSI 30 – 4102 [Facilities Design](#)

– NWSI 30 – 5101 [Facilities Physical Security](#)

6.2.1 Physical and Environmental Protection Policy and Procedures (PE-1): The following PE controls establishes and meets the DOC and NOAA requirement that system owner must document the physical and environmental protection controls which are also documented in the NOAA8881 IT SSP.

6.2.2 Physical Access Authorizations (PE-2): NOAA8881 systems are physically located in federally owned or leased facilities. Access to these areas is controlled by the SO and the MIC/HIC at each facility. DOC requires that operating units control all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and to verify individual access authorizations before granting access to the facilities.

- The Regional Director (RD) and the MIC/HICs will ensure:
 - All government employees and contractors have a valid NOAA ID before any system access is granted.
 - CR will use the procedures for issuing/re-issuing of ID Badges (Personal Identity Verification cards) established by NOAA to ensure compliance with DOC and Homeland Security requirements.
 - All CR employees are encouraged to wear / display their ID Badge at all times even if it's not required by the government facility.
 - All contractual (cleaning crews¹, etc.) having the required background check may access the computer room or other controlled areas for cleaning purposes only. Janitorial staff not having the required background check is not allowed in these controlled areas unless they are escorted.
 - All personnel authorized access to the facility where the information system resides are documented on an access list (except for those areas within the facility officially designated as publicly accessible) and removed from this list when access is no longer granted or required. The access list review requirement is annually.

6.2.3 Physical Access Control (PE-3): All areas under the scope of the NOAA8881 system will be secured with lockable doors that can be opened by a key and/or a government issued NOAA badge. The CRH computer and communication rooms are controlled access area with appropriate locking mechanisms. Field office computer rooms may remain unlocked for operational reasons, providing the access door is properly labeled as a restricted area², that outside facility doors are secure and visitor access controls (i.e. building monitoring and electronic surveillance) are functional and operating at each facility.

¹ Janitorial Employees must have the required background investigation in accordance with the Contractor Security Procedures – Janitorial Service Regional Memorandum, date December 15, 2009 - http://intra.crh.noaa.gov/crh/admin/workforce/contractor_security/janitorial_services_memo.php

² All controlled or restricted area must be properly identified. See Appendix F for sample sign.

6.2.4 Access Control for Transmission Medium (PE-4): Adequate physical protection needs to be applied to wiring closets and communication demarc areas to prevent accidental damage, disruption, or intentional physical tampering of transmission lines. Each office needs to assess and apply the necessary protective measures; e.g. locked wiring closets, locked/disconnected spare jacks, protection of cabling by conduit or trays, etc..

6.2.5 Access Control for Output Devices (PE-5): This control applies to the physical access to output devices (i.e. monitors, printers, faxes, or audio). Information system data that is considered sensitive or private must be protected from unauthorized personnel. Display medium should be located or positioned where only the authorized person having access can view or control the output access.

6.2.6 Monitoring Physical Access (PE-6): The visitor access logs in security control (PE-8) will be reviewed by the MIC/HIC monthly and retained for 3 years³, after which they may be destroyed. If there is an apparent security violation or suspicious physical access activity, the logs need to be reviewed upon the awareness of the possible violation and a copy of the log will become part of the incident response documentation.

6.2.7 Visitor Control (PE-7): DOC requires that operating units control physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible. MIC/HICs will ensure:

- All visitors will sign the entry log located in the reception area.
- All visitors are escorted and their activities monitored at all times.
- All contract workers and/or company repair personnel entering the data center or other controlled/restricted areas must show proper company credential before being allowed unescorted access into the controlled space.

6.2.8 Access Records (PE-8): NOAA8881 requires that operating units maintain a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited⁴.

6.2.9 Power Equipment and Power Cabling (PE-9): Installation of power equipment and power cabling in accordance with NWS Facilities directives and system modification procedures provide the necessary system protection to minimize damage and destruction. Below are two guidelines to meet this control:

- ❖ Power conductors shall be run in conduit per the NEC
- ❖ Data/Phone conductors are considered "protected" if they are in conduit, above the ceiling, below the floor or within the footprint of the equipment rack.

³ General Records Schedule (GRS) 24 IT Operations and Management Records

⁴ May be omitted in a small single organizational facility such as a WFO/RFC

6.2.10 Emergency Shutoff (PE-10): The emergency shutoff control for WFO and RFC facilities is the building's main circuit breaker located in the main facility's electrical room. Non WFO /RFC offices need to ensure that there is an emergency shutoff device for the building and document its location in the local station duty manual (SDM).

6.2.11 Emergency Power (PE-11): NOAA8881 system requires that:

- Operating units provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
- Long term alternate power supply is available and sufficient to maintain minimum operation of the system during an extended loss of the primary power source.
- UPS batteries are tested at least annually by contractor or CRH personnel.
- Full backup power system tests are performed at least monthly.

6.2.12 Emergency Lighting (PE-12): Any lighting in the building that is set to run on a back-up system (i.e. generator or battery) is considered emergency lighting. All facilities need to test routinely and document the manner in which the control is implemented.

6.2.13 Fire Protection (PE-13): At a minimum, every facility will have an adequate number of fire extinguishers to protect the facility. Six extinguishers is the normal number for a typical WFO facility. Offices may elect to have other fire protection controls in place such as smoke detectors, sprinkler systems, and fixed fire hoses. Facilities with WAN/LAN infrastructure that are not staffed 24/7 need to employ an automatic notification of any activation to an emergency responder organization. All fire protection controls need to be locally documented to include the manner in which the control is implemented, the location within the facility, and dates controls tested.

6.2.14 Temperature and Humidity Controls (PE-14): Facilities with critical WAN/LAN infrastructure (i.e. CRH, WFO and RFC) need to have temperature and humidity controls in their computer rooms. Annual maintenance needs to be completed and documented for these controls.

6.2.15 Water Damage Protection (PE-15): Facilities with critical WAN/LAN infrastructure (i.e. CRH, WFO and RFC) need to have a master water shutoff valve that is tested at least annually. The location of the shutoff valve needs to be locally documented and accessible to office personnel who would need to use it in case of a water system failure.

6.2.16 Delivery and Removal (PE-16): Delivery and removal of IT system components must be controlled. Deliver and pickup of items beyond the public access of the facility's front door area will require delivery/pickup persons to sign in and be escorted per PE-7 and PE-8 controls.

6.2.17 Alternate Work Site (PE-17): An alternate work site is defined as any site where CR employees perform work-related functions such as an official alternate backup location, telework location, or any commercial facility where NOAA8881 IT information system assets and/or agency data information is used. System controls that are in place at the primary work site

should be available at the alternate work location. A 24/7 telephone number to the local office IT security staff needs to be given to all employees working at an alternate location in the event of an on-site IT security problem. At field offices, this normally would be the office's operations telephone number, and at CRH, this will be the Central Region Call Center telephone number.

6.2.18 Location of Information System Components (PE-18): The facility's construction, building electrical layout, and configuration management of the system determines location of IT systems components. The physical and environmental risks within a facility must be considered in the location and re-location of system components. These risks need to be evaluated and minimized to protect the system.

6.2.19 Information Leakage (PE-19): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

6.3 Contingency Planning (CP): NOAA8881 will follow the DOC and NOAA policies and procedures for contingency planning. The Contingency Planning functions will follow the management procedures described below.

Relevant Documents

- FIPS 199 [Standards for Security Categorization of Federal Information and Information Systems](#)
- FIPS 140 – 2 [Security requirements for Cryptographic Modules](#)
- NIST 800 – 12 [An Introduction to Computer Security](#)
- NIST 800 – 16 Rev. 1 [Information Security Training Requirements: A Role- and Performance-Based Model](#)
- NIST 800 – 34 Rev. 1 [Contingency Planning Guide for Information Technology Systems](#)
- NIST 800 – 50 [Building an Information Technology Security Awareness and Training Program](#)
- NIST 800 – 84 [Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](#)

6.3.1 Contingency Planning Policy and Procedures (CP-1): NOAA has established CP-1 as a common control in which all system owners are required to comply with the policies and implementation procedures of these policies. The compliance with these policies and procedures according to the system categorization are tracked for each information system within NOAA and are part of an overall Assessment and Accreditation (A&A) plan. It is the responsibility of the SO to ensure that IT Contingency Plan documents are developed, IT Contingency Exercises are established, conducted, and the results documented in accordance with the plan.

6.3.2 Contingency Plan (CP-2): NOAA8881 will follow the DOC and NOAA policies and procedures for developing, maintaining, and exercising the IT contingency plan using the guidance in National Institute of Standards and Technology Special Publication (NIST SP) 800-34. The IT Contingency Plan will be annually reviewed and updated, as necessary, as part of the Continuous Monitoring of the system plans and procedures. CR requires that the operating units review the contingency plan for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. Any changes to personnel, addresses, or contact information that affect the

designated teams should be updated promptly and submitted to the CR ISSO.

6.3.3 Contingency Training (CP-3): NOAA8881 will follow the DOC and NOAA policies and procedures for training, testing, and exercising the IT contingency plan. The CR ISSO will ensure the annual training and testing and exercises are accomplished as part of the Continuous Monitoring annual plan updates. IT Contingency Plan response team members will be trained in their duties upon initial assignment to the role and at least annually thereafter. The MIC/HIC will log training on a locally developed form to include individual name, position, and dates of training and provide it to the CR ISSO. The CR ISSO will use the scenarios from the IT Contingency Plan Test Plan to conduct testing and exercises at least annually. The results will be recorded, documented, and filed as an artifact to show control compliance.

6.3.4 Contingency Plan Testing and Exercises (CP-4): Tabletop and functional type testing and exercises are required annually for the following four IT business critical services:

- Telephone
- Network
- Web
- Desktop

All offices need to submit a report to the System Owner (SFD Chief) which describes the test environment (e.g. scenario, type of testing, services/functions tested and/or activated, date performed, etc.) that is exercised. The report also needs to include any areas of weaknesses discovered along with recommendations for improving in those areas. Actual restoration of failed IT events is preferred over exercises, but they must be documented in accordance with this control to be counted towards the annual requirement.

Additional information concerning contingency plan testing can be found in the CR WAN/LAN IT Contingency Test Plan.

6.3.5 Contingency Plan Update (CP-5): This security control has been withdrawn in NIST 800-53 revision 3 and incorporated in the CP-2 control.

6.3.6 Alternate Storage Sites (CP-6): Each office is to identify an alternate storage site for their system backup media. The geographical separation between the primary site and alternate site is to be determined by each CR office based on the restoration times for criteria IT resources. Three additional factors also need to be considered in selecting a site: potential accessibility in the event of an area-wide disaster, accessible hours, and physical security. Alternate storage site information is to be placed in the office IT CP Appendix document and provided to the CR ISSO.

6.3.7 Alternate Processing Site (CP-7): An alternate processing site is to be identified in the office IT CP Appendix document and provided to the CR ISSO.

6.3.8 Telecommunications Services (CP-8): Alternate telecommunication service arrangements are described in the NOAA8881 system IT Contingency Plan. Priority and alternate service provisions are included in the telecommunications agreements within the System and managed by the CR Communication Manager. For short-term disruptions, CR

offices will use backup cellular phones, VSAT, and radios where installed. For long-term disruptions, responsibilities for telecommunications service will shift to the service backup location.

6.3.9 Information System Backup (CP-9): DOC requires that operating units to conduct backups of user-level and system-level information (including system state information) contained in the information system, set back-up frequency schedules, and store backup information at an appropriately secured location. This includes, but not limited to, all Active Directory servers, OS core files, registry, configuration files, profiles and user data.

The backup frequency schedule of a device or computer is based on its criticality within the IT infrastructure. Normally, network type devices which provide critical business functions would be considered critical assets that would need to be backed up on a weekly frequency schedule. The frequency backup schedule for non-critical assets will be the responsibility of the local SM. CR requires that information systems test backup information media quarterly to ensure media reliability and information integrity. This includes reloading data from the backup media. Offices may use actual restored events to meet this requirement, providing they document the event and capture the elements defined in the CR IT Contingency Test Plan document.

There are a number of basic factors that must be considered and included in an office backup plan. Offices should consider the below factors in order to achieve and maintain an effective critical asset backup program.

1. **Backup Windows:** Because of the large number of files that require backup, the impact of backups on file server performance must be considered.
 - a. A full backup should only occur after business hours.
 - b. Incremental backups are left to the discretion of the local IT staff.
2. **Backup Schedule:**
 - a. Full backups are performed at least weekly, with large file sets offset so as not to overrun the backup window.
 - b. Incremental backups are made nightly on weekdays and on weekends if necessary.
3. **Backup Retention:**
 - a. Full backups will be retained until the next full backup is available to restore the system.
 - b. Incremental backups will be retained until at least the next full backup is completed.
4. **Tape and Tape Drive Maintenance:**
 - a. Cleaning and storage tapes will not be used in excess of the manufacturer's recommended use schedule.

- b. Tape drives will be cleaned according to the manufacturer's recommended cleaning interval.

5. Media Sanitization:

- a. Retired media⁵ and configurable network devices will be sanitized before disposal using methods designed to meet DOC and NOAA requirements.
- b. Sanitization records for the above devices will be kept locally for 3 years after the component is deleted from the Sunflower system.

6.3.10 Information System Recovery and Reconstitution (CP-10): Recovery priority and goals are covered in the IT CP. Recovery and reconstitution is included as part of the testing process. In the event of a loss of critical data, local backups are used as the primary restoration method. If a restore of data is needed and there is a catastrophic failure at the primary site, then backups are regenerated from the off-site backups. Configuration checklists and/or images along with security patches will be applied to all restored resources to ensure the security posture of the system. Restoration procedures for non-standard COTs hardware/software are documented locally, either through the Station Duty Manual or an office restoration plan, to ensure that restored hardware and software are restored to its proper configuration. The NWS and CR require at least annual testing and documenting of the recovery and reconstitution controls per the current NOAA8881 IT CP Test Plan-Results document.

6.4 Configuration Management (CM): Configuration Management establishes and maintains consistency of an IT system's performance, functionality, and physical attributes based on its design and operational requirements throughout its life cycle. It ensures that changes made to hardware, software, firmware, and documentation are consistent with applicable IT security laws, Executive Orders, directives and policies. It is a managed approach to maintain the security posture of an IT system.

Relevant Documents

- NIST 800 – 12 [An Introduction to Computer Security](#)
- NIST 800 – 53 Rev. 3 [Recommended Security Controls for Federal Information Systems](#)
- NIST 800 – 70 Rev. 2 [National Checklist Program for IT Products: Guidelines for Checklist Users and Developers](#)
- NIST 800 – 100 [Information Security Handbook: A Guide for Managers](#)
- NIST 800 – 128 [Guide for Security-Focused Configuration Management of Information Systems](#)
- NWSI 30 – 1203 [Configuration Management for Operational Systems](#)
- NWSI 60 – 702 [Management, Operational and Technical Controls](#)
- CR Supplement 01– 2005 [Central Region Configuration Management for IT Systems](#)
- Central Region IT Security Program *Configuration Management Plan*

6.4.1 Configuration Management Policy and Procedures (CM-1): NOAA has established CM-1 as a common control in which all system owners are required to comply with the policies and implementation procedures of these policies. Regional CM is addressed in the current Central

⁵ Includes media in fax, copiers, or printers

Region Supplement – Central Region Change Management for Information Technology (IT) Systems.

6.4.2 Baseline Configuration (CM-2): All IT system components used within the NOAA8881 system will have baseline configuration documentation that is updated as necessary to reflect changes within the component’s life cycle. Central Region IT system components (i.e. Operating Systems, Cellwatch, NA systems, file servers, network devices and structure, etc.) under Central Region CM need to maintain its regional configuration baseline. Request for change of national or regional CM items must be submitted in accordance with NWS and CR CM policy. Offices should develop local CM policy and procedures to cover local configuration items within their office.

The centralized management of the OPSNET, formerly known as NOAANET, requires that all Wide Area Networks and Local Area Networks only have approved firewalls and routable devices in order to maintain network connection integrity. Thus, the lowest organizational level authorized to implement and manage firewalls and routable device is the region as authorized by System Owner and OPSNET. The only routable device that local offices may have is a wireless access point, providing it meets the DOC/NOAA and CR policies under control AC-18.

Baseline Configuration responsibilities:

- CR ISSO will
 - Develop, review and approve all security configuration checklists.
 - Allow for modifications to take into account local policies and needs.
 - Maintain a repository of checklists for dissemination throughout CR.
- System Owner and Security Managers will ensure
 - Security settings use the most restrictive mode consistent with operational requirements.
 - System configuration checklists are reviewed, and used to certify all systems before they can be connected to the network.
 - Security configuration checklists provide
 - Instructions for configuring an information technology (IT) product to a baseline level of security
 - Scripts, templates, and pointers to patches, updates or firmware upgrades as appropriate.
 - Administrative practices as well as security settings for an IT product, e.g., changing default passwords and applying new patches.
- System Administrators will
 - Ensure system configurations are tested before applying to operational system devices
 - Certify a system by using an appropriate checklist to ensure that proper security features or settings are applied to the system before system is put into operational use.

- Validate the security posture of a system using a vulnerability assessment tool approved by NOAA

6.4.3 Configuration Change Control (CM-3): All CR configuration managed systems will follow the CR configuration management supplement document relating to change control. All moderate and major changes require written requests to be submitted to the CR Change Control Board (CCB) for review, testing approval, and implementation. No changes shall be done to any of these systems without first having approval from the CR CCB. The Operations and Service Improvement Process (OSIP) is the configuration change control for NWS.

6.4.4 Security Impact Analysis (CM-4): The primary responsibility to analyze changes in configuration lies with the designated IT staff within CRH and with the local SAs. Analyzing security change occurs during regional IT visits, continuous monitoring (CM-7) activities, and local office self-assessments. Pre-configuration and post-configuration evaluations must occur to ensure the security posture of the system.

6.4.5 Access Restrictions for Change (CM-5): Access restriction changes will be submitted to the appropriate office Security Manager for review and approval. Upon approval, the office SA will make the appropriate changes as approved. If the changes cannot be changed locally due to higher level technical controls, the local SA will need to elevate the request to the appropriate regional SA.

6.4.6 Configuration Settings (CM-6): Configuration security settings of components and products within the NOAA8881 system will follow the established mandatory configuration settings, to the most restrictive mode consistent with operational requirements. Automated mechanisms are used to centrally manage, apply, and verify these configuration settings. There will be a restrictive group policy based on DOC/NOAA/NWS IT Security Policy that will be propagated from the CR active directory root server to all desktops in CR. Only qualified SAs and appropriately authorized individuals have physical and logical access to these automated mechanisms and tools. These root group policies will not be modified from their original settings. The local office can expand on these restrictions, but cannot minimize them for local group policies. Additional group policy settings have been developed at CRH based on USGCB, DISA, CIS and NSA STIGS. Configuration settings and control checklists are required to document and ensure that devices follow Federal “Best Practices” and NIST standards. See the current NOAA8881 Configuration Management Plan (CMP) in the SSP documentation for additional guidance and details.

6.4.7 Least Functionality (CM-7): All CR systems will apply the rule of least functionality to all IT devices. Some of the functions and services, provided by default, may not be necessary to support essential organizational requirements. Offices need to ensure that all unnecessary functions are disabled or removed from the systems before placing the system into the operational environment. Least functionality settings need to be reviewed annually in order to preserve the security posture from removed system legacy devices that no longer require certain functions and services open.

6.4.8 Information System Component Inventory (CM-8): An Information System Component Inventory is required and will be taken at least annually or whenever there is a significant change in inventory. The determination as to whether there is a significant change is the responsibility

of the CR ISSO. The inventory covers both hardware devices and software licensing. Since the inventory needs to accurately reflect the state of the system at a given time, automated tools such as Microsoft System Center Configuration Manager (SCCM), SpiceWorks, etc. are recommended to capture the data. Below are the required data fields for each inventory.

Hardware inventory will include the minimum fields for each device:

- ❖ Computer Name
- ❖ Operating System
- ❖ Service Pack Level
- ❖ Serial number
- ❖ Asset Tag (CD barcode)
- ❖ Manufacturer
- ❖ Model

Software inventory will include the minimum fields for each software title:

- ❖ Software Program
- ❖ Software Version
- ❖ Authorized License quantity
- ❖ Current usage quantity

6.4.9 Configuration Management Plan (CM-9): A system Configuration Management Plan (CMP) establishes the process to manage and document the effects of change or differences in IT configurations. The document is intended to be a living document, and consequently, it should be placed under CM and the respective changes managed according to CM policies referenced.

6.5 System Maintenance (MA): DOC requires that information system maintenance policy and procedures are established for all IT systems consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Relevant Documents

- FIPS 140 – 2 [Security requirements for Cryptographic Modules](#)
- NIST SP 800 – 12 [An Introduction to Computer Security](#)
- NIST SP 800 – 37 [Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)
- NIST SP 800 – 40 Ver. 2 [Creating a Patch and Vulnerability Management Program](#)
- NIST SP 800 – 53 Rev. 3 [Recommended Security Controls for Federal Information Systems](#)
- NIST SP 800 – 63 [Electronic Authentication Guideline](#)
- NIST SP 800 – 88 Rev. 1 [Guidelines for Media Sanitization](#)
- NIST SP 800 – 100 [Information Security Handbook: A Guide for Managers](#)
- DOC ITSP [Information Technology Security Program Policy](#)

6.5.1 System Maintenance Policy and Procedures (MA-1): NOAA has established MA-1 as a hybrid control in which all system owners are required to comply with the policies and implementation procedures for this control. The System Owner (SO) is responsible for

implementing a System Maintenance policy for their IT System and will use it to assess the MA security control. The NOAA8881 System Maintenance policy is as follows:

Regular and routine maintenance of the IT system is important in order to ensure the system's availability. The purpose for the policy and procedures is designed to support, promote, and implement the below maintenance objectives:

1. Ensure IT hardware is properly maintained and in good working condition;
2. Ensure IT related software, operating systems, and system environments are in good working order;
3. Assure that the status of these systems meets existing organizational, industry, and other accepted "best practices" as they relate to operational and security requirements;
4. Leverage the program as a tool to enhance overall security posture in relation to the Confidentiality, Integrity, and Availability (CIA) model.

In order to achieve the above objectives, maintenance of the system will be placed into the following three categories:

1. **Preventive Maintenance:** Tasks performed on a system to correct or prevent degradation of performance, and to correct other minor issues prior to them becoming larger problems. For many systems, this would include tasks such as disk defragmentation, file system cleanup, minor physical cleaning, anti-virus scanning, and backups.
2. **Scheduled Maintenance:** This is a system of performing on-going, routine maintenance procedures at periodic scheduled intervals. The purpose behind scheduling routine maintenance tasks such as upgrades, patches, cleaning, and installs is to provide a measure of predictability and to move any expected downtime to off-peak hours. Maintenance of this sort is often required for servers and other infrastructure systems, and is usually the responsibility of internal IT support personnel.
3. **Corrective Maintenance:** The system is broken, and must be repaired or replaced. Corrective maintenance can range from a simple component swap to replacement of an entire system. Corrective maintenance may be performed by internal maintenance personnel, outside vendors, or a combination of either.

The CRH IT Branch and each MIC/HIC is responsible for developing their local procedures to support the MA objectives for their respective offices. Only system administrators are allowed to perform system maintenance. However, some of the PM tasks of disk defragmentation and file system clean on desktops and laptops may be assigned as a user level function.

6.5.2 **Controlled Maintenance (MA-2):** Scheduled and routine maintenance on the NOAA8881 IT system or its component will utilize the principles of controlled maintenance to ensure that the system obtains the most efficient utilization of labor, equipment, and material. Thus, offices need to inventory, inspect, plan, and schedule IT equipment maintenance, and perform an analysis to ensure it is meeting the objective of this control, which is, to see increase productivity, savings, and a standard of achieved maintenance. Offices are encouraged to use the Engineering Management Reporting System (EMRS) calendar to schedule controlled

maintenance.

6.5.3 Maintenance Tools (MA-3): Maintenance tools refer to any COTS diagnostic hardware tool or appliance, any COTS diagnostic software tool, or any downloaded open source diagnostic software tool. The use of vulnerability scanners, spyware removal tools, registry cleaners, etc. needs approval from CRH prior to using to determine if any system information is being sent unaware from a system to an unauthorized destination.

- CR offices will use the standard NOAA approved enterprise level tools for scanning and anti-virus protection.
- CRH will develop, maintain, monitor, and approve the use of all maintenance tools
- System Administrators will:
 - Ensure tools are used only by authorized personnel.
 - Inspect all maintenance tools brought into facility for improper modifications.
 - Check media containing diagnostic test programs for malicious code before it is used on system.
 - Check all maintenance equipment/tools (i.e. Network Analyzers with memory, etc.) able to retain information and, if appropriate, sanitize them to ensure no organizational information is retained in the equipment memory.
 - Security or hacker tools will not be installed on any IT system unless authorization is provided by the CR ISSO.

6.5.4 Non-Local Maintenance (MA-4): Non-Local maintenance and diagnostic activities are allowed within the trusted network, using the appropriate secure network protocols and established identification and authentication techniques. Non-local remote maintenance is allowed from outside the trusted network only through the CRH controlled VPN appliance and NEVER from public-access equipment per the remote user access agreement. There will be no direct remote connection into boundary edge devices. Remote root access is not permitted on any device. Administrator's will use their normal user account and then switch to their elevated privileged account.

6.5.5 Maintenance Personnel (MA-5): Only qualified maintenance personnel are authorized to perform maintenance on the NOAA881 IT system. The overall determination of personnel qualifications is the responsible of the SM with input from the ESA. Maintenance personnel, whether internal or external, will be limited to only those areas within the system that requires maintenance. If technical controls cannot be used to limit system access, a CR staff person with appropriate access authorization must supervise the maintenance personnel during the performance of maintenance activities on the system. In the event external personnel (contract or outside of CR) are utilized for system maintenance, the conditions of access should be documented in a statement of work, memorandum of agreement, Service Level Agreement, or other contractual documents to include PS-6 Access Agreements. These documents should be maintained at least three years beyond the completion/termination of the external services contract.

6.5.6 Timely Maintenance (MA-6): The IT System critical capabilities are defined by the system owner in the Business Impact Analysis (BIA) Appendix F of the SSP. Refer to the resource outage impact and allowable outage time table in the BIA document.

6.6 System and Information Integrity (SI): System and information integrity procedures provide controls to protect data from accidental or malicious alteration or destruction and to assure users that the information meets their quality and reliability expectations.

Relevant Documents

- FIPS 199 [Standards for Security Categorization of Federal Information and Information Systems](#)
- NIST SP 800 – 37 [Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)
- NIST SP 800 – 40 ver. 2 [Creating a Patch and Vulnerability Management Program](#)
- NIST SP 800-61 Rev 1 [Computer Security Incident Handling Guide](#)
- NIST SP 800 – 45 Ver. 2 [Guidelines on Electronic Mail Security](#)
- NIST SP 800-83 [Guide to Malware Incident Prevention and Handling](#)
- NIST SP 800-92 [Guide to Computer Security Log Management](#)
- NIST SP 800-94 [Guide to Intrusion Detection and Prevention Systems](#)
- DOC CITR-002 [Safeguarding Data on Foreign Travel](#)
- NOAA IT [Security Manual 212-1302 \(V4.2\)](#)

6.6.1 System and Information Integrity Policy and Procedures (SI-1): NOAA has established SI-1 as a common control in which all system owners are required to comply with the policies and implementation procedures of these policies. The following SI controls establish the policy and procedures to comply and be consistent with the relevant documents above.

6.6.2 Flaw Remediation (SI-2): Flaw remediation is required for all information system components containing proprietary or open source software to protect the system or vulnerabilities or potential vulnerabilities resulting from flaws. Proprietary software can be found in either commercial/government off-the-shelf information technology component products or in custom-developed applications. System Administrators need to identify, correct, and share information on flaws and mitigation actions with the other regional personnel who may be affected by the same flaws.

6.6.3 Malicious Code Protection (SI-3): The NOAA8881 system employs virus protection mechanisms at critical information system entry and exit points, at workstations, servers, and on mobile computing devices. The NOAA enterprise solution is the McAfee Enterprise Product Suite which includes antivirus for Windows, Linux, and MAC platforms and other endpoint security solutions. Active directory GPOs and E-Policy Orchestrator will ensure automatic downloads and audit tracking of antivirus activities for all domain computers. If performance is an issue for Linux platforms, the open source program ClamAV may be used in place of the McAfee LinuxShield product, but it must be enabled and configured for daily signature database updates.

Mobile computing devices and media that have been outside the control of NWS IT Security controls are deemed ‘at-risk assets’ that must be thoroughly inspected and scanned for malicious code. The following guidance addresses these concerns and provides additional procedural details.

NOAA/NWS Government - Owned Computing Assets – Foreign Travel

All government-owned assets (i.e. laptops, Blackberry PDAs, USB Thumbdrives, CD/DVD disk, etc.) must follow the Commerce Information Technology Requirement (CITR) guidance in CITR-002, Safeguarding Data on Foreign Travel.

All Computing Devices/ Removable Media – IT staff available

Any computing device and/or removable media taken out of the office and exposed to any non-government or public network needs to be thoroughly scanned for software viruses and other malicious unwanted code. The IT staff must perform a full OnDemand scan of the computer/removable media on a system that is not connected to an NWS network, using the McAfee Virus scanner with the current vendor dat files. This can be accomplished as follows.

- ❖ Inspect and update the McAfee dat files
- ❖ Disable network connection in the operating system or unplug the computer from the network.
- ❖ Run a full OnDemand scan on the computer and/or the removable device.
- ❖ Upon a clean scan, the computer /removable media can be reconnected to the network, or if a virus is found, a full scan must be run on both the device and computer to remove the virus and the incident must be reported on a NOAA 47-43 form.

NOTE: If the AV scanner detected any viruses/malicious, the computer system/removable media may not be reconnected to an NWS network even if the scanner stated the virus was deleted or cleaned until the IT staff has taken all the necessary actions requested by the N-CIRT.

All Computing Devices/ Removable Media – No IT staff available

As stated in the above paragraph, any computing device and/or removable media taken out of the office and exposed to any non-government or public network needs to be thoroughly scanned for software viruses and other malicious unwanted code. If IT staff is not available to perform a virus scan (such as at a conference, off-duty, etc.), any employee with the technical knowledge and background may scan a computer /removable media, providing its usage is deemed mission critical and the below steps are followed:

- ❖ Ensure the laptop, computer and/or removable media is not connected from any NWS network, by unplugging the cable or disabling the network connection.
- ❖ Inspect and ensure the McAfee dat file is up to date. The current vendor dat file may need to be downloaded and installed on controlled portable media and installed on unit.
- ❖ Run a full OnDemand scan on the computer and/or the removable device.
- ❖ Once the virus scan has been completed and there were no detected viruses/malicious code, the computer system / removable device may be used and connected to the network

NOTE: If the AV scanner detects any viruses/malicious, the computer system/removable media may not be reconnected to an NWS network even if the scanner stated the virus was deleted or cleaned until it is determined by the IT staff that device/media is safe.

6.6.4 Information System Monitoring (SI-4): NOAA has established SI-4 as a hybrid control in which all system owners are required to comply with the policies and implementation procedures of these policies. As such, DOC requires that operating units employ tools and techniques to monitor events on Moderate- and High-impact information systems, detect attacks, and provide identification of unauthorized use of the system.

The NOAA8881 system will supplement this control with the use of the tools like: Zabbix, Nagios, SNORT (SNORBY) and Logwatch. The responsibility for deploying these tools lies with the NWS CRH IT branch for regional managed devices and with the local ESA for locally managed devices that require monitoring. Log data from these devices will be archived on a separate server. Software IDS tools fall under the SA-7 control and as such require approval authorization provided by the CR ISSO prior to being installed and implemented.

6.6.5 Security Alerts, Advisories, and Directives (SI-5): The NOAA8881 System ISSO receives security alerts, advisories, and directives from a number of different sources to include but not limited to the following: OMB, DOC, NOAA, NWS, US-CERT, N-CIRT, NWS CIO, Microsoft, and McAfee. These alerts and advisories are reviewed and appropriately sent to local IT personnel for review and/or actions. Offices are encouraged also to forward other security information that they may receive from reliable sources to the CR ISSO.

6.6.6 Security Functionality Verification (SI-6): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

6.6.7 Software and Information Integrity (SI-7): The integrity of software and information is protected through the use of limiting access and privilege to system administrators and to those having a need to load and maintain software and information within the system. Only authorized enterprise software and authorized use of other third party /open source software is allowed. Cryptographic hashes methods like SHA-1, SHA-2, and MD5 checksum need to be used to validate the integrity of the software file. The access and changes to protected information databases are restricted to the database managers and others individuals who have a need for the data.

6.6.8 Spam Protection (SI-8): Spam protection software is used on internal computers through the use of enterprise level end point protection software and invoking the built-in Commercial off the shelf (COTS) functionality with the Windows Operating System software. Mail servers and government mobile computing devices are outside the NOAA8881 systems and are managed by another NOAA IT system. Although technical controls aid in the detection and filtering of spam and spyware attacks, all users must remain vigilant to these threats to further protect the system.

6.6.9 Information Input Restrictions (SI-9): The least privilege concept in the AC-6 control along with using role-based access technical and application control mechanisms restrict information input by unauthorized users. The restrictions apply to both data and system information.

6.6.10 Information Input Validation (SI-10): Information input validation is achieved with the implementation of configuration management for system devices and development of application

standards such as input accuracy and validation of syntax of configuration files, scripts, databases, and web pages.

6.6.11 Error Handling (SI-11): The notification messages from COTS and custom applications used within the system provides user notifications when errors are discovered in input, accuracy and/or validation controls within the systems. The error handling alerts in some cases are real-time alerts, alerting a user of a wrong password or an SA of a system malfunction or system alerts that are logged and available to only authorized SAs for analysis. Error handling for custom developed applications needs to be properly documented and maintained across the life cycle of the system.

6.6.12 Information Output Handling and Retention (SI-12): The information output handling and retention of system generated and/or stored information will be consistent with the guidance and directive of the NOAA Records Management Policy which incorporates the policy and standards set forth in the General Records Schedules. Any system output handling and retention not specified in this supplement will follow appropriate guidance from the CR Administrative Services Division (ASD), NOAA Records Management Guide, or the appropriate General Record Schedule.

6.6.13 Predictable Failure Prevention (SI-13): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

6.7 Media Protection (MP): All media used within the system will employ an adequate security level commensurate to its classification sensitivity throughout the media's life cycle. The controls must provide protection in the handling, storing, and destruction of the media whether it be paper hardcopies or electronic softcopies. Protection controls must specifically address media authorized access, media safeguards in storage and in transport, and the destruction of the media when no longer required.

Relevant Documents

- FIPS 199 [Standards for Security Categorization of Federal Information and Information Systems](#)
- NIST SP 800 – 12 [An Introduction to Computer Security](#)
- NIST SP 800 – 37 [Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)
- NIST SP 800-53 [Recommended Security Controls for Federal Information Systems](#)
- NIST SP 800 – 56A [Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography](#)
- NIST SP 800 – 57 [Recommendation for Key Management Part I, Part II, and Part III](#)
- NIST SP 800 – 60 rev.1 [Guide for Mapping Types of Information and Information Systems to Security Categories: \(2 Volumes\) - Volume 1: Guide Volume 2: Appendices](#)
- NIST SP 800 – 88 Rev. 1 [Guidelines for Media Sanitization](#)
- NIST SP 800 – 100 [Information Security Handbook: A Guide for Managers](#)
- NIST SP 800 – 111 [Guide to Storage Encryption Technologies for End User Devices](#)
- DOC ITSP [Information Technology Security Program Policy](#)
- DOC CITR-002 [Safeguarding Data on Foreign Travel](#)

– DOC CITR-005 Removable Media Devices

6.7.1 Media Protection Policy and Procedures (MP-1): To ensure compliance with DOC and NOAA procedures, the following media protection controls will be considered and implemented as applicable.

- ❖ Access controls
 - Exercise least privilege concept (user has a need to access)
 - Ensure only authorized users have access (maintain access lists)
 - Ensure proper output control (read-only versus read/print)
- ❖ Safeguard controls
 - Accurate categorization and labeling of media (determine information sensitivity)
 - Protect removable media⁶ with regionally approved solutions (i.e. McAfee Endpoint Encryption for Files and Folders, McAfee Data Loss Protection (DLP, etc.)
 - Secure storage (encryption, locked cabinets/safes, etc.)
 - Secure media transport (authorized personnel, recipient verification, use approved media protection methods and procedures)
- ❖ Destruction
 - Consider all copyright and licensing issues of COT software before destroying/disposing (does EULA allow transfers or must it be destroyed)
 - Sanitization before leaving office control or re-cycling (determine whether to physically destroy, use system removal steps or use appropriate media sanitization software per NIST SP 800-88)

Documentation and auditing the above safeguards is a local management requirement.

6.7.2 Media Access (MP-2): Media access of the IT Information system will follow the same strictness as any other information access within the region. Access is granted and restricted on a ‘need to know’ basis and applies to both non-digital (e.g., paper, microfilm) and digital media (e.g., hard drives, thumb drives, diskettes, digital video tape, CD/DVD disk, etc.). Automated mechanisms to restrict access will be used as applicable (i.e. system technical controls like the McAfee Endpoint Encryption for Files and Folders to restrict unauthorized access, password protected devices and documents, etc.). Any media that is restricted needs to have a listing of authorized individuals approved by the local security manager.

6.7.3 Media Marking (MP-3): Media that is not to be shared in the public domain (i.e. internal use only, For Official Use Only (FOUO), Controlled Unclassified Information (CUI) or classified information) must be properly labeled and controlled to protect the information and the agency. Labeling of such media can be included in the document in the header and/or footer areas or on the outside of the media label.

6.7.4 Media Storage (MP-4): Storage of media must meet the security rigors commensurate to

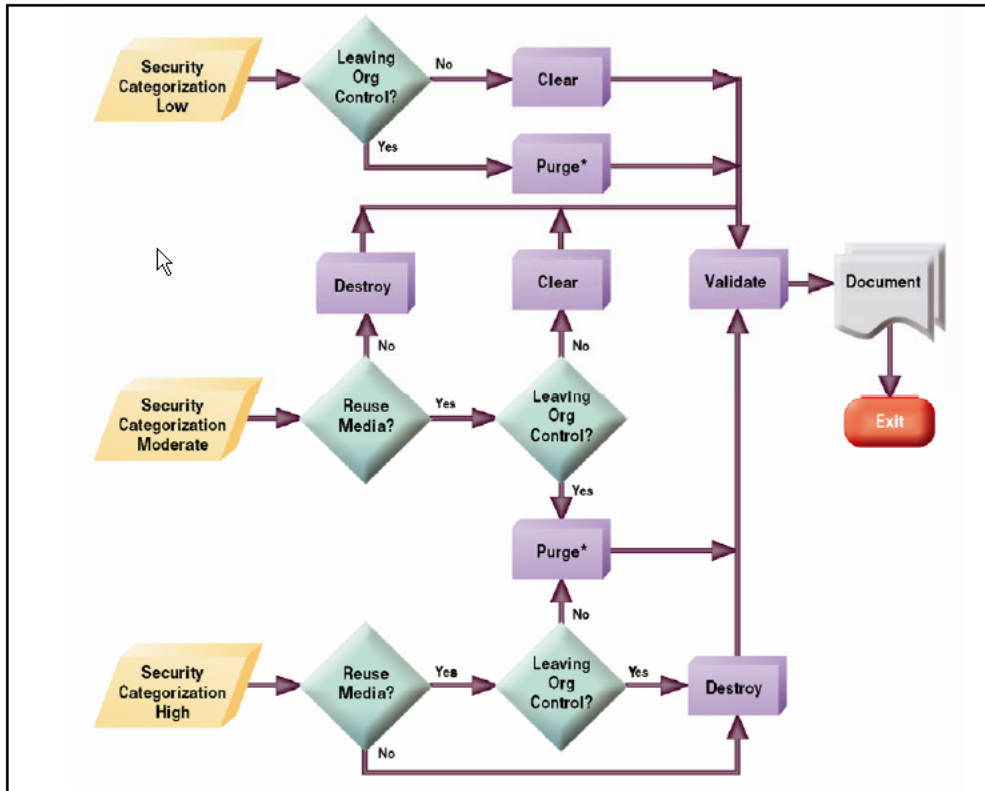
⁶ Media used for system admin duties and other approved media by System Owner are exempt

the highest information sensitivity level stored on the media. For example, fewer protection measures are needed for media containing public released weather information or public domain data. However, controlled unclassified information (CUI) and PII information requires stricter media storage measures. There is an exception to this media storage rule when the portable media leaves the United States. DOC Interim Information Technology Require – 002 (CITR-002), Safeguarding Data While on Foreign Travel, recommends the media be encrypted with FIPS140-2 validated encryption.

6.7.5 Media Transport (MP-5): Protection of digital and non-digital media transported outside controlled areas will be commensurate to the sensitivity of the media being transported. Media which contains sensitive but unclassified information (e.g. PII, network, etc.) or higher must be in the possession of a NOAA employee or NOAA contract employee who has been properly screened per the PS-3 Personnel Screening control.

Offices must keep document logs which records and tracks all transportation activities to include pickup, receipt, transfer date and location, identification of media (i.e. paper, drives, tapes, etc.) and initials of courier. The logs will be retained for two years, after which time, they may be destroyed.

6.7.6 Media Sanitization (MP-6): In order to comply with DOC policy to track, document and verify sanitization activities, Central Region offices will need to document sanitization activities for all assets that are excess and/or donated. Also, the level of confidentiality of data stored on the media is a significant factor in determining whether to reuse media or the method of sanitization. The below diagram taken from NIST 800-88 rev1 shows the appropriate action to take for the specific security category. Offices need to refer to NIST 800-88 for guidance on identifying options for sanitizing media or devices with internal media storage. The retention of destruction worksheets is three years based [General Records Schedule \(GRS\)4](#) guidelines, after which time, they may be destroyed. A sample of a destruction worksheet is provided in Appendix B.



6.8 Incident Response (IR): Incident response is an organized approach to addressing and managing the aftermath of a security breach or an attack which are commonly referred to incidences. An IT Incident Response Plan (IRP) includes the policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs.

Relevant Documents

- NIST SP 800 – 16 Rev. 1 [Information Security Training Requirements: A Role- and Performance-Based Model](#)
- NIST SP 800 – 37 [Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)
- NIST SP 800 – 50 [Building an Information Technology Security Awareness and Training Program](#)
- NIST SP 800 – 53 [Recommended Security Controls for Federal Information Systems](#)
- NIST SP 800 – 61Rev. 1 [Computer Security Incident Handling Guide](#)
- NIST SP 800 – 84 [Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](#)
- NIST SP 800 – 115 [Technical Guide to Information Security Testing and Assessment](#)
- DOC ITSP [Information Technology Security Program Policy](#)
- NOAA [Incident Response Policy](#)

6.8.1 Incident Response Policy and Procedures (IR-1): NOAA has established IR-1 as a common control. The compliance with DOC and NOAA incident response policy and procedures according to the system categorization is tracked for each information system within

NOAA using the NOAA 47-43 web-based IT Security Incident Reporting form. 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.

6.8.2 Incident Response Training (IR-2): NOAA has established IR-2 as a common control within NOAA which is part of an overall Assessment and Accreditation plan. There is a comprehensive section within the annual NOAA IT Security Awareness course that includes roles and responsibilities, and deals with how to recognize an information security incident and to immediately contact the N-CIRT. All information security incidences are reported directly to the N-CIRT. Additional SA training may also provide incident response training as it applies to specific systems.

6.8.3 Incident Response Testing and Exercises (IR-3): NOAA has established IR-3 as a common control within NOAA which includes preparation, detection and analysis, containment, eradication, and recovery handled by the NOAA Computer Incident Response Team (N-CIRT). The NOAA IT Security Office during its evaluation of the NOAA Common Controls will test and exercise annually this control.

6.8.4 Incident Handling (IR-4): NOAA has established IR-4 as a common control within NOAA. Since the N-CIRT's primary mission is to respond to computer security incidents, it determines and assists local offices on what countermeasures need to be deployed to defend, contain, eradicate, and recover from an incident.

6.8.5 Incident Monitoring (IR-5): NOAA has established IR-5 as a common control within NOAA. The N-CIRT uses the NOAA Form 47-43 system which has automated mechanisms in place to report, track, and monitor the incident until it is no longer a threat.

6.8.6 Incident Reporting (IR-6): NOAA has established IR-6 as a common control within NOAA. The N-CIRT reports incidents to the DOC-CIRT, US-CERT, and OIG; and law enforcement agencies. Every office location needs to have a printed copy of the procedures for incident handling readily available to all users who need to be familiar with the reporting process. Specific reporting information for the NOAA8881 system is provided in NOA8881 Incident Response Plan which is part of the System Security Plan (SSP). Local offices should develop local procedures which capture office specific data/processes unique to the office.

6.8.7 Incident Response Assistance (IR-7): NOAA has established IR-7 as a common control within NOAA. The N-CIRT Form 47-43 online web reporting system is the main system to report and respond to IT incidences. The N-CIRT may call offices who report an incident. They will use the NOAA 47-43 database system to document advice and additional procedures to follow in gathering forensic information. During a computer security incident, the N-CIRT serves as the authoritative role overseeing and managing every phase of the incident response.

6.8.8 Incident Response Plan (IR-8): NOAA8881 will follow the DOC and NOAA policies and procedures for developing, and maintaining the system's Incident Response Plan. The CR ISSO will coordinate with the System Owner on developing the plan. The plan will be annually reviewed, updated, and distributed by the CR ISSO as part of the system's Continuous Monitoring activities.

6.9 Awareness and Training (AT): Continuous and ongoing awareness and training activities for NOAA employees (and contractors) is a major cornerstone for NOAA's IT Security Program. An active security awareness program can greatly reduce many risks which cannot be addressed through security software and hardware devices. It is the human element of security that must be addressed which helps prevent a major IT system security crisis.

Relevant Documents

- NIST SP 800 – 12 [An Introduction to Computer Security](#)
- NIST SP 800 – 16 Rev. 1 [Information Security Training Requirements: A Role- and Performance-Based Model](#)
- NIST SP 800 – 37 [Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)
- NIST SP 800 – 50 [Building an Information Technology Security Awareness and Training Program](#)
- NIST SP 800 – 53 Rev. 3 [Recommended Security Controls for Federal Information Systems](#)
- NIST SP 800 – 100 [Information Security Handbook: A Guide for Managers](#)
- DOC ITSP [Information Technology Security Program Policy](#)
-

6.9.1 Security Awareness and Training Policy and Procedures (AT-1): NOAA has established AT-1 as a common control in which all system owners are required to comply with the policies and implementation procedures of these policies. The System Owner will support the established NOAA policy and procedures with the dissemination of awareness and training requirements to local offices. The System owner will determine the level or extent of security training required to support their system security posture and delineate which training shall be mandatory to grant access to their systems.

6.9.2 Security Awareness (AT-2): The NOAA IT Security Awareness, Training, and Education Program apply to all users (government, contractor, associate or temporary personnel) who will be using NOAA IT resources. Temporary personnel include visitors, guest workers, etc., who plan to work at a NOAA site and use NOAA IT resources for one month or more. All new NOAA IT users must take the NOAA IT Security Awareness Course (SAC) within 3 days of being assigned use of IT equipment that will allow them access to the course and annually thereafter. IT Security Training beyond the minimum user awareness level shall be provided to personnel who manage, design, implement or maintain systems such as SAs, ISSOs, SMs, SOs and AOs. Temporary personnel who use NOAA IT resources less than a month (e. g., HAM operators) are not required to complete the NOAA IT Security Awareness Training. Therefore, the local office needs to ensure that NOAA IT behavioral information on the use of government IT resources is provided to this group of temporary personnel. This can be accomplished by developing local usage and conduct guidelines or using the regional guidelines as shown in Appendix F. Below are the minimal areas that need to be addressed:

- Verify the identity of the volunteer, their FCC status, and their community status,
- Provide them our expectations for using government IT resources,

- Ask them to read and sign the acceptable use document,
- Provide appropriate level of supervision for the temporary worker, and
- Use appropriate operational and technical controls on accessible IT resources.

6.9.3 Security Training (AT-3): Any employee that has duties and responsibilities assigned above the normal user level staff needs to maintain a level of proficiency higher than the IT SAC security training to support the evolving security needs of the system. This training may be a mix of technical and security awareness training offered by many sources (e.g., SANS Institute, N-CIRT workshops, DOC and NOAA E-Learning, vendor training, etc.). Additional SANS courses may be available to NOAA employees at a discount. Please contact the CR ISSO for additional information.

6.9.4 Security Training Records (AT-4): The following systems will be used to meet DOC and NOAA requirements to document and monitor individual security training activities:

- NOAA IT Security Awareness Course (SAC) database
- DOC/NOAA/NWS Learning Management System (LMS)
- SF182 Training Forms

6.9.5 Contacts with Security Groups and Associations (AT-5): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7. Technical Controls: Technical Controls are executed security controls by computer systems. The implementation of technical controls must be consistent with the management of security within DOC, NOAA, NWS, and CR.

7.1 Identification and Authentication (IA): Identification is the process whereby a network element recognizes a valid user's identity. Authentication is the process of verifying the claimed identity of a user. A user may be a person, a process, or a system (e.g., an operations system or another network element) that accesses a network element to perform tasks or process a call.

7.1.1 Identification and Authentication Policy and Procedures (IA-1): NOAA has established IA-1 as a hybrid control. Identification, authentication and password controls are technical measures that prevent unauthorized people (or unauthorized processes) from entering an IT system. System Owners should be alert to the fact that NOAA has augmented the DOC policy, providing detailed instructions for this control family that apply to subsequent items in this control family that are not being repeated herein. Below is an overview:

- Unique account identifiers
- Correlate actions to Users
- User ID/account maintenance
 - Monitor and take actions to create and delete accounts
 - Disable user IDs that have been inactive for 30 or more days
 - Disable separating/ terminating user accounts within 24 hours of notification and remove the disabled account within a week of SA notification unless the Security Manager determines that removing the disabled account would adversely affect operations

7.1.2 User Identification and Authentication (Organizational Users) (IA-2): All systems in the NOAA8881 system will be configured to identify and authentic organizational end-user to ensure that the user is associated with the proper assigned security attributes (e.g. identity, groups, roles, security or integrity levels). Multifactor (i.e. two factor authentication – something you know and something you have) which is Level 3 compliant is required for remote system access and will be required upon regional implementation of its capability.

7.1.3 Device Identification and Authentication (IA-3): System components within the NOAA8881 system will provide established device identification and authentication information before establishing a connection. Device technical controls (i.e. media access control (MAC), TLS authentication, Kerberos, radius server, etc.) will be used to comply with this control.

7.1.4 Identifier Management (IA-4): The issuance of unique system identifiers for users and verifying user identity is accomplished through COTS functionality. It is the responsibility of the local Security Manager (SM) to review and approve account requests from users. Once an account request is approved, the SM will advise the SA who will create and set up the accounts. Inactive accounts that have not been used by the user in the past 30 days will be disabled. The SA will advise the SM of all disabled accounts due to user inactivity. The SM will determine whether to leave the account in a disabled status or have it deleted from the system.

7.1.5 Authenticator Management (IA-5): System authentication information (i.e. password, certificates, etc.) will be safeguarded to ensure the integrity of the system from unauthorized persons. Default authentication information for devices will be changed before the device is placed into the operational environment. Distribution of this information is limited to SAs. Lost and/or compromised authentication information is considered an IT Security Incident which must be reported immediately, using the NOAA 47-43 form. Changing and refreshing this information will be in accordance with specific security policy for the particular type of authentication (i.e. password every 60 days or reset the shared/group passwords on systems accounts that cannot be disabled or deleted when user status changes, certificates, tokens or key cards before their expiration date).

7.1.6 Authenticator Feedback (IA-6): Authentication information entered during the authentication process will be obscured or invisible to protect the information from possible exploitation/use by unauthorized individuals. The system will provide user feedback for authentication information that is entered wrong or is incorrect in a manner that will not compromise authentication mechanism.

7.1.7 Cryptographic Module Authentication (IA-7): The highest level of Cryptographic Module Authentication for this system is FIPS140-2.

7.1.8 User Identification and Authentication (Non- Organizational Users) (IA-8): All systems in the NOAA8881 system will be configured to identify and authentic a non-organizational end-user to ensure that the user is associated with the proper assigned security attributes (e.g. identity, groups, roles, and security or integrity levels). A risk assessment will be completed to determine the authentication requirements for these users.

7.2 Access Control (AC): Account management procedures define how an organization establishes, activates, modifies, reviews, disables and removes accounts to protect against unauthorized access or misuse. They ensure user access to IT resources is controlled and monitored at all times.

The System Owner has designated that system administrators (SA) are the only personnel who will have the permission to have account management privileges in order to carry out the above account management actions.

Relevant Documents

- NIST SP 800 – 12 [An Introduction to Computer Security: The NIST Handbook](#)
- NIST SP 800 – 53 Rev 3. [Recommended Security Controls for Federal Information Systems and Organizations](#)
- NOAA IT Security Manual ([ITSM](#)) 212-1302 (V4.2)
- DOC ITSP [Information Technology Security Program Policy](#)
- DOC CTR-009 [Password Requirements](#)

7.2.1 Access Control Policy and Procedures (AC-1): This control is an established NOAA hybrid control. System Owners will need to address and implement System-based logical access controls that go beyond the NOAA common policies and procedures to ensure system protection.

7.2.2 Account Management (AC-2): All IT system accounts will follow the account management procedures described below. All account management will be done in Active Directory, whenever possible.

- **Account Authorizing:** The SO has the granting authority for all IT system user and administrator accounts and has delegated this authority to the local SM. The mechanism used to document normal user account information is the NOAA IT Security Awareness Course database.
- **Account Establishment:** The SA will create and administer the user and administrator accounts in the IT system. The accounts will be created with a temporary password that will be changed by the user immediately upon initial login to the account. A list of all user and administrator accounts will be managed by the CR ISSO and administered by the SA to include the following: account user name, the full name of the user, account type (e.g., NOAA employee, Visitor), date of account creation, date of account deactivation, and reason for account deactivation. Any information that cannot be captured by Active Directory or the NOAA IT Security Awareness Course database must be kept locally. Users must complete the NOAA Security Awareness and Training course and acknowledge the Rules of Behavior before they are given credentials (i.e. username and password) for using their established accounts on the network.
- **Account Activation:** Once the user changes the initial temporary password to an approved personal password the account is considered activate.
- **Account Modification:** The SAs are the only people authorized to modify any user accounts as documented by the CR ISSO and approved by the SO.

- **Account Reviews:** All accounts will be reviewed annually. The local SM will validate normal and privileged accounts during the annually NOAA IT Security Awareness Course datacall. Privileged accounts will be documented and validated using the NWSCR Privileged Account Verification pdf form.
- **Account Naming:** The naming convention for user accounts will follow NWS Active Directory (NADS) Standard Operating Procedure - NADS NWS-0004.
- **Account Disabling:** All temporary and emergency accounts will set to automatically expire in 90 days when created by the SA. If an employee no longer requires the account or will not be using the account for an extended period of time, the account will be disabled by the SA.
- **Account Removal:** Once the account is no longer required, such as the employee has retired or left the organization, the account will be immediately deactivated. Within 30 days, a supervisor or person assigned by the SO, MIC/HIC, or the CR ISSO will review the account for any information required to be maintained by the organization or transferred to another employee. Once the account has been reviewed and the contents saved or distributed, the account will be removed.

The establishment of a local generic user account that requires the use of a group password is not permitted by DOC after September 2009 as stated in CITR- 009. Local generic user accounts established before September 2009 can still be used when it is the only option available to meet mission critical operations. **If generic accounts are still used locally, they will be normal user accounts, never be assigned administrative privileges, and must be used in conjunction with another mechanism that can assure individual accountability (such as a separate and unique network user IDs, separate sign in log with date, time and name of individual, etc.).**

7.2.3 Access Enforcement (AC-3): All user and system accounts will be configured to follow the least privileged concept, granting access only to information for which the user needs to access. Programs directories, ACL's, binaries, etc. must be restricted to only those administrators who have the responsibility to maintain the system. All Microsoft Windows computers will meet the NWS Federal Desktop Core Configuration (FDCC) baseline. All Linux computers will be set to mirror the FDCC requirements as best as possible. All accounts will be set to only operate when an approved complexity password is used. The accounts will automatically lock out users after five (5) unsuccessful login attempts.

7.2.4 Information Flow Enforcement (AC-4): Information Flow Enforcement is conducted throughout the NOAA8881 IT system by using the following mechanisms: firewalls, device ACLs, data exchange controls, authentication (user and machine to machine), interconnection agreements. The basic flow control follows the least privilege concept where the system denies all access by default and only open ports, services, and connections that are required to support the operational mission through its configuration management process.

7.2.5 Separation of Duties (AC-5): Separation of IT administrative duties and IT security duties will be maintained at the regional office. Local offices should try to maintain separation of duties as staffing permits. When separation of duties cannot be maintained local offices will need to have compensating management controls in place to ensure system integrity and security. For example, if the ITO is functioning as the backup SA, there should be a local policy that

would require that administrators use their individual administrator's accounts when performing administrative duties. If that is not possible due to system constraints, then they would first need to log into the system with their normal user account and then log in as an administrative root user.

7.2.6 Least Privilege (AC-6): The concept of least privilege will be used throughout the system to enforce and limit access and control to only those individuals that have a need to know and/or have access to system components to include their information. This will be achieved by Security Managers access reviews.

7.2.7 Unsuccessful Login Attempts (AC-7): The maximum number of consecutive failed (invalid access) attempts by a user within a fifteen (15) minute period is five (5). The information system will be configured to automatically lock the account when the maximum number of unsuccessful attempts is exceeded. Lockout time is fifteen (15) minutes before the user can resume login actions.

7.2.8 System Use Notification (AC-8): All computing systems in the NOAA8881 system will have an approved DOC warning banner, similar to the banner below, displayed during login. This includes all windows and linux workstations and servers. Any remote access (VPN, Remote Desktop, SSH, FTP, etc.) must also display this banner upon login.

***** WARNING ***** WARNING *****

"This is a United States National Weather Service computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms."

***** WARNING ***** WARNING *****

DOC approved warnings banner may be found on the NOAA Computer Security Page at the following url: <https://www.csp.noaa.gov/banners/Banner-DOC.html>

7.2.9 Previous Logon (Access) Notification (AC-9): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.2.10 Concurrent Session Control (AC-10): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.2.11 Session Lock (AC-11): System lock mechanisms will be used and initiated after fifteen (15) minutes of inactivity of a computer. Computers at WFO/RFC sites used to process mission critical time-sensitive severe warnings are exempt from initiating this control. If a computer is not in the office's operational area, it doesn't qualify for the exemption. Since physical location of these computers is maintained in space accessible only to NWS employees and/or where visitors are always under NWS personal supervision, the following compensating controls are used for exempted operational computers: PE-2, PE- 3, PE-6, PE-7, PS-2, and PS-3.

7.2.12 Session Termination (AC-12): This security control has been withdrawn in NIST 800-53 revision 3 and incorporated in the SC-10 control.

7.2.13 Supervision and Review—Access Control (AC-13): This security control has been withdrawn in NIST 800-53 revision 3 and incorporated in the AC-2 and AU-6 controls.

7.2.14 Permitted Actions without Identification or Authentication (AC-14): The ability to access the system without having to authenticate with unique user credentials is not allowed. The only exception would be if any office has set up public access kiosk, providing that it has been properly secured, hardened, and documented.

7.2.15 Automated Marking (AC-15): This security control has been withdrawn in NIST 800-53 revision 3 and incorporated in the MP-3 control.

7.2.16 Security Attributes (AC-16): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.2.17 Remote Access (AC-17): DOC and NOAA policy requires agency organizations to monitor and control remote access into their IT systems. Remote access into the NOAA8881 system will be through the centrally managed Virtual Private Network (VPN) appliance at CRH. Remote users must sign and submit a Central Region Remote Access User IT Agreement through their supervisor to the CR ISSO. Two-factor authentication is required when it becomes available. Under no circumstances will public-access equipment be used to remote into the IT system.

7.2.18 Wireless Access (AC-18): The following CR restrictions on wireless access are in addition to DOC, NOAA and NWS policy:

- Laptops or PCs with built in wireless transmitters must have the “ad-hoc” mode disabled to prevent ad hoc networks from being established that may create a bridge from an unsecured network to a secured network (LAN).
- Wireless networks may not be used to access information system components that store, process, or transmit PII.
- Wireless reception must not extend beyond the immediate area of CR ownership.
- All wireless configurations and access must be documented and approved by the CR ISSO before placed into operations. The following below documentation needs to be submitted:
 - Memo for Record stating the purpose and usage
 - Statement of Use to any NOAA/NWS guests
 - CR Wireless Access Point Checklist
- The CR ISSO will submit wireless documentation to the CIO’s office in order for NOAA to register it.

Internal Wireless Access

- Only 802.11i (WPA-Enterprise mode) encryption standard is allowed.
- Users must be authenticated through a central managed solution.
- Audit logs must be reviewed weekly.

- 802.11 wireless networks are prohibited in areas where they will disrupt the NOAA mission, such as meteorological instrumentation research.
- Use of ad-hoc mode for 802.11 wireless connections is prohibited.

7.2.19 Access Control for Mobile Devices (AC-19): Only government-owned mobile devices with known identifiable ownership are allowed on the NOAA 8881 IT System. Government-owned devices that have left the physical control of the office environment (i.e. travel or telework) must be examined by local IT staff prior to it being connected back onto the network. For devices that left the United States or its territories, offices will need to comply with current DOC CTR-002, Safeguarding Data on Foreign Travel. Scanning for malicious code will be in accordance with the SI-3 security control. See MP-4 and MP-5 control for protecting the information residing on mobile devices.

Wireless communications devices like aircards and WiFi devices must be connected to an authorized mobile phone carrier. Apply the below appropriate security controls to mobile devices:

- Device configuration baseline that documents the device settings
 - Change device default network SSID and network key
 - Pre-shared Key (PSK) authentication – WPA2 or higher
 - Disable SSID broadcasting
- Usage policy
 - Normally only to be used outside the office to meet operational needs
 - Inside office use permitted as backup to failed internet access
 - DOC Password Authentication must be invoked and changed used during each deployment
 - All users must comply with DOC, NOAA, and NWS Internet Use Policy
 - Record and track users who have been given permission to connect to device
 - User restricted to Federal, State or local government officials/employees
- Property Chain of Custody
 - Report lost or stolen devices to the CRH Communication Program Manager

7.2.20 Use of External Information Systems (AC-20): No external information system (i.e. personally-owned equipment) may be connected directly to the NOAA8881 IT system. External information systems include but are not limited to: personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, USB thumb drives / memory sticks, or any other agency's IT property. Per DOC CTR-002, no personally owned laptops shall be used on foreign travel to perform DOC-related work. Any personally owned computer taken to a foreign country for any reason shall not be connected to the DOC infrastructure, physically or via VPN until it goes through a complete verification scan by local IT staff, as directed by this policy (i.e. SI-3) and is re-approved by the SO.

Equipment used for teleworking or other government or university IT systems that interconnect with the NOAA8881 system must have one of the following approved written documentation: CR Telework Agreements, Memorandum of Understanding (MOU) and/or an Interconnection Security Agreement (ISA). The signing approval official for all NOAA8881 system interconnection agreements remains with the System Owner.

7.2.21 User-based Collaboration and Information Sharing (AC-21): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.2.22 Publicly Accessible Content (AC-22): The NOAA8881 IT System CR/WAN/LAN does not have any publicly accessible devices. Therefore, this control does not apply to this system.

7.3 Audit and Accountability (AU): All audit and accountability functions will follow the management procedures described below. All NOAA8881 IT systems within the system boundary, including computers, firewalls, routers, and intelligent switches, will log events and these event logs will be stored by the system. The event logs for perimeter devices will be archived and stored on a regional system log server for at least 120 days. There is no storage requirement for event logs from individual computers unless there is a documented security incident, in which case, those logs will be stored and archived per the direction of the N-CIRT. Normally, the event logs from individual computers are allowed to roll and overwrite existing log files.

Relevant Documents

- NIST SP 800 – 12 [An Introduction to Computer Security](#)
- NIST SP 800 – 53 Rev 3. [Recommended Security Controls for Federal Information Systems and Organizations](#)
- DOC ITSP [Information Technology Security Program Policy](#)
- NOAA IT Security Manual ([ITSM](#)) 212-1302 (V4.2)

7.3.1 Audit and Accountability Policy and Procedures (AU-1): All NOAA8881 information systems will be configured to produce, store, and retain audit records of specific system, application, network, and user activity in accordance with established applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Specific auditing guidance for the NOAA8881 system is established in the AU-2 through AU-11 controls.

7.3.2 Auditable Events (AU-2): Audit tracking is important to the NOAA8881 system security to detect and track unauthorized attempts by a user or outside third party. The following minimum set of auditable events is to be set and collected by IT system (where applicable):

Audit account logon events: Tracks users' who have logged on and off the local machine.

- Success – Failure

Audit Account Management: Tracks changes to the security accounts database.

- Success – Failure

Audit Directory Services Access: Audits users' access to Active Directory objects.

- Failure

Audit Logon Events: Tracks users' who have logged on or off the network.

- Success – Failure

Audit Object Access: Tracks unsuccessful attempts to access objects.

- Failure

Audit Policy Change: Tracks changes to security policy

- Success

Audit Privilege Use: Tracks unsuccessful attempts to use privileges.

- Failure
- Audit System Events:** Tracks events that affect the entire system.
- Success

7.3.3 Content of Audit Records (AU-3): The following content will be required for every audited event:

1. Type
2. Date
3. Time
4. Source
5. Category
6. Event
7. User
8. Computer

7.3.4 Audit Storage Capacity (AU-4): Sufficient hard drive storage space will be allocated to the storage of audit logs on perimeter /edge devices so that they are not over written or lost and meet the required minimum storage period of at least 120 days. Audit storage capacity settings for Windows computers are applied at the root GPO level which can only be modified by the assigned enterprise administrator.

7.3.5 Response to Audit Processing Failures (AU-5): IT systems and components in the NOAA8881 system will configure the audit logs to overwrite older entries instead of shutting the system down when the log size grows to maximum. All systems will be configured to at least the size of the Windows security log size default setting. Since the internal device audit logs are rolled and overwritten, there is no need to have alert notification unless they are deemed critical assets. Assets deem critical by System Owner will have alerts set and distributed to appropriate IT staff. Responses to failures will be based on the NOAA8881 Business Impact Analysis (BIA) plan.

7.3.6 Audit Review, Analysis, and Reporting (AU-6): Audit review, analysis, and reporting are primary functions of system administrators, Information Technology Officers (ITOs), and the CR ISSO. The level of monitoring and analysis will be commensurate to level of risk exposure of the devices. For example, devices within the trusted network protected by firewalls will normally not require the same level of review and analysis as perimeter devices like firewalls, public FTP servers, or wireless access points.

The review and monitoring of perimeter devices should be reviewed at least every three business days but not less than weekly. A sampling of internal devices needs to be checked at least weekly. However, if there are indications that these devices are being exposed to an increased level of threat (i.e. numerous external attacks or perimeter devices or an internal threat of a disgruntled or potentially disgruntled employee), a more frequent monitoring and review schedule will be required to ensure system integrity. As per [NWSI 60-702](#), the frequency for analysis, the dates performed, and the results will be documented and maintained throughout the life cycle of the device/system. Central Region offices will use the NWS Engineering Management Reporting System to record and track audit activities. A sample EMRS A-26 is located in Appendix G. Please note that until the ITSA equipment code can be implemented into

the EMRS system, please use the PCSA in the Equipment Code and in Block C under the SPECIAL PUROSE REPORTING INFORMATION section enter "ITSA."

Reporting of inappropriate or unusual activity which meets the criteria outlined in the NOAA8881 Incident Response Plan will need to be reported to the NOAA Computer Incident Response Team (N-CIRT). Other suspicious or unusual activities need to be reported to the regional ISSO.

All perimeter devices and components deemed critical to the system's operations and security need to employ an automated mechanism to alert administrators and/or security personnel of device/network failures or attacks.

7.3.7 Audit Reduction and Report Generation (AU-7): The NOAA8881 system will use the enterprise level automated mechanism tools when they become available. Until such time, Security Managers should maintain locally descriptive audit information documentation. At minimum the documentation should include systems being audited, the level of frequency, tools used, if any along with when reports are generated.

7.3.8 Time Stamps (AU-8): All NOAA8881 IT systems, including computers, firewalls, routers, and intelligent switches will use a time stamp on all audit event log entries. The time stamp for regional devices will be derived from the Windows server located and maintained at Central Region Headquarters in Kansas City, MO. The Windows server will receive its time from two government Internet Time Service Servers: NIST (time.nist.gov) and US Naval Observatory. Linux systems receive time stamps individually from NIST. For local field offices, their devices will be configured to receive their time from the NTP server on the MPLS network. Since continuous connectivity to the time server provides real-time synchronization, there is no need to establish synchronization frequency schedule.

The use of UTC timestamps⁷ will be used to maintain consistency throughout the NWS enterprise.

7.3.9 Protection of Audit Information (AU-9): All NOAA8881 IT system audit logs and their directories will have their permissions set to allow access only by the root or administrator accounts.

7.3.10 Non-repudiation (AU-10): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.3.11 Audit Record Retention (AU-11): The retention of audit records will be in accordance with [General Record Schedule 20](#) guidelines as defined in **Section 1 – Files/Records Relating to the Creation, Use, and Maintenance of Computer Systems, or Electronic Records** or within the ninety (90) day guidance established by DOC ITSSP whichever is longer. The GRS 20 schedule allows for the deletions or destruction when the agency determines they are no longer needed for administrative, legal, audit, or other operational purpose.

The determination of record retention is contingent on the reason for retaining the records. The

⁷ This requirement applies only to servers. Desktops may continue to be set to local time.

retention of perimeter device electronic files will be kept for one year while internal device electronic files will be allowed to be overwritten by the system. If the records are required to satisfy administrative, legal, audit, or other operational purpose requests, the files will be delivered to the requesting party who will retain and determine the record disposition. For example, if system logs are requested from the N-CIRT, the N-CIRT will retain and dispose of the records after they are deemed no longer required for forensic purposes.

7.3.12 Audit Generation (AU-12): All IT systems that have the capability to generate systems audit logs and records will be configured to capture those events as defined in AU-2 and AU-3.

7.3.13 Monitoring for Information Disclosure (AU-13): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.3.14 Session Audit (AU-14): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4 System and Communications Protection (SC): The System and Communications Protection (SC) family of controls applies to the protection of information transmitted within and outside the information system.

Relevant Documents

- NIST SP 800 – 37 [Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)
- NIST SP 800 – 53 Rev. 3 [Recommended Security Controls for Federal Information Systems](#) NIST SP 800 – 56A [Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography](#)
- NIST SP 800 – 57 [Recommendation for Key Management Part I](#), [Part II](#), and [Part III](#)
- NIST SP 800 – 111 [Guide to Storage Encryption Technologies for End User Devices](#)
- DOC ITSP [Information Technology Security Program Policy](#)
- NOAA IT Security Manual ([ITSM](#)) 212-1302 (V4.2)

7.4.1 System and Communications Protection Policy and Procedures (SC-1): The establishment and dissemination of SC policies and procedures will be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and coordinated within the NWS directive and all other appropriate means of communicating policy and procedures.

7.4.2 Application Partitioning (SC-2): Application partitioning will be maintained throughout the system in order to separate user functionality from information system management functionality. For example, user interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. Any changes in system and workflow design must include an application partitioning analysis and identify appropriate configuration management controls to control adequate separation.

7.4.3 Security Function Isolation (SC-3): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.4 Information in Shared Resources (SC-4): Information on shared resources may be left as small parts or traces (remnants) of information remaining after a resource transfers from one user to another user. Control of information system remnants, sometimes referred to as object reuse, prevents information, including encrypted representations of information, from being shared with unauthorized users. Therefore, it is important to prevent information produced by the actions of a prior user/role from being available to any current user/role that obtains access to a shared system resource after that resource has been released back to the information system.

It is the responsibility of the System Administrator to configure information system components from leaving remnants of information from authorized users. The NADS GPO's and United States Government Configuration Baseline (USGCB)⁸ settings will automatically clear memory page files on reboot and clean the temporary folders at the end of session. Any Windows or non-Windows computer not controlled by Active Directory will need to be manually configured to remove remnant information.

7.4.5 Denial of Service Protection (SC-5): Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks over the Internet has risen sharply and become more sophisticated in the last several years. In order to minimize the launch of denial of service attacks against the information systems, all firewalls, routers and access points will be configured to reduce the threat of these attacks. The below countermeasures will be implemented appropriately on perimeter and routable devices within the NOAA8881 system:

1. Allow only the necessary ICMP traffic into and out of an environment.
2. Configure perimeter routers to reject as incoming messages any packets that contain internal source IP addresses since such packets are spoofed.
3. Disable direct broadcast functionality at border routers to make sure NWS networks are not used as an amplifier for attacks on other networks.
4. Employ network-based IDS to watch for suspicious activity.
5. Apply vendor patches during the NOAA quarterly scans or within 45-days following known patch release whichever is sooner.
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.

⁸ Former known as Federal Desktop Core Configuration (FDCC)

Network monitoring tools like **Multi Router Traffic Grapher (MRTG)**, SNORT, and Logwatch will be used to monitor the traffic load and attacks on the network.

7.4.6 Resource Priority (SC-6): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.7 Boundary Protection (SC-7): The majority of incidents that originate outside the un-trusted network can be mitigated through monitoring and controlling communication connection at the external boundary. The only access point to the Internet or other un-trusted networks will be through the Central Region communication infrastructure via the NOAANET MPLS where firewall controlled access is maintained and monitored or through other approved routes by the system owner. There will be no external access at any field location unless an operational requirement can be established and regional permission is granted from CRH. If an external access point is granted, the access point either needs to be on a separate stand-alone network which never touches the trusted network or isolated by a WSH or CRH approved firewall to include the firewall ruleset. Failure to apply standard consistent configuration to these resources greatly increases the risk of compromise or harm resulting from network attacks. Network Operation Center managers and other network and information system owners/managers will ensure filtering of incoming (ingress) and outgoing (egress) traffic at appropriate internet connection points to maximize protection while minimizing risk.

7.4.8 Transmission Integrity (SC-8): Information transmission channels of incoming and/or outgoing data must have security controls at the same level or higher commensurate to the data being transmitted to ensure data integrity. For example, remote logins with confidential information will utilize secure protocols like Secure Shell (SSH), Secure Socket Layer (SSL), Transport Layer Security (TSL), Virtual Private Networks (VPN), and secure HyperText Transmission (HTTPS). Protocols used will be documented in the NOAA8881 System Security Plan.

7.4.9 Transmission Confidentiality (SC-9): Like transmission integrity, data confidentiality must be maintained, using the same controls outlined in SC-8 above.

7.4.10 Network Disconnect (SC-10): This control applies mainly to remote type connections (dial-in, VPN, SSH) established by a network layer between two users or computers for the sharing or transferring of data. The Central Region organizational defined time period of connection inactivity is 30 minutes. All network technical controls will be set to disconnect the connection after 30 minutes of inactivity. The inactivity period may be set to less than 30 minutes upon the discretion of the Security Manager. If an operational condition arises to where the session termination time must exceed the 30 minute timeframe, the Security Manager will contact and provide the operational justification to the CR ISSO. The CR ISSO will evaluate the risk and make a recommendation to the System Owner who has the final authority to make the risk based decision to accept or reject extending the session termination time. An example of an exception would be where there are network interconnection agreements in place that specify operational connection requirements between the two system parties. Remote system session connections established through interconnection agreements are controlled and bound through the following compensating controls: CA-3 and SA-9.

Domain connection partnership between domain controller/s and clients are not subject to this

control as the system uses the AC-11 Session Lock and AC-12 Session Termination controls applied via GPOs as compensating controls to mitigate risks associated with this control.

7.4.11 Trusted Path (SC-11): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.12 Cryptographic Key Establishment and Management (SC-12): Until such time as an enterprise solution is established and implemented, the NOAA881 system will use COTS Cryptographic functionality (i.e. Kerberos with self-generated keys/certificates) and other Public Key Cryptography.

7.4.13 Use of Validated Cryptography (SC-13): Cryptographic mechanisms when used will need to comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and other government guidance. Validation certificates issued by the NIST Cryptographic Module Validation Program, including FIPS 140-1, FIPS 140-2, and future amendments, remain in effect and the modules remain available for continued use until a validation certificate is specifically revoked. NWS envisions a common cryptographic control being part of NOAANet when completed and fully operational.

7.4.14 Public Access Protections (SC-14): NWS provides controls supporting integrity and availability of web content managed by the NWS Web Farm family of services. Any other public access to NWS information through another forum, such as social media, needs to be coordinated with the System Owner and the NWS CIO in order to ensure sufficient security controls are in place to protect the NWS network and NWS information availability and integrity. Whatever solution(s) are approved and implemented need to be documented and records retained at least across the life cycle of the product.

7.4.15 Collaborative Computing Devices (SC-15): The use of a camera and microphone devices are authorized when participating in activities that support the mission of the NWS. However, remote activation of any collaborative computing is prohibited.

7.4.16 Transmission of Security Attributes (SC-16): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.17 Public Key Infrastructure Certificates (SC-17): The NOAA8881 system does not issue or use public key certificates.

7.4.18 Mobile Code (SC-18): Use of mobile code technologies such as JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript is limited to mission required activities. Usage of USGCB settings and active directory group policy limits installation of mobile code programs to system administrators.

7.4.19 Voice Over Internet Protocol (SC-19): NOAA has established SC-19 as a common control in which all system owners are required to comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and other government guidance for this control. Currently, the NOAA8881 system has not implemented VoIP. The implementation, support, and administration of VoIP are regional functions within the Systems and Facilities Division who will follow the NOAA established guidelines found in Appendix C: VoIP of

NOAA IT Security Manual 212-1302.

7.4.20 Secure Name/Address Resolution Service (Authoritative Source) (SC-20): As a system within NOAANET, the NOAA8881 system utilizes the NOAA DNSSEC architecture and provisioning for its domain name services. All system workstations will point to the internal DNS servers.

7.4.21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC- 21): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.22 Architecture and Provisioning for Name/Address Resolution Service (SC-22): As a system within NOAANET, the NOAA8881 system utilizes the NOAA architecture and provisioning for its domain name services. All system workstations will point to the internal DNS servers.

7.4.23 Session Authenticity (SC-23): The implementation and use of security protocols in SC-8 and SC-9 and using Active Directory domain services authentication for computers satisfy this control.

7.4.24 Fail in Know State (SC-24): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.25 Thin Nodes (SC-25): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.26 Honeypots (SC-26): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.27 Operating System-Independent Applications (SC-27): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.28 SC-28: Protection of Information at Rest (SC-28): Information at rest is the state of information when it is located on a secondary storage device, such as, a disk, USB or tape drive with the information system. This control is intended to protect the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information by employing appropriate cryptographic mechanisms to prevent unauthorized disclosure and modification of the information.

7.4.29 SC-29: Heterogeneity (SC-29): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.30 SC-30: Virtualization Techniques (SC-30): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.31 SC-31: Covert Channel Analysis (SC-31): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.32 SC-32: Information System Partitioning (SC-32): Information System Partitioning is part of the NOAA8881 defense-in-depth protection strategy. By using separate physical environments with managed interfaces, system information can be restricted to authorize users or information flow among partitioned system components.

7.4.33 SC-33: Transmission Preparation Integrity (SC-33): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

7.4.34 SC-33: Non-Modifiable Executable Programs (SC-34): The NOAA8881 system is categorized as a moderate system. Therefore, this control is not applicable.

8. Information Security Program Management Controls: Information security program management controls are developed and implemented to address the organization –wide security program.

8.1 Program Management (PM): The PM controls complement the other security controls, focusing on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

Relevant Documents

- FIPS Publication 199 [Standards for Security Categorization of Federal Information and Information Systems](#)
- NIST SP 800 – 30 [Risk Management Guide for Information Technology Systems](#)
- NIST SP 800 – 37 [Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems](#)
- NIST SP 800 – 39 [Managing Information Security Risk](#)
- NIST SP 800 – 55 Rev. 1 [Performance Measurement Guide for Information Security](#)
- NIST SP 800 – 60 Rev.1 [Volume I Guide for Mapping Types of Information and Information Systems to Security Categories](#) and [Volume II Appendices](#)
- NIST SP 800-65 [Integrating IT Security into the Capital Planning and Investment Control Process](#)
- NWS Policy Directive (PD) 60-5 [Enterprise Architecture Program](#)
- NWS Policy Directive (PD) 30-51 [Physical Security](#)

8.1.1 Information Security Program Plan (PM-1): The Information Security Program Plan used by organizations within DOC is a compilation of policy, procedures, and planning documents at the different organizational levels. Common controls that are inheritable by one or more organizational systems are documented in a single common controls plan by NOAA.

8.1.2 Senior Information Security Officer (PM-2): The Senior Information Security Officer position in the NWS is referred to as the Chief Information Security Officer (CISO) who is appointed by the NWS CIO.

8.1.3 Information Security Resources (PM-3): The Information Security Resources for the NOAA8881 IT System is a part of the capital planning and investments documented in Exhibits 53 and 300 prepared by DOC and NOAA.

8.1.4 Plan of Action and Milestones (POA&M) Process (PM-4): The standards by which NOAA line offices are expected to comply when executing their system-based POA&Ms are documented in the NOAA Plan of Action and Milestones (POA&M) Management Standard plan. The CR ISSO coordinates with the AO, SO, and local SMs to ensure that all IT security weaknesses are entered and tracked through completion. Refer to the CA-6 control for submittal details.

8.1.5 Information System Inventory (PM-5): An inventory of all assigned IT information systems (i.e. NOAA8881) is kept and maintained by DOC through the use of the DOJ Cyber Security Assessment and Management (CSAM) tool.

8.1.6 Information Security Measures of Performance (PM-6): Information security measures are used to facilitate decision making and to improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data. These measures are obtained at different levels within the organization through the use of data calls and other methods of data collection. Security performance goals and objectives are established and disseminated through policy channels and plans.

8.1.7 Enterprise Architecture (PM-7): IT Enterprise Architecture (EA) aligns IT resources within an organization to improve business performance in assisting to execute their core mission. It is the roadmap to systematically define the current baseline and provide for a desired environment for evolving information systems and emerging technologies. The primary purpose of an EA is to *inform*, *guide*, and *constrain* the decisions for the enterprise, especially those related to IT investments. NWS Policy Directive 60-5, Enterprise Architecture Program, establishes the EA objectives and the authorities and responsibilities for each level with the agency. All Central Region offices need to collaborate with Central Region Headquarters before making significant changes within their local IT environment to ensure that proposed changes are aligned and consistent with the NWS Enterprise Architecture.

8.1.8 Critical Infrastructure Plan (PM-8): DOC and NOAA uses the DOC Phased Facility Security Program Development Handbook as the foundation document along with the latest DHS National Security Advisory System (HSAS) to support this security control to ensure that all Commerce critical infrastructure/key resource facilities and buildings receive adequate and sustainable security and associated physical and environment controls. The NWS maintains its Risk Management Strategy under NWS PD 30-51 to protect field office property. In addition, each office will have a continuity of operations plan and conduct disaster recovery exercises to verify that viable controls have been put in place to ensure sustainability of critical infrastructure/key resource assets.

8.1.9 Risk Management Strategy (PM-9): Risk Management Strategy standards and guidelines for offices under DOC are published in NIST Special Publications 800-30 and 800-37. The NOAA Risk Management Framework (RMF) document provides the structured process to determine and deal with risks found within the system.

8.1.10 Security Authorization Process (PM-10): In addition to the implementation of the Risk Management Framework and the employment of associated security standards and guidelines, the security authorization process for information systems requires defining specific roles and

designating authorizing officials within the risk management process who can assess unacceptable risk within a system. DOC Commerce Interim Technical Requirement number 4 (CITR-004) that addresses the DOC certification and accreditation of systems establishes the process. NWS Instruction (NWSI) 60-701 Assignment of Responsibilities defines the security authorization process within the NWS. The Central Region Director is the appointed authorizing official for the NOAA8881IT system.

8.1.11 Mission/Business Process Definition (PM-11): The mission and business processes are identified, analyzed, and documented in the system's Business Impact Analysis Plan. The Central Region Headquarters COOP plan establishes the decision-making process that allows for an assessment of emergency situations and determination of the best course of action for response and recovery that affects mission critical business functions.

APPENDIX A Abbreviations and Acronyms

Abbreviation/Acronym	Meaning
ASD	Administrative Services Division
AO	Authorizing Official
A&A	Assessment & Authorization
CISO	Chief Information Security Officer
CITR	Commerce Interim Technical Requirement
COOP	Continuity of Operations Plan
CUI	Controlled Unclassified Information
CSAM	Cyber Security Assessment and Management
DOC	Department of Commerce
EA	Enterprise Architecture
EMRS	Engineering Management Reporting System
ESA	Electronic Systems Analyst
EULA	End User License Agreement
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standardization
FISMA	Federal Information Systems Management Act
FOUO	For Official Use Only
GOTS	Government off-the-shelf
GRS	General Record Schedule
HIC	Hydrologist In Charge
ISSO	Information System Security Officer
IT	Information Technology
ITO	Information Technology Officer
MIC	Meteorologist in Charge
MPLS	Multi Protocol Label Switching
NCIRT	NOAA Computer Incident Response Team
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NOAANET	NOAA Network
NWS	National Weather Service
NWSI	NWS Instructions
PII	Personally Identifiable Information
PEPPP	Physical and Environmental Protection Policies and Procedures
POA&M	Plan of Action and Milestones
PD	Policy Directive

Abbreviation/Acronym	Meaning
RD	Regional Director
SA	System Administrator
SDM	Station Duty Manual
SFD	Systems and Facilities Division
SM	Security Manager
SO	System Owner
SP	Special Publication
USGCB	United States Government Configuration Baseline
VPN	Virtual Private Network
WFMO	Workforce Management Office

APPENDIX B NOAA Sanitization Validation and Destruction Worksheet

**NOAA Computer/Hard Drive Sanitization Validation
and PDA/Cell Phone Destruction Worksheet**

To be submitted as part of the required Final Event or Excess Receipt documentation

Organization: NWS
 Property Custodian Code (Custodian Area): 54022E097
 Equipment Type: Computer/Hard Drive

The Equipment Types Computer/Hard Drive and PDA/Cell Phone cannot be combined on the same worksheet

Barcode:	<u>CD0001578944</u>	Model Number:	<u>Z602</u>
Serial Number:	<u>FGTR5674323TY</u>	Description:	<u>Laptop</u>
Final Disposition:	<u>Disposed</u>	Sanitization Method:	<u>Purge</u>
Other Final Disposition (Explain): _____			
Barcode:	<u>CD0001578945</u>	Model Number:	<u>VIS12</u>
Serial Number:	<u>K000ER566743A</u>	Description:	<u>Server</u>
Final Disposition:	<u>Disposed</u>	Sanitization Method:	<u>Clear</u>
Other Final Disposition (Explain): _____			
Barcode:	_____	Model Number:	_____
Serial Number:	_____	Description:	_____
Final Disposition:	_____	Sanitization Method:	_____
Other Final Disposition (Explain): _____			
Barcode:	_____	Model Number:	_____
Serial Number:	_____	Description:	_____
Final Disposition:	_____	Sanitization Method:	_____
Other Final Disposition (Explain): _____			
Barcode:	_____	Model Number:	_____
Serial Number:	_____	Description:	_____
Final Disposition:	_____	Sanitization Method:	_____
Other Final Disposition (Explain): _____			
ISSO Print Name	<u>XX Sign</u>		<u>9-26-2011</u>
IT Security Official (NWS ISSO)	Signature		Date
PC Print Name	<u>XX Sign</u>		<u>9-26-2011</u>
Property Custodian	Signature		Date
PAO Print Name	<u>XX Sign</u>		<u>9-26-2011</u>
Property Accountability Officer	Signature		Date

APPENDIX C Sample Central Region Risk Analysis Worksheet

CENTRAL REGION RISK ANALYSIS WORKSHEET		
SECTION 1: Risk Analysis (To be completed by Local Office prior submitting request to NWS CR ISSO)		
Site Location (City, State and NOAA SYSTEM ID:		Date of Request:
Name of Requestor:	Phone Number:	Email:
SECTION 2: Hardware/Software (To be completed by Requestor)		
State Operational Requirement:		
Hardware or Software Product Name and Description:		
Network Path (If Applicable): <input type="checkbox"/> Intranet <input type="checkbox"/> Internet		
Source IP(s)/Subnet(s):	Port(s):	
Source Device Description:		
Protocol(s): <input type="checkbox"/> TCP <input type="checkbox"/> UDP		
Destination IP(s)/Subnet(s):	Port(s):	

CENTRAL REGION RISK ANALYSIS WORKSHEET		
SECTION 3: Local Information Systems Security Manager (SM) needs to be complete this section prior to submitting request to submitting to CRH.		
Name of ISSO:	Phone Number:	Email:
Risk Category: <input type="checkbox"/> LOW RISK <input type="checkbox"/> MEDIUM RISK <input type="checkbox"/> HIGH RISK		
Risk Description:		
Notes:		
SECTION 4: NWS CR ISSO		
Reviewed by:		Date of Review:
Risk Category: <input type="checkbox"/> LOW RISK <input type="checkbox"/> MEDIUM RISK <input type="checkbox"/> HIGH RISK		
Risk Description:		
Notes:		
SECTION 5: System Owner or Authorizing Official Review		
Date Reviewed:	<input type="checkbox"/> APPROVED <input type="checkbox"/> NOT APPROVED	
Notes:		

APPENDIX D WFO/RFC Local Security Related Planning Activities Example

NOAA8881 Security Related Planning Activities 2011					
Control	Security Activity	Frequency	Action POC	Date of Last Action/Event	Next Scheduled Event Date
CP-09	Information System Backup	Daily/ Weekly/ Monthly	ISSO	Daily/ Weekly/ Monthly	Daily/ Weekly/ Monthly
AC-02	Account Management ¹	Weekly / Annual	SAs /ISSO	Weekly	Weekly
AC-02	Validate Privileged Accounts	Annual	SM	New Requirement	2011
CA-05	Plan of Action and Milestones (POA&M)	Monthly/ quarterly	ISSO	Monthly	Monthly
RA-05	Vulnerability Scans	Quarterly/ New Systems	ISSO	Each Quarter	3/15/2011 6/15/2011 9/15/2011 12/15/2011
AT-03	Security Training (SAs) Review & Selection	Annual/ Major Change	ISSO	2/15/2011	NLT 4/1/2012
AT-02	Security Awareness Training	Annual	ISSO	May 2011 – Actual date TBD by NOAA	August 31, 2012(Est. – Actual date determined by NOAA)
CA-06	System Accreditation	3 years/ major change	SO	5/7/2010	5/7/2013
CA-07	Continuous Monitoring	Annual	ISSO	5/7/2011	5/7/2012
CM-04	Monitoring Configuration Changes	Annual	ISSO	5/7/2011	5/7/2012
CA-02	Security Assessments	Annual	ISSO	2/3/2011	2/1/2012
PL-6	Security-Related Activity Planning	Annual	ISSO	2/16/11	2/1/2012
CA-03 / SA-9	Review Information System Connections	Annual	ISSO	2/1/2011	2/1/2012
CM-08	Information System Component Inventory ²	Annual	ISSO	2/3/2011	2/1/2012
CP-03 CP-04	Contingency, Training and Plan Testing and Exercises	Annual	ISSO	TBD	5/7/2012
AU-6	Audit Monitoring ³	On-Going	ISSO/ SAs	On-Going	On-Going
RA-02	Security Categorization	3 years/ major change	ISSO	2/1/2010	2/1/2013

¹ Includes review of Account Age Report, account names and privileges
² This inventory is for operational off-network devices (i.e. security PC, phone PC, etc). Inventory for network device will be accomplished using the SCCM.
³ Completed IAW CRS 02-2010 IT Security Policies & Procedure supplement.

APPENDIX E IT System Interconnection Agreement Templates

MEMORANDUM OF UNDERSTANDING

**“National Weather Service -
NWS, Central Region”**

And

“Organization B Name”

{Date of Agreement entered by CRH}

Organization A

**National Weather Service
Central Region
20-30-xx-xxx**

Organization B

**Org B Company Name
Org B Division/Section Name**

INTRODUCTION

The purpose of this document is to establish a management understanding between the “National Weather Service Central Region” and “**Organization B Name, City, ST**” regarding the management, operation and security of the connection between the “National Weather Service Central Region” and “**Organization B Name, City, ST**”. This agreement will govern the relationship between the “National Weather Service Central Region Headquarters” and “**Organization B Name, City, ST**”, including designated managerial and technical staff.

AUTHORITY

The authority for this agreement is based on the Federal Information Security Management Act (FISMA) 4.2.7 requirements for the National Weather Service to obtain written agreements between interconnected systems.

BACKGROUND

It is the intent of both parties to this agreement to a {enter type of connection here} connection from the “**Organization B Name, City, ST**”, to the National Weather Service (NWS) Central Region Headquarters (CRH) network system which is part of the CR WAN/LAN. The agreement is to provide access to {enter protocol and port number here} between “**Organization B**” and CRH for the exchange of products using {enter software and/or connection type}. The expected benefit of the interconnection is necessary and essential to further the mission of the NWS in that it enables {describe the benefits for one or both parties to include the shared information/data}.

Benefit Example - The expected benefit of the interconnection is necessary and essential to further the mission of the NWS in that it enables collaboration between the NWS and NDSU in order to share hydrologic data and forecasts.

Each IT system is described below:

- **SYSTEM A (NOAA8881)**
 - National Weather Service
 - Central Region Headquarters
7220 101st Terrace
Kansas City, Missouri 64153
 - Allow {enter connection type to destination device}
 - Technical Contact: {enter Name} – {enter phone number}
 - Operational Contact: {enter Name} – {enter phone number}
 - ISSO Contact: {enter Name} – {enter phone number}

- **SYSTEM B (Organization B Name, City, ST)**
 - Organization B Company Name
Organization B Division/Section Name
Organization B Address 1
Organization B Address 2
Organization B Address 3
Organization B Address 1
 - Allow {enter connection type to destination device}
 - Operational and Technical Contact: {enter Name} – {enter phone number}

COMMUNICATIONS

Frequent formal communications are essential to ensure the successful management and operation of the interconnection. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels. All communications described herein must be conducted in writing unless otherwise noted.

The owners of System A and System B agree to designate and provide contact information for technical leads for their respective system, and to facilitate direct contacts between technical leads to support the management and operation of the interconnection. To safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit, the parties agree to provide notice of specific events within the time frames indicated below:

- **Security Incidents:** Technical staff will immediately notify their designated counterparts by telephone or e-mail when a security incident(s) is detected. The other party may take steps to determine whether its system has been compromised and to take appropriate security precautions. The system owner will receive formal notification in writing within five (5) business days after detection of the incident(s).
- **Disasters and Other Contingencies:** Technical staff will immediately notify their designated counterparts by telephone or e-mail in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems.
- **Material Changes to System Configuration:** Planned technical changes to the system architecture will be reported to technical staff before such changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture within one (1) month of implementation.
- **Personnel Changes:** The parties agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, both parties will provide notification of any changes in point of contact information. Both parties also will provide notification of changes to user profiles, including users who resign or change job responsibilities.

SECURITY

Both parties agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit. Each party certifies its respective system is designed, managed, and operated in compliance with all relevant federal laws, regulations, and policies. Current security on the connection is controlled {enter control description here}.

Description Example - controlled by the firewall iptables and configuration scripts on the LDM server. All traffic will be restricted to communication and data transfer of allowed ip addresses only.

TIMELINE

This agreement will remain in effect for (3) years from the last date in the signature block below. After (3) years, this agreement will expire. The agreement and documentation should be reviewed for content and contact changes annually. If the parties wish to continue this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. The newly signed agreement should explicitly supersede the old agreement, which should be referenced by title and date. If one or both of the parties wish to terminate this agreement prematurely, they may do so upon 30 days advanced written notice or in the event of a security incident that necessitates an immediate response.

SIGNATORY AUTHORITY

I agree to and will abide by the terms of this agreement.

**National Weather Service
Central Region WAN/LAN
System Owner**

**Org B Company Name
Org B Company Div/Section
Org B City, ST
Org B Designated Approving
Authority Title**

{Enter SO name}

Date

{Enter DAA name}

Date

INTERCONNECTION SECURITY AGREEMENT

Between

**“National Weather Service -
NWS, Central Region”**

And

“Organization B Name”

{Date of Agreement entered by CRH}

Organization A

**National Weather Service
Central Region
20-30-xx-xxx**

Organization B

**Org B Company Name
Org B Division/Section Name**

1. INTERCONNECTION STATEMENT OF REQUIREMENTS.

a. The requirements for interconnection between the “National Weather Service (NWS) – Central Region” and “Organization B Name” located at “Organization B Address, City, ST Zip”, is for the express purpose of transmitting {enter type of data here} information between named parties. The information will be exchanged in accordance with the technical specifications and definitions agreed to by both parties.

Data Example - hydrologic products and hydrologic

b. No other services are authorized under this agreement. Other than the passing of data stated in paragraph 1a, and only between ip addresses in paragraph 1c are authorized.

c. The pertinent details of the interconnection are:

- {enter connection detail 1 here}
- {enter connection detail 2 here}
- {enter connection detail 3 here}
- {enter connection detail ...x here}

Example of details for LDM connection:

- NDSU LDM host is iwi.ndsu.nodak.edu/xxx.xxx.xxx.xxx
- CRH LDM host is ldm.crh.noaa.gov/xxx.xxx.xxx.xxx.
- Connection between NDSU and CRH is public domain.
- Data sent by NDSU is delivered to LDM port 388.
- Data sent by CRH is delivered to LDM port 388.

d. {Enter Organization B name here}, without exception and any expectation of privacy, freely submits all information transmitted to the CRH. CRH, without exception and any expectation of privacy, freely submits all information transmitted to the {Enter Organization B name here}.

2. SYSTEM SECURITY CONSIDERATIONS.

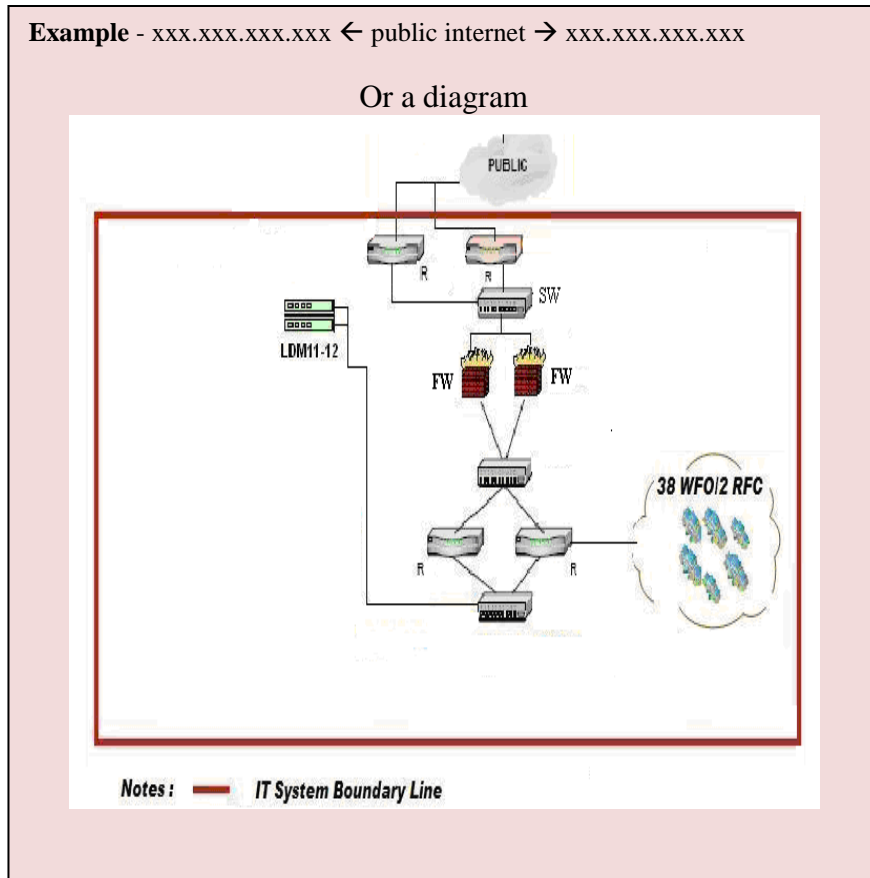
List all appropriate security controls in this section. Delete any that don't apply.

- a. The interconnection between Org A and Org B is solely a {enter type of connection here} connection.
- b. No data is passed on this line which requires security.
- c. All data is open unless otherwise stated.
- d. The sensitivity of all data filed is unclassified.
- e. Policy documents that govern the protection of the data are under the Department of Commerce IT Security Program Policy and Minimum Implementation Standards (DOC ITSPP) document.
- f. All security incidents that have any effect on the security posture of CRH must be reported to NOAA Computer Incident Response Team (N-CIRT) via the web-based NOAA 47-43 form at https://www.csp.noaa.gov/V3_Form/index.php or by telephone at 301-713-9111.

3. **TOPOLOGICAL DRAWING.** The two systems are joined by {enter protocol and/or port number here}. The line connection between CRH and {Org B} is public domain internet.

{Enter Org B Name} interconnection {Enter Org A Name}

{Enter a topology diagram or simple describe interconnection here}



SECTION 4 - SIGNATORY AUTHORITY. This ISA is valid for three years after the last date on either signature below. It will be reviewed and validated annually and updated as necessary. This agreement may be terminated upon 30 days advanced written notice by either party or in the event of a security exception that would necessitate an immediate response.

**National Weather Service
System and Central Region
WAN/LAN
System Owner**

**Org B Company Name
Org B Company Div/Section**

**Org B City, ST
Org B Designated Approving
Authority Title**

{Enter SO name} Date

{Enter DAA name} Date

APPENDIX F **Restricted/Controlled Area Sign – Sample**



APPENDIX G HAM Usage Guideline Example

NWS Central Region IT Resource Acceptable Use Guidelines For HAM Operator/Other⁹ Volunteers

Central Region's purpose for establishing IT Resource Acceptable Use Guidelines is to provide the volunteer an awareness of the acceptable use of government IT resources and to provide an overview of actions required to protect the IT resource. The principles here are based upon the following goals:

- Ensure the availability of data and processing resources.
- Ensure the integrity of data processing operations and protect them from unauthorized use.
- Ensure the confidentiality of the processed data, and prevent unauthorized disclosure or use.

Effective security is a team effort involving the participation and support of every computer user. Knowing these guidelines and conducting activities accordingly will establish a culture of openness, trust and will protect the government's IT resources.

Central Region is committed to protecting employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of government. These systems are to be used for business purposes in serving the interests of the National Weather Service, and of our clients and customers in the course of normal operations. Inappropriate use exposes the NWS to risks including virus attacks, compromise of network systems and services, and legal issues.

Volunteer Uses:

Acceptable Uses

- Retrieve and view real-time to near real-time meteorological data from WWW to assist in duties
- Retrieve and view watch and warning products from the NWS website to assist in duties
- Printing products from websites to assist in duties

Unacceptable Uses

- Retrieving and viewing any website not associated with assigned duties
- Printing from any website not associated with assigned duties
- File transfer
- Email
- Circumventing user authentication or security of any host, network or account.

Usage Statement

I, _____ have reviewed and understand the above IT
(Print full name)

Resource Acceptable Use Policy. I agree to provide protection in my use of government IT resources. I fully understand the use of these IT resources is solely used for official purposes in providing weather information to other volunteers in the course of assisting the NWS.

(Date)

⁹ temporary workers (e. g., HAM operators, etc.) who will not use IT resources for more than a month annually

APPENDIX H Annual Privileged Accounts Verification Form

NWS CENTRAL REGION ANNUAL PRIVILEGED ACCOUNTS VERIFICATION

Purpose and Scope: This form is used to conduct and document the annual review of all privileged accounts within the NWS CR WAN/LAN system. In order to manage and maintain the CR WAN/LAN, certain individuals must be granted privileged rights within a particular IT system far in excess of that of a typical user of that IT system. These individuals, due to their access to the IT system, must understand the impact of their actions when using privileged accounts.

Definitions:

Privileged Account - The IT system accounts utilized by privileged users to perform management and maintenance of the system.

Privileged Use - Use of rights beyond that of a typical IT system user to manage and maintain an IT system.

Privileged User - The users granted the rights of Privileged Use.

System Administrator - Is a privileged user.

Privileged Accounts - The level of privileges of actual system accounts vary widely from system to system and depend upon the privileged role being fulfilled. Typical operating system level accounts are generically referred to as "administrator" or "root" level accounts. Other privileged users, such as account management personnel may only have rights to create, delete and change user accounts.

Local Computer Privileges - There are two main categories of privileged users on a computer or network. These categories include:

1. Power user (PU) - Can change many system settings and install programs that don't affect Windows system files.
2. Administrators (Admin) - Have complete access to read and write any data on the system and add or remove any programs or change system settings. Only users with special training or demonstrable skills should be allowed to change system settings and install programs that are not operating system programs.

PRIVILEGED ACCOUNTS SECTION

Type of Privileged Account	Name	System & justification for privileged account

LOCAL SECURITY MANAGER'S (SM) REVIEW AND VERIFICATION

SM acknowledges and verifies: I have reviewed the above privileged account users and verify there is an operational need for them to have a privileged account/s. I also verify they have the necessary training and skills to perform changes within the system at the assigned privileged level. Each member has been briefed on the proper use of the account and **understands that their privileged account is not to be used in lieu of their normal user account.**

Security Manger's Name:	SID:
Security Manger's Signature:	Date:
	Phone:

APPENDIX I EMRS Report Auditing A-26 Sample

GENERAL INFORMATION

NEW RECORD

Date of Audit: 07/01/2010 07:00 (Local)

1. Open Date: 07/01/2010 07:00 (Local)

2. Op Initials: []

3. Response Priority: Routine Immediate Low Not Applicable

4. Close Date: 07/01/2010 15:00 (Local)

5. Maintenance Description: 999 characters left
IT SYSTEMS

Audit Scope and Logs Reviewed: []

AUDIT SCOPE: [DESKTOP|SERVER|WAP|FIREWALL|LAN|LOG(S) REVIEWED: [WINDOWS EVENT|LOGWATCH|OTHER LOCAL]

EQUIPMENT INFORMATION

6. Station ID: PAH

7. Equipment Code: PCSA

8. Serial Number: 001

9. TM: S

10. AT: X

11. How Mal: 999

Alert: []

MISCELLANEOUS INFORMATION

15. Maintenance Comments: 724 characters left

FINDINGS: [NARRATIVE HERE]

16. Tech Initials: CDC

SPECIAL PURPOSE REPORT INFORMATION

17. SPECIAL PURPOSE REPORT INFORMATION

a. Mod No. []

b. Mod Act/Deact Date: []

c. Block C: ITSA

d. Trouble Ticket No.: 8123

e. USOS Outage Doc No. []

NOAA 47-43 Report ID: []

Contract Maintenance Disclaimer:

Buttons: Commit A26, Schedule on Commit, Place on Hold, Schedule on Hold, Copy A26, New A26, Cancel