Department of Commerce · National Oceanic & Atmospheric Administration · National Weather Service

NATIONAL WEATHER SERVICE Instruction 60-701
APRIL 14, 2020

Information Technology

IT Security Roles and Responsibilities

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

OPR: W/ACIO (Paula Reis) **Certified by:** W/CIO (Beckie Koonge)
Type of Issuance: Routine

This is a living document that is changed as required to reflect system, operational, or organizational changes.

SUMMARY OF REVISIONS: Superseded NWS Instruction 60-701, Assignment of Responsibilities, and dated 28 May 2012. This is a routine review and update of this policy to keep this document current, increase applicability, and reduce ambiguity. Changes include: a) Revised some roles and responsibilities, b) Added the Enterprise Architect (EA) role and c) Editorial changes to ensure clear and concise policy guidance, and improve readability.

KOONGE.BECKIE.A.1408306880 Digitally signed by KOONGE.BECKIE.A.1408306880 Date: 2020.03.31 10:47:56 -04'00'

Beckie Koonge Date
Acting NWS Assistant Chief Information Officer (ACIO)

Table of Contents **Page**

1.0. 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). It is based on guidance provided by sources such as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Department of Commerce (DOC) Information Technology Security Baseline Policy (ITSBP) and National Oceanic and Atmospheric Administration (NOAA) Information Technology Security Manual (ITSM). While there may be some redundant responsibilities, the goal is to have the information in one document, focused on NWS IT security roles.

2.0. IT Security Roles and Responsibilities

The structure for security implementation and administration within NWS is defined within this instruction and establishes the following roles and responsibilities:

2.1 Assistant Chief Information Officer (ACIO)

2.1.1. Oversees the NWS IT Security Program ensuring mission first approach.

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 (FISMA) of 2014 (as amended).

2.1.4. Reports the status of the NWS IT Security Program to the NWS Assistant Administrator (AA) and monitors and responds to changes in the threat landscape.

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. Responsible for taking annual role-based security training commensurate with the role, per DOC and NOAA requirement.

2.1.8. Serves as the Co-Authorizing Official (AO) for the authorization of all low and moderate systems under his or her direct ownership authority.

2.2. 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 (ITSOs) who will implement the IT Security Program.

2.2.3. Ensures each NWS system with a FISMA ID has an appointed Information System Security Officer (ISSO).

2.2.4. Ensures that all IT systems are identified and has an Authority to Operate (ATO).

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, 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 at a minimum commensurate with DOC and NOAA requirements.

2.3. Enterprise Architect (EA)

2.3.1. Assists in reducing complexity within the IT infrastructure to facilitate security.

2.3.2. Collaborates with System Owners, Authorizing Officials and IT Security Officers to facilitate authorization boundary determinations.

2.3.3. Coordinates with security and privacy Subject Matter Experts (SMEs) to determine the optimal placement of systems/system elements within the NWS IT architecture, and to address security and privacy issues between systems and the IT architecture.

2.4. IT Security Officer (ITSO)

2.4.1. Serves as the liaison for the NWS IT Security Program for all information systems.

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

2.4.3. 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).

2.4.4. Conducts continuous monitoring of the NWS FISMA systems to ensureeffective implementation of and compliance with established policies and procedures.

2.4.5. Establishes procedures for an IT security awareness and training program for allNWS personnel, including specialized role-based training as necessary for systems administrators, etc.

2.4.6. Acts as the NWS central point of contact for all security related incidents.

2.4.7. Provides information to appropriate NWS personnel concerning risks and potentialrisks to NWS systems.

2.4.8. If requested by the SO and approved by the CISO, can function as the SecurityControl Assessor (SCA) for the requesting NWS system(s).

2.4.9. Responsible for maintaining a security certification at a minimum commensurate with DOC and NOAA requirements.

2.5. Authorizing Official (AO)

2.5.1. Oversees the budget and business operations of the information systems within theirarea of responsibility.

2.5.2. Determines the authorization boundary in collaboration with NWS stakeholders.

2.5.3. Assumes responsibility for operating an information system and collaborate with theCo-AO for an acceptable level of risk to operations, assets, or individuals by granting an Authorization to Operate (ATO).

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

2.5.5. Responsible for taking annual role-based security training commensurate with the role.

2.5.6. Appoints qualified personnel in writing to act and assume the roles and responsibilities of a System Owner (SO).

2.5.7. Appoints qualified personnel in writing to act and assume the roles and responsibilitiesof an Information System Security Officer (ISSO).

2.6. System Owner (SO)

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

2.6.2. Responsible for ensuring adequate documentation of security controls both in place and planned. This includes tailoring of applicable controls in FIPS 200.

2.6.3. Responsible for ensuring all POA&Ms are developed, maintained and reviewed at a minimum monthly in the Cyber Security Assessment and Management (CSAM) tool.

2.6.4. Responsible for identifying viable and feasible solutions to ensure the closure of POA&Ms at the agreed upon dates.

2.6.5. Ensures data both in transit and at rest receives adequate protection commensurate with the risk impact associated with the data and Federal regulations (i.e. FIPS 140-3).

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

2.6.7. Responsible for ensuring hardware and software inventory for their respective FISMA systems are adequately and accurately reviewed, and documented at least annually.

2.6.8. Responsible for ensuring the identification of End of Life (EOL) hardware and software for their respective FISMA systems and plan adequately for replacement or upgrades in order to ensure the security posture of the system.

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

2.6.10. Responsible for ensuring that all code/application onboarding within their environment are developed with adequate security controls, tested in a lower environment (i.e. development/test) before being deployed into production as well as ongoing maintenance of the code throughout its Software Development Life Cycle (SDLC).

2.6.11. Performs security impact analysis prior to implementing any system or network changes in order to re-evaluate sensitivity of the system, risks, and mitigation strategies.

2.6.12. 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.

2.6.13. Reports all incidents to the NWS ITSO and NOAA Computer Incident Response Team (N-CIRT).

2.6.14. 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 per DOC and NOAA requirements.

2.6.15. Responsible for defining the annual role-based security training for system administrators or those with privileged access. System administrators or those with privileged access are required to have a higher degree of technical knowledge in effective security practices and implementation.

2.6.16. Ensures IT contracts pertaining to the system include provisions for security as defined by the Federal Information Security Modernization Act (FISMA) of 2014 (as amended) and Service Level Agreements (SLAs) as applicable.

2.6.17. Ensures appropriate system-level security controls and documentation are maintained for the information system of their responsibility on an ongoing basis.

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

2.7. Information System Security Officer (ISSO)

2.7.1. 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 and data management).

2.7.2. Assists in the determination of an appropriate level of security commensurate with the level of sensitivity and risk impact.

2.7.3. Develops and maintains all applicable security documentation (i.e. System Security Plan, Contingency Plan, Configuration Management Plan, etc.) on behalf of the SO for all FISMA ID systems under their responsibility with support from key stakeholders.

2.7.4. Conducts a Security Impact Analysis (SIA) when there is a significant change to their respective FISMA system (i.e. onboarding new applications, system update, decommission, etc.) and engages with key stakeholder to ensure periodical review and potential re-evaluation of system sensitivity, data risks, and mitigation strategies.

2.7.5. Coordinates with personnel with information security responsibilities (e.g., System Owner, System Administrators, Security Managers, Security Engineers, etc.) to ensure that security impact analyses are integrated in the Configuration Change Management and continuous monitoring process.

2.7.6. Is the point of contact for all security incidents within their area of responsibility and reports using the Incident Response Reporting Application (NIRRA) or equivalent application determined by NOAA.

2.7.7. Provides FISMA ID specific information to facilitate the investigation and mitigation of security incidents.

2.7.8. Works with SO and other key stakeholders to ensure that hardware and software inventory for all their respective FISMA systems are adequately documented, reviewed and updated at a minimum annually or if there is a significant change.

2.7.9. Assists or facilitates scans (i.e. Nessus, Nmap, manual and/or automated code reviews, pentest, etc.) and aids with the mitigation process for identified vulnerabilities per applicable remediation timeframes.

2.7.10. Will not function 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.

2.7.11. Oversees that 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.

2.7.12. Monitors and reviews security policy, and communicate these changes to applicable stakeholders as needed.

2.7.13. Ensures the security of all interfaces whether internal or external are captured, for external systems/ entities facilitates the development, approval and consequent reviews and updates of the interconnection documentation (i.e. ISA, SLA, MOU, and MOA).

2.7.14. Obtains and maintains a role-approved professional certification at a minimum commensurate with DOC and NOAA requirements.

2.7.15. Develops, tracks, and manages POA&Ms on behalf of the SO.

2.8. Security Control Assessor (SCA)

2.8.1. Conducts security assessments for all FISMA systems. For Moderate and High systems, the SCA must be independent. Independent is defined as independent from the persons directly responsible for the development and day to day operation of the systems.

2.8.2. Assists System Owners and ISSOs in determining whether existing assessment results may be reused.

2.8.3. Provides recommended mitigation strategies for identified vulnerabilities attributed to NWS information systems.

2.9. System Administrator* (SA)

*The system administrator role includes the following: database administrators, network administrators, web administrators, and application administrators, etc.

2.9.1. Responsible for implementing DOC, NOAA, and NWS security policies, procedures, and guidelines on local systems and other applicable areas.

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

2.9.3. Responsible for specific aspects of system security, such as adding and deleting user accounts as authorized by the SO or ISSO.

2.9.4. Responsible for vulnerability scanning, patching systems, implementing secure configurations as prescribed in the system security plans, and normal operations of the system in collaboration with the SO and ISSO.

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

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

2.9.7. Participates in the initial and annual assessments of system safeguards and program elements.

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

2.9.9. Ensures the integrity of technical security controls.

2.9.10. Reports all incidents to the SO and ISSO and assists in the investigation of incidents as directed.

2.9.11. Reads and adheres to all applicable training, use policies or other rules of behavior regarding use and abuse of operating unit IT resources.

2.9.12. Develops, documents, review and updates at a minimum annually system administration and operational procedures and manuals.

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

2.9.14. Assists key stakeholders to adequately monitor the hardware and software EOL for their respective FISMA system and make recommendations for the planning, testing, deployment and consequent decommission of inventory of the system.

2.9.15. Knowledgeable about which systems or parts of their respective FISMA systems for which they are directly responsible (e.g., network equipment, servers, LAN, etc.).

2.9.16. Facilitates the documentation of all applicable topological diagram and their maintenance.

2.9.17. Takes appropriate measures to protect the sensitive data they handle.

2.9.18. Will not function as the ISSO on any system he/she functions as the SA unless a waiver with justification is requested from the NWS AO.

2.9.19. Responsible for taking the NOAA annual security awareness training and completing the annual role-based security training for system administrators or those with privileged access as defined by the SO.

2.9.20. Works with the SO and ISSO to ensure hardware and software inventory for their FISMA ID are adequately documented, reviewed and updated at a minimum annually or when

there is a significant change.

2.9.21. Responsible for adhering to NWS and industry security baseline guidance (i.e. STIGS, CIS Benchmarks etc.), hardening of their environment and facilitating security changes via the Change Control Board (CCB) or Change Advisory Board (CAB).

2.10 System User

2.10.1. Knows and abides by all applicable DOC, NOAA and NWS policies and procedures (as amended).

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

2.10.3. Reads and adheres to all applicable training and awareness materials, use policies and other rules of behavior regarding use or abuse of operating unit IT resources.

2.10.4. Knows which system components for which they are directly responsible for (printer, desktop, etc.).

2.10.5. Reports all incidents to their appropriate system administrator and ISSO as soon as an incident occurs.

2.10.6. Will utilize a loaner Government Furnished Equipment (GFE) while on foreign travel when there is an official business need and comply with foreign travel requirements.

3.0 References

- DOC ITSBP Version 1.0, June 2019
- NOAA Information Technology Security Manual (ITSM) 212-1301 Version 6.0, May 2019
- NIST Risk Management Framework for Information Systems and Organizations. Special Publication 800-37 Revision 2, December 2018