

NATIONAL WEATHER SERVICE INSTRUCTION 60-703

22 June 2012

Information Technology

IT Security

VULNERABILITY IDENTIFICATION, MITIGATION & REPORTING

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

OPR: OCIO (Sherry Richardson)

Certified by: OCIO (Iftikhar Jamil)

Type of Issuance: Initial

SUMMARY OF REVISIONS:

<u>Signed</u>	<u>6/8/2012</u>
Iftikhar Jamil	Date
NWS Chief Information Officer	

Table of Contents

1 Introduction.....3
2 Scope.3
3 Responsible Parties3
4 Performing Scans3
5 Vulnerabilities Scans4
 5.1 Frequency.....4
 5.2 Initial Scans.....4
 5.3 Routines Scans5
 5.4 Internal Scans5
 5.5 External Scans.....5
6 Mitigation Scans5
7 Enforcing Remediation Timeframes.....6
8 Patches6
9 Reporting.....6
10 Maintaining Accepted Vulnerability Records.....7
11 References.....7

1. Introduction

This policy prescribes the minimum methodology used in the routine vulnerability identification and mitigation process for National Oceanic & Atmospheric Administration (NOAA), National Weather Service (NWS) systems. Routine, credential vulnerability scanning is required for all NWS accredited systems and is authorized under the NOAA/NWS Information Technology Security Program. NWS Information Technology Security Officers (ITSO) and Information System Security Officers (ISSOs) are responsible for ensuring that network vulnerability 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 policy. Routine scanning is 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. The objectives of this policy are to assure that:

- All accredited systems are routinely scanned and vulnerabilities are corrected in a timely manner in accordance with NOAA and NWS policy;
- NWS has implemented a standard process that all scanning personnel are following; and
- Vulnerability scanning and eradication has minimal impact on operational systems.

2. Scope

This policy applies to all NWS systems that fall under the purview of the NWS IT Security program as defined by the Federal Information Security Management Act of 2002 (FISMA) or are supported by a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA).

3. Responsible Parties

The responsible party for the security scanning of the NWS systems is the Information System Security Officer (ISSO) who reports to the System Owner (SO) or designate. However, the SO may designate the System Administrator (SA) to conduct the scan with oversight from the ISSO. In all cases, the ISSO is ultimately responsible for ensuring that security related vulnerability scans are conducted on a routine basis. Vulnerabilities are corrected in accordance with an approved change management process defined in the approved System Security Plan. For vulnerabilities that cannot be corrected because of technical or programmatic obstacles, ensure an approval process is in place authorized by the SO and Authorizing Official (AO) that assumes the risk for the vulnerabilities not being mitigated.

4. Performing Scans

If possible, vulnerability scans should be performed during periods of reduced usage. These times are traditionally not during business hours for production systems. However, for 24/7 operations that is not practical. The time frame that the scans are to be performed on production

systems must be negotiated between the SO, SA, and the ISSO. The NOAA Computer Incident Response Team (NCIRT) is notified via the NOAA Form 47-43 about scheduled scans and provided the IP address of the scanner.

5. Vulnerability Scans

There are many types of vulnerability scans but they fall into three basic groups; Initial, Routine, and Mitigation.

5.1. Frequency

ISSOs or SAs perform routine scanning and reports are issued for remediation. SAs are responsible for remediating vulnerabilities in a timely manner. If the vulnerabilities cannot be remediated within a reasonable time period a report is sent to the SO recommending compensatory measures to protect the network. Scanning may be conducted at any time, but generally will occur in the following frequencies:

- Initial:
 - Certification
 - Discovery
 - As needed
- Routine
 - Internal Vulnerability Scans: Quarterly
 - CyberScope Scans: Monthly
 - External Scan: Semi-Annually
- Mitigation
 - As needed to verify correction

5.2. Initial Scans

Initial scans are local, credentialed scans and include Certification scans and Discovery scans.

Prior to bringing any system into production mode, all systems should be scanned by performing an automated initial certification scan. If it is not technically feasible to scan a system prior to bringing it into a production system, then a checklist covering basic security points should be completed by the scanning party with the cooperation of the system owner prior to connecting it to the production system. The system will then be subjected to an automated certification scan immediately after it is connected in the production environment. Certification scans should show compliance with the United States Government Configuration Baseline (USGCB) standard where applicable or DOC, Commerce Information Technology Requirement Security Configuration Checklist Program (CITR-017).

Discovery scans are usually the first scan that is conducted on a network. It establishes the inventory, the operating systems, and the baseline configurations. Since scanning is a process, the

initial discovery scan establishes the foundation for the scanning program for that network or system. Future scans will be conducted based on modifications to the initial scans which could include the exclusion of IPs that are not applicable or have acceptable vulnerabilities or the addition of new IPs.

5.3. Routine Scans

Routine scans are conducted weekly, monthly, quarterly or semi-annually based on the data collected in the initial discovery scan. There are Internal Scans (which include CyberScope) and External Scans.

5.4. Internal Scans

All internal scans are scanned from a point on the system's network segment (i.e., inside the firewall) to identify vulnerabilities that could be exploited by a knowledgeable insider or a hacker that has penetrated the perimeter defense. The results of this scan are compared against a baseline to identify new vulnerabilities and submitted quarterly in a report to the NOAA Security Operations Center (SOC). Vulnerability scans are primarily corrected through a robust patching program.

A USGCB scan is a focused, internal scan that is based on predetermined configuration settings of certain operating systems and browsers. The Office of Management and Budget (OMB) requires that a USGCB scan and a vulnerability scan be conducted monthly and submitted via CyberScope. The SOC TSC has a specific CyberScope policy and repository dedicated to CyberScope scanning and submission. CyberScope scans are required on the 24th of each month after "patch Tuesday" so that the scan results submitted to OMB will reflect the latest patch deployment.

5.5. External Scans

External scans are non-credentialed perimeter scans that provide a comprehensive view of network vulnerabilities that could be exploited by an external hacker. All perimeter external devices managed by NWS should be scanned externally (e.g., from outside the firewall) at least twice a year and after any configuration changes to the perimeter device. If non-NWS personnel manage the external perimeter protection devices then they are responsible for the security of the devices and NWS is not required to scan them. Since external scans for NWS systems involve testing the perimeter device, ensure the all configurations are backed up and all necessary parties (ITSO, SO, ISSO, ISP, Firewall Administrator, etc.) have prior notification. External scans are focused on misconfigurations in perimeter devices and public facing web servers that could allow an attacker to penetrate the network or deface or deny access to systems.

6. Mitigation Scans

Mitigation scans are the subsequent actions conducted as a result of the deficiencies discovered in the scans. They are conducted after the scan data has been provided to the SA/NA and the

identified vulnerabilities have been corrected. 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.

Communicate mitigation actions to the SO and ISSO. The ISSO saves this response for reference. Mitigation actions that cannot be implemented during the scanning cycle period should be POA&M items.

If the SO, SA/NA, and ISSO cannot agree on acceptance or mitigation, the decision of which action to perform will be made by the AO or designee. The ISSO and SA/NA are responsible for the mitigation of vulnerabilities to include organizing the action between other involved parties, if applicable.

7. Enforcing Remediation Timeframes

The SO, SA, and ISSO will ensure that remediation time frames for routine scanning and correction of identified vulnerabilities are followed. Failure to comply with remediation time frames for identifying and correcting deficiencies is a violation of NOAA/NWS policy and may result in loss of authorization to operate the system. CTR 16 states, “Vulnerabilities shall be remediated within 30 days of discovery for FIPS 199 High Impact systems, 60 days for Moderate Impact systems, and 90 days for Low Impact systems.”

For most NWS locations, it is not possible to comply with the timeframes. For example, it is not possible to remediate all High, Medium, and Low vulnerabilities in all High Impact systems every 30 days. CTR 16 states, “Timeframes for remediation may be modified as appropriate based on the impact level of the system, vulnerability, compensating controls, and likelihood of exploit”. Therefore, the NWS policy is that for High and Moderate Impact systems, all Critical and High vulnerabilities will be remediated within 30 days and all Medium vulnerabilities within 60 days. Low vulnerabilities will be remediated after the High and Mediums are remediated.

8. Patches

A large aspect of the scanning process is to verify that NWS systems have the appropriate, current patches installed. If possible, system administrators should apply patches in a non-production environment before they are applied to production servers to ensure that the patches do not affect the existing production applications. Document patch updates through the system’s configuration management process. Routine scanning and patching is a vital component of a mature IT security program.

9. Reporting

Scan reports will be provided in the standard format as required by NOAA SOC TSC.

- Monthly: CyberScope
- Quarterly: Vulnerability

Monthly reports are submitted to the SOC for the Cyberscope scans and quarterly for vulnerability scans.

10. Maintaining Accepted Vulnerability Records

The SO and the ISSOs maintain documentation approved by the AO of accepted vulnerabilities for each scanned system.

11. References:

- Office of Management and Budget Memorandum 04-25, FY 2004 Reporting Instructions for Federal Information Security Management Act
- Office of Management and Budget Memorandum 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operation Systems
- Office of Management and Budget Memorandum 07-18, Ensuring New Acquisitions Include Common Security Configurations
- Office of Management and Budget Memorandum 08-22, Guidance on the Federal Desktop Core Configuration (FDCC)
- Office of Management and Budget Memorandum 10-15 FY 2010, Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- NIST SCAP Publications
<http://scap.nist.gov/publications/index.html>
- U.S. Department of Commerce IT Security Program Policy and Minimum Implementation Standards
- U.S. Department of Commerce CyberScope Reporting Services
http://home.commerce.gov/cio/ITSITnew/CM/DOC_CyberScope_Reporting_Services.html
- NOAA 212-1300, Information Technology Security Manual
- CITR 016 – Vulnerability Scanning and Patch Management, January 25, 2012