Report In Brief

JULY 15, 2014

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

Significant Security Deficiencies in NOAA's Information Systems Create Risk in Its National Critical Mission

OIG-14-025-A

Background

The National Oceanic and Atmospheric Administration's (NOAA's) information systems are crucial to its ability to reliably perform its national critical mission. They provide hazardous weather forecasts and warnings, which are essential in protecting life, property, and the nation's economy.

This information technology (IT) security audit focused on select systems in two line offices that support NOAA's critical mission: the National Environmental Satellite, Data, and Information Service (NESDIS) and the National Weather Service (NWS).

Specifically, we evaluated information security controls and security-related documentation for four NESDIS systems to determine whether key security measures adequately protect them. Additionally, we reviewed the independent security control assessments of five NWS systems to determine whether the controls were adequately assessed.

Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to secure their information technology (IT) systems through the use of cost-effective management, operational, and technical controls.

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 (OMB), the Department of Homeland Security, and Congress annually.

WHAT WE FOUND

Information systems connected to NESDIS' critical satellite ground support systems increases the risk of cyber attacks. The Polar-orbiting Operational Environmental Satellites' (POES') and Geostationary Operational Environmental Satellites' (GOES') mission-critical satellite ground support systems have interconnections with systems where the flow of information is not restricted, which could provide a cyber attacker with access to these critical assets.

NESDIS' inconsistent implementation of mobile device protections increases the likelihood of a malware infection. In our review of selected Windows components on four NESDIS systems, we found that (a) unauthorized mobile devices had been connected to POES, GOES, and Environmental Satellite Processing Center (ESPC), and (b) GOES and ESPC did not consistently ensure that Microsoft Windows' AutoRun feature was disabled.

Critical security controls remain unimplemented in NESDIS' information systems. Our review of four NESDIS information systems found that NESDIS did not (1) appropriately remediate vulnerabilities, (2) implement required remote access security mechanisms, and (3) implement the secure configuration settings control on IT products.

Improvements are needed to provide assurance that independent security control assessments are sufficiently rigorous. We found that 28 of 60 (47 percent) of the independent assessments of security controls have deficiencies and may not have provided NOAA's authorizing official with an accurate implementation status of the system's security controls.

WHAT WE RECOMMEND

That NESDIS' Assistant Administrator and NOAA's Chief Information Officer:

1. Conduct a review to determine risks posed by NESDIS' restricted systems' current interconnections and ensure that USAF identifies all of DMSP's interconnections
2. Document and convey to NOAA senior management the risks identified with these interconnections
3. Require that interconnected systems have completed control assessments and are authorized to operate before establishing an interconnection
4. Pursue USAF commitment to conduct security assessments on DMSP
5. Prevent components' moving between the GOES and SWPC networks for maintenance activities
6. Implement security mechanisms to protect against the use of unauthorized mobile devices
7. Determine a feasible remediation timeframe for applying patches to POES, GOES, and ESPC
8. Ensure appropriate priority to remediation of high-risk vulnerabilities in the required timeframe. If remediation is not feasible, ensure documentation of vulnerabilities and implementation of compensating controls.
9. Ensure (a) information system compliance with all applicable remote access and telework policies and (b) implementation of two-factor authentication
10. Ensure NESDIS telework policy compliance with Department policy on personal devices
11. Implement necessary security mechanisms to secure against remote access via personal computers
12. Ensure that appropriate attention is given to implementing required secure configuration settings in a timely manner and continue the implementation

That NOAA's Chief Information Officer:

13. Develop a quality control process for assurance that security controls are appropriately assessed before the authorization package is assembled and submitted to the authorizing official