

NATIONAL MARINE FISHERIES SERVICE POLICY DIRECTIVE 32-106

JUNE 16, 2003

Information Management

***NOAA FISHERIES HEADQUARTERS NETWORK SERVER
DEPLOYMENT POLICY***

NOTICE: This publication is available at: <http://www.nmfs.noaa.gov/op/pds/>

OPR: F/CIO

Certified by: F//CIO (L. Tyminski)

Type of Issuance: Revised October 2014

SUMMARY OF REVISIONS: Minor updates to reflect new format and current network server environment

Introduction

NOAA Fisheries Office of the Chief Information Officer manages Headquarters datacenter infrastructure that supports multiple operating systems and applications on physical servers and virtualization environments. Infrastructure Operations Team is responsible for maintaining the new server deployments in NOAA Fisheries Local Area Network.

The most critical aspect of deploying a secure server is careful planning before installation, configuration, and deployment. Careful planning will ensure that the server is as secure as possible and in compliance with all relevant NOAA policies. Many server security and performance problems can be traced to a lack of planning or management controls. The importance of management controls cannot be overstated.

The Chief Information Officer (CIO) will approve the deployment of all network servers prior to their installation on Fisheries Headquarters Local Area network. This policy applies to all Headquarters organizations, and excludes desktops and laptops used by a single user performing routine administrative functions, such as word processing and electronic messaging.

Objectives

- Installing and configuring systems in compliance with the NOAA security policies and standard system and network configurations
- Maintaining systems in a secure manner, including frequent backups and timely application of patches
- Monitoring system integrity, protection levels, and security-related events
- Following up on detected security anomalies associated with their information system resources
- Conducting security tests as required.

Authorities & Responsibilities

- Chief Information Officer. The CIO is responsible for the Fisheries Headquarters datacenter infrastructure.
- Server Administrator (SA) Server administrators are system architects responsible for the overall design, implementation, and maintenance of a server.
- Network Administrator. Under the Fisheries CIO, the network administrator is responsible for the daily operation of the WAN/LAN, including the placing of all circuit orders with authorized service providers, configuring all WAN/LAN-related equipment, ensuring that network security is appropriate, and maintaining up-to-date documentation of the network topology and WAN/LAN hardware configuration.
- ITSO (Information Technology Security Officer). The ITSO is responsible for developing and implementing the NOAA Fisheries IT security program.
- HQ Change Control Board. This Board assists the CIO with final approval/disapproval decisions. After the Change Control Board makes a recommendation to approve or

disapprove a change, the HQ Change Control Board meets with the CIO to discuss risks and risk mitigation for the change. The HQ CCB Board consists of the Infrastructure Operations Manager, Network Operations Manager, ITSO, Deputy CIO, and staff of other potentially affected system, such as the Systems Development staff, Help Desk, or the RITC representing the SCR.

- LAN Administrators. These are the individuals responsible for operating each Fishery's LAN and who coordinate with the Fisheries Network Administrator on all WAN-related issues.
- System Lead (SL) - A system administrator, responsible for ensuring that the operations of the system are carried out efficiently and effectively. The SL may also be, but is not necessarily, the primary administrator for the particular system components (i.e. The SL for Windows operating systems may be the Windows system administrator). SLs are responsible for ensuring that the NOAA4010 policies and procedures are enforced within the boundaries of the system.

Measuring Effectiveness

It is essential to use the defined metrics to track the effectiveness of deployments of all network servers will allow the improvements. Information security continuous monitoring can serve as a measure of the success of all network servers' deployments for an ongoing awareness of information security, vulnerabilities, and threats to support OCIO risk management decisions.

NOAA Fisheries Office of the Chief Information Officer Conduct periodic risk assessments to identify the specific threats against the network servers and determine the effectiveness of existing security controls in counteracting the threats.

References

- National Institute of Standards and Technology (NIST) SP 800-30, *Risk Assessment Guide for Information Technology Systems*.
- National Institute of Standards and Technology (NIST) SP 800-123, *Guide to General Server Security, July 2008*.

Signed _____

ES
Eileen Sobeck
Assistant Administrator of NOAA Fisheries

12/15/14

Date