NATIONAL WEATHER SERVICE Instruction 60-701
28 May 2012

Information Technology
IT Security

Assignment of Responsibilities

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

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

SUMMARY OF REVISIONS: Superseded NWS Instruction 60-701, Assignment of Responsibilities, and dated November 14, 2003. Deleted definitions section and added additional roles and responsibilities. Revised some roles and responsibilities.

Signed 5/14/2012
Iftikhar Jamil Date
NWS Chief Information Officer

Table of Contents

1 Introduction 3

2 Assignment of Responsibilities 3
2.1 Chief Information Officer (CIO) 3
2.2 Chief Information Security Officer (CISO) 3
2.3 NWS IT Security Officer (ITSO) 4
2.4 Authorizing Official (AO) 5
2.5 System Owner (SO) 5
2.6 IT System Security Officers (ISSO) 6
2.7 Certification Agent/Certification Assessor (CA) 7
2.8 Network and System Administrators (N/SA) 7
2.9 End Users 9
2.10 Chief Financial Officer (CFO) 9

1 Introduction. The National Weather Service (NWS) Information Technology (IT) Security Program establishes the required framework of security controls that ensure the inclusion of security in the daily operation and management of NWS IT Systems and Resources. The management structure provides a foundation for effectively managing the confidentiality, integrity, and availability of the information and the information systems supporting the mission of the NWS. This Instruction defines the roles and responsibilities specified for all NWS employees (federal and contractor).

2 Assignment of Responsibilities. The structure for security implementation and administration within NWS is defined within this instruction, which establishes the following authorities and responsibilities:

2.1 NWS Chief Information Officer (CIO)

2.1.1 Oversees the NWS IT Security Program.

2.1.2 Appoints, in writing, a Chief Information Security Officer (CISO) to implement the IT Security Program.

2.1.3 Ensures the implementation of the NWS IT Security Program which complies with NOAA guidance in regards to Federal Information Security Management Act of 2002 (FISMA).

2.1.4 Reports the status of the NWS IT Security Program to the NWS Assistant Administrator (AA), and identifies any weaknesses of the program.

2.1.5 Approves and issues policy and/or instructions that establish a framework for the NWS IT Security Program.

2.1.6 Monitors, evaluates, and reports the status of IT security within NWS to the NOAA CIO and the NWS AA.

2.1.7 Functions as the AO for all NWS systems unless the role of AO is re-delegated to the Financial Management Center (FMC) directors.

2.1.8 Responsible for taking annual role-based security training commensurate with the role, per Department of Commerce (DOC), Commerce Interim Technical Requirements (CITR) CITR-006: Information System Security Training for Significant Roles.

2.2 NWS Chief Information Security Officer (CISO)

2.2.1 Responsible for ensuring that the appropriate operational security posture is maintained for NWS information systems and programs.

2.2.2 Designates in writing the NWS Information Technology Security Officers which will implement the IT Security Program.

2.2.3 Ensures each NWS system with a FISMA ID has an appointed ISSO.

2.2.4 Ensures that all IT systems are identified and accredited.

2.2.5 Serves as a voting member of the NOAA IT Security Council and attends regularly scheduled meetings to obtain current information on issues relating to Federal, Department of Commerce (DOC), and NOAA IT security law, policies, regulations, guidelines or concerns.

2.2.6 Provides security program budgetary advice consistent with business needs to appropriate levels of management for planning purposes.

2.2.7 Advises appropriate levels of management about technological advances in IT security which can be used on an organizational scale to improve the security of the system or can keep the same level of security at a reduced cost.

2.2.8 Responsible for maintaining a security certification as specified by DOC CITR-006.

2.3 <u>NWS IT Security Officer (ITSO)</u>

2.3.1 Serves as the central point of contact for the NWS IT Security Program for all information systems.

2.3.2 Develops and maintains NWS IT security policy, procedures, standards, and guidance consistent with Federal, DOC, and NOAA requirements.

2.3.3 Ensures that all systems have in place effective security documentation, including a risk assessment, current IT security plans that accurately reflect system status, annual system assessments, current tested contingency plans, and current Authorization and Assessment (A&A).

2.3.4 Conducts continuous monitoring of the NWS IT Security Program to ensure effective implementation of and compliance with established policies and procedures.

2.3.5 Establishes procedures for an IT security awareness and training program for all NWS personnel including specialized training as necessary for systems administrators, Contracting Officer’s Technical Representatives (COTRs), etc.

2.3.6 Acts as the NWS's central point of contact for all incidents.

2.3.7 Provides information to appropriate NWS personnel concerning risks and potential risks to NWS systems.

2.3.8 If requested by the SO and approved by the CISO, can function as the Certification Agent/Certification Assessor (CA) for the requesting NWS system(s).

2.3.9 Responsible for maintaining a security certification as specified by DOC CITR-006.

2.4 Authorizing Official (AO)

2.4.1 Oversees the budget and business operations of the information systems within their area of responsibility.

2.4.2 Assumes responsibility for operating an information system at an acceptable level of risk to operations, assets, or individuals by granting an Authorization to Operate.

2.4.3 Approves system security requirements, including but not limited to, the System Security Plans (SSP), Interconnection Security Agreements (ISA), Memorandums of Agreements (MOA) and/or Memorandums of Understanding (MOU).

2.4.4 Responsible for taking annual role-based security training commensurate with the role, per DOC CITR-006: Information System Security Training for Significant Roles.

2.4.5 Appoints qualified personnel in writing to act and assume the roles and responsibilities of Information System Security Officer (ISSO).

2.5 System Owner (SO)

2.5.1 Ensures security considerations in application systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e., life cycle management).

2.5.2 Responsible for ensuring all controls are in effect or have associated POAMs and all POAMs are closed on schedule.

2.5.3 Responsible for establishing, training, testing and updating IT contingency plan.

2.5.4 Ensures the security of data residing on their system(s).

2.5.5 Determines and implements an appropriate level of security commensurate with the FIPS 199 categorization of their system.

2.5.6 Maintains an updated list of hardware and software inventory operated/used by the system.

2.5.7 Develops and maintains security plans and contingency plans for all FISMA ID systems under their responsibility.

2.5.8 Performs security impact analysis whenever the level of security on a system or network is modified in order to re-evaluate sensitivity of the system, risks, and mitigation strategies.

2.5.9 Conducts assessments of system safeguards and program elements, and ensures initial authorization and assessment of the system as well as the annual assessments for continuous monitoring.

2.5.10 Reports all incidents to the NWS ITSO and NOAA Computer Incident Response Team (NCIRT).

2.5.11 Responsible for taking annual role-based security training commensurate with the role and ensures that system personnel are properly designated monitored and receive appropriate role based IT security training as designated in DOC CITR-006.

2.5.12 Ensures IT contracts pertaining to the system include provisions for security.

2.5.13 Ensures appropriate system-level security controls and documentation are maintained for the information system of their responsibility.

2.5.14 Recommends to the AO in writing, qualified personnel to act and assume the roles and responsibilities of Information System Security Officer (ISSO).

2.6 <u>Information System Security Officer(s) (ISSO)</u>

2.6.1 Advises the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e., life cycle management).

2.6.2 Assists in the determination of an appropriate level of security commensurate with the level of sensitivity.

2.6.3 Assists in the development and maintenance of security and contingency plans for all FISMA ID systems under their responsibility.

2.6.4 Participates in security impact analysis to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies.

2.6.5 Participates in security impact analysis of system safeguards and program elements and in authorization and assessment (A&A) of the system for continuous monitoring.

2.6.6 Is the point of contact for all security incidents within their area of responsibility and reports using the NOAA 47-43 form to the NOAA Computer Incident Response Team (NCIRT).

2.6.7 Handles and investigates incidents in cooperation with and under direction of the NWS ITSO and NCIRT.

2.6.8 Participates in vulnerability scanning and penetration testing of systems/networks.

2.6.9 Functions as the network and/or systems administrator for any system they are assigned to as the ISSO unless a waiver with justification is requested from the NWS AO. Separation of duties dictates that an ISSO cannot be a systems administrator for the same IT system.

2.6.10 Ensure all user accounts are disabled within 24 hours of notification of user's separation from NWS and immediately for individuals being separated for adverse reasons.

2.6.11 Monitor and review security policy, practices, and procedures.

2.6.12 Ensure the security of all interfaces between NWS and external systems, develop and maintain interconnection documentation (ISA, SLA, MOU, and MOA).

2.6.13 Responsible for maintaining a security certification as specified by DOC CITR-006.

2.7 Certification Agent/Certification Assessor (CA).

2.7.1 Conduct security assessments for all FIPS 199 systems. For Moderate and High systems, the CA must be independent. Independent is defined as independent from the persons directly responsible for the development and day to day operation of the systems.

2.7.2 Assist System Owners and ISSOs in determining whether existing assessment results may be reused.

2.7.3 Provide recommended mitigation strategies for identified vulnerabilities attributed to NWS information systems.

2.8 Network and System Administrators (N/SA).

2.8.1 Responsible for specific aspects of system security, such as adding and deleting user accounts as authorized by the system owner or ISSO, patching systems, implementing secure configurations as prescribed in the system security plans, and normal operations of the system in keeping with job requirements.

2.8.2 Responsible for implementing DOC, NOAA, and NWS security policies, procedures, and guidelines on local systems and networks.

2.8.3 Assists in the development and maintenance of security and contingency plans for FISMA ID systems under their responsibility.

2.8.4 Participates in security impact analysis to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies.

2.8.5 Participates in assessments of system safeguards and program elements and in authorization and assessment of the system.

2.8.6 Evaluates proposed technical security controls to assure proper integration with other system operations.

2.8.7 Identifies requirements for resources needed to effectively implement technical security controls.

2.8.8 Ensures the integrity of technical security controls.

2.8.9 Reports all incidents to the system ISSO and system owner and assists in the investigation of incidents as directed.

2.8.10 Reads and understands all applicable training and awareness materials.

2.8.11 Reads and understands all applicable use policies or other rules of behavior regarding use or abuse of operating unit IT resources.

2.8.12 Develops system administration and operational procedures and manuals.

2.8.13 Evaluates and develops procedures that assure proper integration of service continuity with other system operations.

2.8.14 Knows which systems or parts of systems for which they are directly responsible (e.g., network equipment, servers, LAN, etc.).

2.8.15 Knows the sensitivity of the data they handle and take appropriate measures to protect it.

2.8.16 Functions as the ISSO on any system he/she functions as the system administrator unless a waiver with justification is requested from the NWS AO.

2.8.17 Responsible for maintaining the system(s) baseline(s), coordinating changes with the ISSO, SO and Change Control Board (CCB) and obtaining approval for baseline deviations.

2.9 End Users.

2.9.1 Aware of the sensitivity of the information they are responsible for and the proper handling thereof in order to maintain the confidentiality, integrity and availability of the information.

2.9.2 Reads and understands all applicable training and awareness materials.

2.9.3 Reads and understands all applicable use policies and other rules of behavior regarding use or abuse of operating unit IT resources.

2.9.4 Knows which systems or parts of systems for which they are directly responsible (printer, desktop, etc.).

2.9.5 Reports all incidents to their appropriate system administrator and ISSO in a timely manner.

2.9.6 Knows and abides by all applicable DOC, NOAA and NWS policies and procedures.

2.9.7 Successfully completes annual IT Security Awareness training and by doing so, re-certifies their knowledge of and adherence to the NWS Rules of Behavior.

2.10 Chief Financial Officer

2.10.1 Review cost estimates of each major information security investment.

2.10.2 Review and report financial management information on security investments, as required.

2.10.3 Comply with legislative and OMB defined responsibilities as they relate to IT capital investments.