NATIONAL WEATHER SERVICE POLICY DIRECTIVE 60-7
12 December 2011

Information Technology

Information Technology Security Policy

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

OPR: OCIO (Sherry Richardson) **Certified by:** OCIO (Iftikhar Jamil)
Type of Issuance: Routine

SUMMARY OF REVISIONS: Supersedes NWS Policy Directive 60-7, Information Technology Security Policy, and dated August 28, 2003.

1. This directive establishes the policy framework for the implementation, maintenance, and oversight of the National Weather Service (NWS) Information Technology (IT) Security Program.

2. NWS IT security policy derives from, and will henceforth be managed in accordance with, Department of Commerce (DOC) and National Oceanic & Atmospheric Administration (NOAA) IT security policies, standards, and practices, including DOC Commerce Interim Technical Requirements (CITRs). The DOC and NOAA IT security requirements are based upon Federal statute, including the Clinger-Cohen Act of 1996 and Federal Information Security Act (FISMA) of 2002; Federal regulatory requirements, including Office of Management and Budget (OMB) regulations and Federal Information Processing Standards (FIPS); and Special Publications of the National Institutes of Standards and Technology (NIST). These documents can be accessed at https://www.csp.noaa.gov/policies/ .

3. The Assistant Administrator for National Weather Services (AA/NWS) is responsible for ensuring the implementation of information security protection measures commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of NWS systems and information.

3.1 Pursuant to Section 4 of the NOAA IT Security Manual 212-1301, the NWS Chief Information Officer (CIO) has been delegated as the Authorizing Official (AO) for all NWS systems and has further delegated the AO authority to the NWS Financial Management Center (FMC) Directors for all IT systems under their direct control. This authority cannot be further delegated.

3.2 The NWS CIO has designated in writing a Chief Information Security Officer (CISO), Information Technology Security Officer (ITSO), and an alternate ITSO, who will provide assistance to FMC Directors and staff in ensuring the development, implementation,

maintenance, and reporting requirements established by Federal law and DOC and NOAA IT Security policies, standards, and practices.

3.3 FMC Directors will appoint in writing qualified individuals to serve as System Owners for all the information systems assigned to them.

3.4 The System Owner will appoint in writing an Information Systems Security Officer (ISSO) who will ensure the NWS system is documented and protected in accordance with laws, NOAA, and NWS policy. The ISSO will not also function as the system administrator for any system which he/she serves as an ISSO to ensure separation of duties.

3.5 System administrators will be assigned to systems to provide general IT support for operations. In additional they are and to provide technical assistance and implementation in the secure configuration of the systems and in response to security incidents as directed by authorized incident responders the ISSO. Maybe a system administrator will not serve as the system administrator and ISSO on the same system.

4.0 Each user of NWS IT resources is responsible for understanding and complying with Federal IT security statutes and DOC and, NOAA, and NWS IT Security policies, standards, and practices. Any questions regarding compliance with these requirements documents should shall be raised with the user's immediate supervisor and then the system ISSO. If required, the ISSO will escalate the issue to the NWS CISO.

5. This policy directive is supported by the references listed in Attachment 1.

___Signed_____11/28/2011_____
John L. Hayes Date
Assistant Administrator for Weather Services

Attachment 1

REFERENCES

The NWS Information Technology Security Policy is based upon Federal statutes, OMB regulations, and Federal Information Processing Standards as incorporated in the Department of Commerce and NOAA IT security polices, standards, and practices as set forth below. This list is not all inclusive.

- The Paperwork Reduction Act, 44 USC § 3501, et. seq.
- Federal Information Security Management Act of 2002
- Clinger Cohen Act of 1996
- The Privacy Act of 1974 as amended
- Office of Management and Budget Circular A-130, Appendix III, Management of Federal Information Resources
- Federal Information Processing Standards as set out at http://csrc.nist.gov/publications/PubsFIPS.html
- U.S. Department of Commerce IT Security Program Policy and Minimum Implementation Standards
- U.S. Department of Commerce Physical Security Manual
- U.S. Department of Commerce National Security Information Manual
- U.S. Department of Commerce Information Technology Security Manual
- U.S. Department of Commerce Information Technology Management Handbook
- Department Administrative Order 207-1, Security Programs
- NOAA Administrative Order 212-13, Information Technology Security Policy
- NOAA 212-1300, Information Technology Security Manual
- CITR 001, Federal Desktop Core Configuration (FDCC), January 2009
- CITR 002, Safeguarding Data on Foreign Travel, June 2008
- CITR 003, Continuous Monitoring Plan (CA-7), November 2008
- CITR 004, Certification and Accreditation Process, February 2008
- CITR 005, Removable Media Devices, December 11, 2008
- CITR 006, Information System Security Training for Significant Roles, September 2010
- CITR 008, Remote Access, September 2009

- CITR 009, Password Requirements, September 2009
- CITR 011, Peer-to-Peer Technology, September 2009
- Special Publications of the National Institute of Standards and Technology (NIST) as set out at http://csrc.nist.gov/publications/PubsSPs.html