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

# *NATIONAL WEATHER SERVICE INSTRUCTION 60-703*
***MAY 12, 2021***

***Information Technology***

***Information Technology Security Policy 60-7***

# *VULNERABILITY MANAGEMENT*

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

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

***SUMMARY OF REVISIONS:*** Supersedes NWS Instruction 60-703, *Vulnerability Identification*, *Mitigation & Reporting*, dated June 03, 2016. This is a routine review and update to keep this document current, increase applicability, and reduce ambiguity. Changes include: a) Editorial changes to ensure clear and concise policy guidance, and improve readability; and b) Updates to the NWS vulnerability remediation timeframes to align them with current Department of Commerce (DOC) and National Oceanic and Atmospheric Administration (NOAA) policies.

KOONGE.BECKIE.A.1408306880 Digitally signed by KOONGE.BECKIE.A.1408306880
Date: 2021.04.28 10:11:42 -04'00'

Beckie Koonge Date
NWS Authorizing Official
Designated Representative (AODR)

# VULNERABILITY MANAGEMENT

Table of Contents Page

## 1 Introduction

This policy prescribes the minimum requirements used in the Vulnerability Management process for the National Oceanic and Atmospheric Administration's (NOAA's) National Weather Service (NWS) systems. Vulnerabilities are weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Credentialed vulnerability scans are required for all NWS authorized systems under the NOAA/NWS Information Technology Security Program. NWS System Owners are ultimately responsible for ensuring that network vulnerability scans and system configuration compliance scans are conducted on all systems under their control to correct misconfigurations and reduce vulnerabilities to an acceptable level commensurate with Department of Commerce (DOC), NOAA, and NWS policies. Scans must be conducted and deficiencies mitigated as part of the continuous monitoring process to ensure the security of NWS systems and data. By establishing and maintaining compliance with this policy, risks and costs to both NOAA and NWS can be reduced.

Policy objectives for NWS Federal Information Security Modernization Act of 2014 (as amended) (FISMA) systems:

- Provide NWS standard scanning process that must be followed by all personnel with scanning duties.
- Scan the complete Internet Protocol (IP) space of all NWS accredited systems and mitigate vulnerabilities within the timeframes mandated in DOC, NOAA and NWS policies.
- Ensure scanning and mitigations are conducted with minimum or no impact to the mission.

## 2 Scope

This policy applies to all NWS systems that fall under the purview of the NWS IT Security Program as defined by FISMA and supported by a Memorandum of Understanding/Agreement (MOU/MOA), as applicable.

## 3 Responsible Parties

**System Owner (SO)**: Responsible for ensuring that vulnerabilities are mitigated in accordance with the change management process defined in the approved System Security Plan (SSP). For vulnerabilities that cannot be corrected because of technical or programmatic obstacles, the SO ensures an approval process is in place authorized by the Authorizing Officials (AOs) that documents and assumes the risk for the vulnerabilities not being mitigated in accordance with DOC timelines.

**System Administrator (SA)**: Responsible for vulnerability and compliance scans, patching systems, implementing secure configurations as prescribed in the system security plans, and normal operations of the system in collaboration with the SO and Information System Security Officer. The SA is responsible for ensuring that credentialed security related vulnerability scans are conducted on a routine basis.

**Information System Security Officer (ISSO)**: Assists or facilitates scans (i.e., Nessus, Nmap, etc.) and aids with the mitigation process for identified vulnerabilities per applicable remediation timeframes. The ISSO works with the SA to ensure that adequate scan results are available in the NOAA Security Operations Center (SOC) Tenable.sc CyberScope repository in order to provide accurate aging determination and prioritization of vulnerability remediation.

## 4 Performing Scans

All NWS FISMA systems must perform vulnerability scans at periods with minimum impact to business operations (i.e., during periods of reduced usage). However, 24/7 operations stakeholders must work together to identify the best time to conduct scans taking into consideration the time frames prescribed in this policy.

It is mandatory that all scans (with the exception of Discovery scans as defined in section 5.1.2) be conducted with credentials (administrative privileges) to ensure that all vulnerabilities are identified.

FISMA systems required to have a penetration test conducted annually must notify the NOAA Computer Incident Response Team (N-CIRT) via NOAA Incident Response Reporting Application (NIRRA), and upload the Rules of Engagement (ROE) prior to conducting a penetration test. If other than a high FISMA system is selected for a pen test by the Chief Information Security Officer (CISO), system personnel must follow the guidance provided here.

The NWS Office of the Assistant Chief Information Officer (OACIO) reserves the right to conduct scans at a frequency defined by the Assistant Chief Information Officer (ACIO).

## 5 Vulnerability Scan Categories

NWS vulnerability scans fall into three categories: Initial, Routine, and Mitigation scans.

### 5.1 Initial Scans

The Initial scan is a key element in the system development lifecycle. Initial scans include Authorization and Discovery scans and must be performed with appropriate credentials.

### 5.1.1 Authorization Scans

Authorization scans take place prior to deployment of any new system into production. All new systems or systems added to an existing FISMA boundary must be scanned prior to being deployed to the production environment. If it is not technically feasible, then a checklist covering basic security points must be completed by the scanning party with the cooperation of the SO. The system will then be subjected to an automated authorization scan immediately after it is deployed to the production environment. Authorization scans will demonstrate compliance with existing security baseline settings.

### 5.1.2 Discovery Scans

Discovery scans are non-credentialed scans conducted to identify hosts that are running on a network. These scans help identify the inventory (including rogue devices), operating systems, baseline configurations, open ports, etc. Since scanning is a process, the Initial Discovery scan establishes the foundation, while future scans will be conducted based on modifications to the Initial scan (i.e., IP modifications, accepted vulnerabilities, etc.).

## 5.2 Routine Scans

### 5.2.1 Internal Scans

All Internal scans should be executed with credentials and conducted from a point on the system's network segment (i.e., inside the firewall) to identify vulnerabilities that could be exploited by a knowledgeable malicious insider or outsider that has breached the perimeter defense. The results of the scan are compared against a baseline to identify new vulnerabilities.

The Office of Management and Budget (OMB) requires a monthly compliance scan using security baseline setting standards, submitted via NOAA SOC CyberScope. Scan results must be uploaded to the NOAA SOC CyberScope repository. Compliance scans are scans performed to validate the implementation and hardening of configuration settings. Compliance scans offer an effective method of identifying whether IT products have been configured to reflect the most restrictive mode consistent with operational requirements.

All NWS FISMA systems must conduct compliance scans at a minimum, monthly, using the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) checklist. Systems that use a checklist other than DISA STIG must document the deviation in the FIPS 200 and seek AOs' approval.

The NOAA vulnerability and compliance scan contain the same scanning policy; therefore, only one scan is required monthly to meet the OMB requirement.

### 5.2.2 External Scans

External scans are scans targeting internet-accessible services or devices which identify misconfigurations and vulnerabilities that may be exploited by an external hacker leading to a network breach, web defacement or denial of service. Externally-facing services or device scans should be executed with credentials from within the system boundary to provide a more comprehensive view of external network vulnerabilities.

All NWS externally-facing services or devices must be scanned at a minimum, monthly, and when new vulnerabilities potentially affecting the system/applications are identified and reported. For those NWS systems that have provided the NWS ITSOs with their external IPs, the scans conducted by the Department of Homeland Security (DHS) satisfy this requirement. If there are changes to the externally-facing services or devices such as IP addresses that are no longer part of the asset inventory, the FISMA system must notify the NWS ITSOs of the change, and scan to ensure compliance with scanning requirements.

Externally facing perimeter protection devices managed by a third-party on behalf of NWS must follow the prescribed scan requirements. Federal and system requirements must be clearly identified and documented. Systems must ensure that all configurations are backed up and all necessary parties have prior notification before external scans begin.

### 5.3 Mitigation Scans

Mitigation scans are conducted after vulnerabilities identified in a Routine scan have been mitigated and are used to verify the correction. Mitigation scans may be conducted as a separate action or may be included in the next routine scan, depending on the sensitivity of the system and the criticality of the vulnerability. Mitigations not implemented during the scanning cycle must be documented by the SO or designee.

## 6 Scanning Frequency

SAs perform routine scans and remediate vulnerabilities in a timely manner. If vulnerabilities cannot be remediated within the DOC mandated timeframe, the SA communicates issues to the SO and ISSO along with recommending compensatory measures to protect the network until the vulnerability can be corrected. Scanning may be conducted at any time, but generally will occur in the following frequencies:

- Initial scan
  - Authorization scan: Prior to deployment into production
  - Discovery scan: As Needed
- Routine scan
  - Internal scan (Compliance scan): Monthly
  - External scan: Monthly
- Mitigation scan: As needed to verify correction

## 7 Patches

A large aspect of the scanning process is to verify that NWS systems have the appropriate, current patches installed. Patches must be downloaded from a trusted vendor source and tested in a non-production environment (if technically possible) prior to deployment. Routine patch updates must be deployed through the system's configuration management process.

### 7.1 Patching Timeframes

System personnel must remediate all identified vulnerabilities on their system via the timeframes listed in the table below. Vulnerabilities with known exploits require greater urgency for remediation and must be given priority. In the event that there are conflicting remediation timeframe guidelines from DOC, NOAA and NWS, the most stringent policy will prevail. SO/ISSO may contact ITSO/ACIO for guidance if enforcing the required timeframes could impact the system's mission. These will be treated on a case-by-case basis.

**Table 1: Vulnerability/Flaw Remediation Timeframes**

| Scan Type ↓ | Vulnerability Severity | | | |
|---|---|---|---|---|
| | Critical | High | Medium | Low |
| Internal Scans | 30 Days | 30 Days | 60 Days | 120 Days |
| External Scans | 14 Days | | | 30 Days |

Systems are required to identify, report, and correct all existing flaws within their boundary. Systems must install newly vendor released security relevant patches, service packs, anti-virus signature updates, hot fixes etc. within the established timetable.

It is imperative to include flaw remediation as part of a system's configuration management (CM) process. A CM process must be in place and followed for the testing of applicable software and firmware updates prior to being installed. This allows for the tracking and verification of remediation actions.

**Note:** In situations where it is not feasible for a system to meet the established timeframes due to technical, business or operational mission needs, the SO/ISSO must implement all possible compensating controls to mitigate the risk. Additionally, the SO/ISSO must document the rationale for not being able to meet the established timeframes along with deployed compensating controls within the FIPS 200, and seek AO's concurrence.

## 8 Reporting

Monthly scan reports must be submitted to the Security Operations Center (SOC) for the CyberScope scans in the standard format as required by NOAA SOC Tenable.sc. Vulnerability scans must be reviewed and analyzed by system personnel to facilitate timely correction of vulnerabilities and to institutionalize the scanning program.

It is imperative that NWS FISMA systems exhaust all possibilities before recasting or accepting risks. In the event there are vulnerabilities that cannot be mitigated due to technical or program constraints, NWS FISMA systems may choose to recast or accept risks reported by Tenable.sc or an equivalent monitoring tool.

## 9 Risk Recast

Recast is the process of lowering or increasing the risk severity of a vulnerability in Tenable.sc. ISSOs are required to provide adequate (i.e., what, why, when and how) justification for each risk recast. Recasting is risk and scenario-based and the decision to modify the risk impact can be influenced by the system mission/environment and other constraints identified by system personnel.

## 10 Risk Acceptance

The NWS risk acceptance process begins when a vulnerability that cannot be mitigated whether by technical limitations, degradation of security posture or other constraints is offered to the AOs for their review and consideration. Risk acceptance may be considered when all options (technical, non-technical) have been exhausted and no feasible alternative can be implemented. Tenable.sc related risk acceptances including false positives must be documented and managed outside of the FIPS 200 via the SO.

## 11 References

- Department of Commerce (DOC) CyberScope Reporting Services
- Department of Commerce (DOC) Information Technology Security Baseline Policy (ITSBP), version 1.0, June 2019
- National Oceanic and Atmospheric Administration IT Security Manual 212-1301 Version 7.0, November 15, 2020
- NIST National Checklist Program Repository https://nvd.nist.gov/ncp/repository
- NIST SCAP Publications http://scap.nist.gov/publications/index.html
- NIST Special Publication 800-37, Revision 2, December 2018
- Office of Management and Budget Memorandum (OMB) 07-18, Ensuring New Acquisitions Include Common Security Configurations
- Office of Management and Budget Memorandum (OMB) 08-22, Guidance on the Federal Desktop Core Configuration (FDCC)