Report In Brief

SEPTEMBER 7, 2012

Background

NTIA is principally responsible for advising the President on telecommunications and information policy issues. These issues include expanding broadband Internet access and adoption in America, ensuring that the Internet remains an engine for continued innovation and economic growth, managing the federal government's use of spectrum (airwaves), and ensuring that America's domestic and international spectrum needs are met while making efficient use of this limited spectrum resource.

Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to secure systems through the use of cost-effective management, operational, and technical controls. The goal is to provide adequate security commensurate with the risk and extent of harm resulting from the loss, misuse, or unauthorized access to—or modification of—information collected or maintained by, or on behalf of, an agency.

In addition, FISMA requires inspectors general to evaluate agencies' information security programs and practices, by assessing a representative subset of agency systems, and the results are reported to the Office of Management and Budget, the Department of Homeland Security, and Congress annually.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Significant IT Security Program Improvements Are Needed to Adequately Secure NTIA's Systems

OIG-12-035-A

WHAT WE FOUND

Fundamental steps for securing NTIA's information and systems have not been taken. When assessing seven NTIA systems, we found these deficiencies: (1) inadequate security categorizations that jeopardize critical bureau information, (2) significant weaknesses in IT software and hardware inventory practices, (3) major inadequacies in NTIA's process to remediate security weaknesses, (4) weaknesses in managing its IT security workforce and developing effective IT security policies and procedures, and (5) significant deficiencies in key IT security controls. These issues have resulted in ineffective management of security controls needed to protect NTIA's systems and information.

WHAT WE RECOMMEND

The Assistant Secretary for Communications and Information should ensure:

1. The authorization status of NTIA's systems is revised to interim authorization to operate until these activities have been completed:

a. System owners and NTIA officials collaborate to identify and categorize all information types that are processed, stored, or transmitted by each system and categorize each system accordingly.

b. System owners develop and maintain an accurate hardware and software inventory for their systems.

c. NTIA implements and assesses appropriate IT security controls.

d. NTIA follows the plan of action and milestones process required by the Department's IT security policy.

2. System owners, IT security officers, authorizing officials, and other staff with critical IT security roles are appropriately trained, earn certifications as required by Department policy, and have the required metrics incorporated into their performance plans.

3. NTIA's chief information officer and IT security officer develop and maintain NTIA security policies, procedures, standards, and guidance consistent with departmental and federal requirements.