



# NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

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

FINAL REPORT NO. OIG-14-025-A

JULY 15, 2014

U.S. Department of Commerce  
Office of Inspector General  
Office of Audit and Evaluation

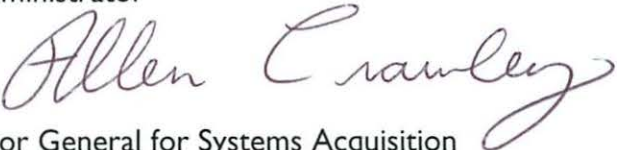
**FOR PUBLIC RELEASE**





July 15, 2014

**MEMORANDUM FOR:** Dr. Kathryn Sullivan  
Under Secretary of Commerce for Oceans and Atmosphere  
and NOAA Administrator

**FROM:** Allen Crawley   
Assistant Inspector General for Systems Acquisition  
and IT Security

**SUBJECT:** *Significant Security Deficiencies in NOAA's Information Systems Create Risk in Its National Critical Mission*  
Final Report No. OIG-14-025-A

Attached is our final report of our audit of NOAA's information technology security program, which we conducted in accordance with the Federal Information Security Management Act. Specifically, we evaluated information security controls and security-related documentation for four National Environmental Satellite, Data, and Information Service (NESDIS) systems to determine whether key security measures adequately protect them. Additionally, we reviewed the independent security control assessments—conducted in FY 2012 and FY 2013 through an intra-agency shared service agreement—of five National Weather Service (NWS) systems to determine whether the controls were adequately assessed.

We found that (1) information systems connected to NESDIS' critical satellite ground support systems increases the risk of cyber attacks, (2) NESDIS' inconsistent implementation of mobile device protections increases the likelihood of a malware infection, (3) critical security controls remain unimplemented in NESDIS' information systems, and (4) improvements are needed to provide assurance that independent security control assessments are sufficiently rigorous.

We have summarized your agency's response in the report and included the formal response as appendix C. The final report will be posted on the OIG's website pursuant to section 8M of the Inspector General Act of 1978, as amended.

In accordance with Department Administrative Order 213-5, please provide us with your action plan within 60 days of the date of this memorandum. We appreciate the cooperation and courtesies extended to us by your staff during our audit. If you have any questions or concerns about this report, please do not hesitate to contact me at (202) 482-1855 or Dr. Ping Sun, Director for IT security, at (202) 482-6121.

Attachment

cc: Steve Cooper, Chief Information Officer  
Mark Paese, Acting Assistant Administrator for Satellite and Information Services,  
NOAA  
Zach Goldstein, Acting Chief Information Officer, NOAA  
Rod Turk, Director, Office of Cyber Security, and Chief Information Security Officer  
Lawrence Reed, Director, Cyber Security Division, NOAA  
Vanessa Griffin, Acting Chief Information Officer, NESDIS  
Iftikhar Jamil, Assistant Chief Information Officer, NWS  
Brian Doss, Audit Liaison, NOAA  
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer



# Report In Brief

JULY 15, 2014

## 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.

## NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

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

OIG-14-025-A

#### 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

# Contents

- Introduction ..... 1
- Findings and Recommendations ..... 3
  - I. Information Systems Connected to NESDIS’ Critical Satellite Ground Support Systems Increases the Risk of Cyber Attacks ..... 3
    - A. POES Is Interwoven with a Department of Defense Information System, Putting POES at Significant Risk ..... 3
    - B. Administration of SWPC Components Within the GOES System Introduces an Unnecessary Security Risk..... 6
  - II. NESDIS’ Inconsistent Implementation of Mobile Device Protections Increases the Likelihood of a Malware Infection..... 8
  - III. Critical Security Controls Remain Unimplemented in NESDIS’ Information Systems .... 10
    - A. NESDIS’ Ineffective Vulnerability Remediation Activities Leaves Its Mission-Critical Assets Vulnerable to Compromise ..... 10
    - B. NESDIS’ Remote Access Deficiencies Leave Its Information Systems Vulnerable to Cyber Attacks ..... 11
    - C. NESDIS’ Critical Mission Support Systems Continue to Lack Secure Configuration Settings..... 13
  - IV. Improvements Are Needed to Provide Assurance That Independent Security Control Assessments Are Sufficiently Rigorous..... 15
- Summary of Agency and OIG Comments..... 17
- Appendix A: Objectives, Scope, and Methodology ..... 19
- Appendix B: List of Acronyms and Abbreviations ..... 21
- Appendix C: Agency Response..... 22



## Introduction

Part of the mission of the National Oceanic and Atmospheric Administration (NOAA) is to understand and predict changes in weather, oceans, climate, and coasts and to share that knowledge and information with other agencies and the public. 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. Our 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).

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

As part of an overall assessment of NOAA's IT security program, we evaluated information security controls and security-related documentation for four high-impact NESDIS systems to determine whether key security measures adequately protect them (see table 1).

**Table 1: NESDIS Information Systems Reviewed**

System Name	Primary Function
<b>Polar-orbiting Operational Environmental Satellites (POES)</b>	Satellite ground support system that provides computing resources necessary to control and collect data for weather imagery data from POES satellites.
<b>Geostationary Operational Environmental Satellites (GOES)</b>	Satellite ground support system that provides computing resources necessary to command and control and collect data for weather imagery data from GOES satellites.
<b>Environmental Satellite Processing Center (ESPC)</b>	NOAA's data-processing system for the nation's environmental satellite data received from POES, GOES, and the European Meteorological Operational Satellite environmental satellites. ESPC distributes environmental data products to the National Weather Service (NWS); the primary forecast centers of the U.S. Navy and U.S. Air Force; and international forecast centers, academia, and private-sector entities.
<b>Search and Rescue Satellite Aided Tracking (SARSAT)</b>	SARSAT relays distress signals—generated by aviators, mariners, and land-based users—to search and rescue services.

Additionally, we reviewed the Federal Aviation Administration’s (FAA) independent security control assessment—conducted in fiscal year (FY) 2012 and FY 2013 through an interagency shared service agreement—of five high- and moderate-impact NWS systems to determine if the controls were adequately assessed (see table 2).

For further details regarding the objectives, scope, and methodology of this audit, see appendix A.

**Table 2: NWS Information Systems Reviewed**

System Name	Primary Function
<b>Aviation Weather Center (AWC)</b>	Enhances aviation safety by issuing warnings, forecasts and analyses of hazardous weather and originates operational forecasts of weather conditions predicted to affect domestic and international aviation. The Center also identifies existing or imminent weather hazards to aircraft in flight and creates warnings for transmission to the aviation community.
<b>Space Weather Prediction Center (SWPC)</b>	Provides real-time monitoring and forecasting of solar and geomagnetic events, is used to conduct research in solar-terrestrial physics, and develops techniques for forecasting solar and geophysical disturbances.
<b>Storm Prediction Center (SPC)</b>	Provides tornado and severe weather watches for the contiguous United States and forecasts the risk of severe thunderstorms, tornadoes, and conditions favorable for wildfires in the contiguous United States.
<b>National Hurricane Center (NHC)</b>	Issues forecasts, advisories, watches, and warnings for tropical cyclones over the Atlantic basin (including the Gulf of Mexico and Caribbean), Northeast Pacific basins, and backs up the Central Pacific Hurricane Center for tropical cyclone forecasts.
<b>National Centers for Environmental Prediction (NCEP) Central Operations</b>	Provides forecast, guidance, and analysis products and services to support the daily public forecasting activities of the National Weather Service and provides tailored support to other government agencies in emergency situations.

## Findings and Recommendations

As part of our annual FISMA work, we reviewed NOAA's IT security program and critical security controls in place to protect its mission capabilities. We found that (1) the flow of information between NESDIS' critical satellite ground support systems and other information systems puts its critical assets at risk of cyber attacks, (2) unauthorized mobile devices increase the risk of a malware infection, (3) NESDIS continues to have unimplemented critical security controls, and (4) improvements are needed to provide assurance that independent security control assessments are sufficiently rigorous.

### I. Information Systems Connected to NESDIS' Critical Satellite Ground Support Systems Increases the Risk of Cyber Attacks

Restricting the flow of information between interconnected systems is a significant part of NESDIS' IT security strategy to protect its mission critical assets—POES and GOES satellite ground support systems—from cyber attacks. However, we found that both POES and GOES have interconnections with systems where the flow of information is not restricted, which could provide an attacker with access to these critical assets. Although system interconnections can facilitate interagency and external communications and services, such connections can also pose significant risk to each interconnected information system (i.e., more easily allow malware to spread, or attackers to use one system to access another).

#### A. *POES Is Interwoven with a Department of Defense Information System, Putting POES at Significant Risk*

Even though NESDIS asserted POES has restricted the flow of information with other systems, we found that POES is actually interwoven with U.S. Air Force's (USAF) Defense Meteorological Satellite Program (DMSP) to the point where they are virtually one system. Specifically, there is no physical or logical separation between the systems (i.e., the systems operate on the same network and data can flow between the systems); they share support personnel, and they share some of the same support services and IT security controls (e.g., access control via a common Microsoft Windows Active Directory domain). This interweaving means that deficiencies in one system's security posture will drastically affect the other system's security.

Unfortunately, because USAF and NOAA disputed for several years (from 2006 to 2010) who was responsible for DMSP's security, neither organization conducted security assessments of DMSP. Ultimately, USAF and NOAA determined in 2010 that USAF was responsible for DMSP. However, USAF has yet to fulfill its responsibilities<sup>1</sup> by determining DMSP's security posture and ensuring that the system meets the Department's security requirements (see exhibit I for a timeline).

---

<sup>1</sup> USAF is responsible for ensuring that (1) DMSP is appropriately authorized, (2) DMSP meets the Department of Commerce's security requirements, and (3) security testing is conducted. See memo from Col. Alec M. Robinson, USAF Program Executive Officer for Environmental Satellites, to NOAA Assistant Administrator for Satellite and Information Services, May 13, 2010, on DMSP Ground Service Life Extension Program (GSLEP).



**DMSP presents a significant security risk to POES.** Without sufficient assessments, both USAF and NOAA have very little knowledge of DMSP's security posture or how DMSP's deficiencies affect the intertwined systems. However, we have identified risk factors that put the POES system at significant risk of a compromise, which could have an impact on NOAA's mission capabilities. Specifically:

- *NESDIS cannot fully understand POES' security risks because DMSP's interconnections with other information systems have not been assessed.* We identified an interconnection that presents significant risk to POES through its interweaving with DMSP. Specifically, DMSP has an interconnection with another NOAA system—one that also has significant security deficiencies of its own—that is connected to the Internet. This other system's connection to the Internet could allow an attacker to gain remote access to DMSP and, through its interweaving with DMSP, to POES. The existence of this interconnection was not conveyed in POES' security authorization package to NOAA management. Consequently, NOAA management did not factor this significant risk into its subsequent risk-

### Exhibit I. Timeline of the POES-DMSP Relationship

- 1994** Presidential Directive (NSTC-2) issued. It places NOAA in charge of combining POES and DMSP, with the goal of reducing duplicative capabilities.
- 1998** NOAA completes the interweaving of POES and DMSP and takes responsibility for DMSP. (NOAA continues to operate DMSP until 2010.)
- 2003** NOAA grants DMSP a 3-year authorization to operate (ATO).
- 2006** DMSP's ATO expires, and NOAA contests its responsibility for DMSP. The dispute continues until 2010. No security assessments or authorizations occur during this time period.
- 2010** USAF resumes responsibility for DMSP and grants an ATO without assessing the system's security posture.
- 2011** USAF and NOAA again dispute responsibility for DMSP's security posture and USAF does not grant an ATO for DMSP nor conducts security assessments.
- 2012** NESDIS officially acknowledges POES and DMSP are interwoven. USAF again does not conduct an assessment of DMSP's security posture. Instead, it grants DMSP an ATO based on POES' security posture.
- 2013** OIG begins to review POES and GOES security postures as part of its audit of NOAA's IT security program. USAF again does not conduct an assessment of DMSP's security posture. Instead, it grants DMSP an ATO based on POES' security posture.

Source: OIG analysis

based authorization decision. DMSP's interconnection significantly increases POES' risk of a compromise and contradicts NESDIS' assertions that risk to its systems was decreased by restricting the flow of information between POES and its interconnected systems.

- *Limited assessments identified significant security deficiencies within DMSP.* Even though DMSP's current security posture is mostly unknown, significant security vulnerabilities were identified by NESDIS' security testing of POES' components in FY 2013, and fixes for some of these vulnerabilities have been available for a decade or more. NESDIS' assessors inadvertently scanned DMSP components and identified serious vulnerabilities that could be easily exploited by an attacker (e.g., weak or default passwords and operating system vulnerabilities with well documented exploits). The presence of such vulnerabilities indicates a significant vulnerability remediation deficiency. Given the level of integration between the two systems, we are concerned that this deficiency is putting both of them at increased risk.
- *POES will remain interwoven with DMSP, and DMSP's security posture will remain deficient for some time.* Presently, NESDIS does not anticipate completing an initial plan until the end of FY 2014 and has asserted that if funding is not available it will abandon any corrective actions and accept the risks of leaving the systems interwoven. Further, USAF does not plan to conduct an assessment of DMSP's security posture until it completes a technology refresh in 2016 (i.e., replace DMSP's legacy hardware and software components). However, there is doubt that the refresh will occur because of the USAF's funding constraints.

We are concerned that the necessary corrective actions to separate these systems will not occur for several more years; thus, the systems would remain interwoven and at increased risk. Further, without an assessment to understand (1) how POES and DMSP are interwoven, (2) the risks to POES, and (3) DMSP's security posture, USAF and NESDIS will not understand the risks to either system and cannot develop an effective plan to address the risks and separate the two systems.

***NESDIS cannot adequately convey to NOAA management the risks to POES.***

NESDIS can neither accurately determine nor appropriately convey POES' security posture, nor the risk level associated with its interweaving with DMSP, because it does not understand all the risks associated with DMSP's security posture and interconnections. For example, the NESDIS assessors who reviewed POES could not effectively assess the system's security posture because the boundaries between POES and DMSP components were so poorly defined (i.e., what components belonged with which system). Because of this, the assessors could not make an accurate determination of POES' security posture without assessing both POES and DMSP. To date, no such assessment has been undertaken.

Although POES and DMSP have been interwoven for years, it was not until POES' March 2012 authorization briefing that NESDIS conveyed to NOAA management that DMSP increased POES' risk of a compromise and began officially including this risk in the Department's risk tracking system. Even though NESDIS did not understand all the risks and their potential impacts, it conveyed to NOAA management that POES' interweaving with DMSP represented a medium risk level (i.e., not implementing security mechanisms on POES presented a medium risk of compromise).

Further, POES staff asserted that firewalls have been installed to prevent unwanted intrusion, thus mitigating some of the risk. However, with the two systems being closely interwoven and sharing resources (e.g., printers, routers, log servers, and access control), such firewalls will not protect POES from an internal threat originating from DMSP. We believe POES is not protected as NESDIS intended. This puts POES' capabilities, which support NOAA's national critical mission, at risk.

*B. Administration of SWPC Components Within the GOES System Introduces an Unnecessary Security Risk*

NESDIS operates a network extension at the NWS' Boulder, Colorado, location that directly connects to the primary GOES ground support system network. This extension hosts multiple server components maintained by SWPC, providing a proprietary one-way link that is designed to move space weather data from GOES to SWPC. We found that SWPC's current system maintenance process, used to remediate security vulnerabilities and deploy new software on components within the GOES system, presents undue risk. Specifically:

- To perform the maintenance activities, SWPC staff disconnects the components from the GOES extension and reconnects the components to the local SWPC network. Once completed, the components are then reconnected to the GOES extension. Should the components contract a malware infection while on the SWPC network, the infection could spread from the returned components on the GOES extension and into the GOES ground support system.
- SWPC has a connection to the Internet through an interconnection with another NWS information system. This Internet connection could allow an attacker to compromise SWPC and, through SWPC, gain access to the GOES extension.

Although the exchange of weather data is governed by an interconnection agreement between GOES and SWPC, we found that neither side has appropriately considered the risks associated with the current maintenance process. We believe that SWPC's maintenance process violates NESDIS' intended protection of the GOES information system. Since GOES maintains other components it owns that reside on the network extension, GOES should have the capability to also maintain these components.

### *Recommendations*

We recommend that NESDIS' Assistant Administrator and NOAA's Chief Information Officer:

1. Conduct a review to determine the risks posed by NESDIS' restricted systems' current interconnections and ensure that the USAF identifies all of DMSP's interconnections with other information systems.
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's commitment that DMSP meets Department of Commerce's security requirements and conduct security assessments, as outlined in a memorandum from the USAF to NOAA on May 13, 2010.
5. Prevent components from moving between the GOES network and SWPC network for maintenance activities.

## II. NESDIS' Inconsistent Implementation of Mobile Device Protections Increases the Likelihood of a Malware Infection

We reviewed a selection of Windows components, such as workstations and servers, on each of the four NESDIS systems to determine if the necessary security protections are in place to prevent unauthorized mobile device usage (e.g., USB flash drives and smartphones connecting to system components). Specifically, we found that

- **Unauthorized mobile devices had been connected to POES, GOES, and ESPC, because each system lacked the necessary protection (see table 3, next page).** Mobile devices can carry malware that, when plugged into a workstation or server, could execute malicious code residing on the device and lead to a compromised system. Accordingly, there has been a long-standing requirement that agencies restrict the use of mobile devices. Implementing required mobile device security mechanisms helps prevent the spread of malware and limits the risk of a compromise of critical assets. Further, mobile devices are one of the means by which an attacker can access and compromise a system with restricted interconnections, such as NESDIS' satellite ground-support systems POES and GOES.
- **GOES and ESPC did not consistently ensure that Microsoft Windows' AutoRun feature was disabled.**<sup>2</sup> This is a critical element of mobile device security. According to a recent study by Microsoft, 26 percent of successful malware propagation was attributed to USB devices taking advantage of Microsoft Windows' AutoRun feature, which allowed malicious code to automatically execute when users plugged their infected mobile devices into computers.<sup>3</sup> In 2009, the U.S. Computer Emergency Readiness Team<sup>4</sup> (US-CERT) issued an alert regarding AutoRun, emphasizing that disabling it can help prevent the spread of malicious code.<sup>5</sup>

Although SARSAT has the necessary protections to prevent the use of unauthorized mobile devices, POES, GOES, and ESPC do not. As it only takes one infected mobile device to spread malware and allow an attacker access to restricted systems like POES and GOES, NESDIS' critical components are at increased risk of compromise.

---

<sup>2</sup> Autorun is a technology used to start some programs or enhanced content (such as video content on mobile device) automatically when a device is connected to a computer.

<sup>3</sup> Microsoft. *Microsoft Security Intelligence Report Volume 11* [Online], [download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft\\_Security\\_Intelligence\\_Report\\_volume\\_11\\_English.pdf](https://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf) (accessed September 16, 2013).

<sup>4</sup> US-CERT, a part of the Department of Homeland Security, leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation.

<sup>5</sup> US CERT. *Microsoft Windows Does Not Disable AutoRun Properly* [Online], [www.us-cert.gov/ncas/alerts/TA09-020A](http://www.us-cert.gov/ncas/alerts/TA09-020A) (accessed September 20 2013).



**Table 3. Review of NESDIS' Mobile Device Usage and Security Protections Implemented on a Selection of Microsoft Windows Components**

Issue	NESDIS Systems Reviewed			
	POES	GOES	ESPC	SARSAT
Percentage of components with recent unauthorized USB device activity	41%	36%	48%	0%
Percentage of components with AutoRun enabled	0%	68%	29%	0%
Types of devices identified	<ul style="list-style-type: none"> <li>• USB flash drives</li> <li>• smartphones</li> </ul>	<ul style="list-style-type: none"> <li>• USB flash drives</li> <li>• smartphones</li> </ul>	<ul style="list-style-type: none"> <li>• USB flash drives</li> <li>• smartphones</li> </ul>	N/A

Source: OIG analysis

### *Recommendation*

We recommend that NESDIS' Assistant Administrator and NOAA's Chief Information Officer:

6. Implement security mechanisms to protect against the use of unauthorized mobile devices.

### III. Critical Security Controls Remain Unimplemented in NESDIS' Information Systems

Our review of the four NESDIS information systems (POES, GOES, ESPC, and SARSAT) identified that NESDIS continues to struggle to implement fundamental security requirements. Specifically, 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 (e.g., operating systems, databases, and web servers).

#### A. NESDIS' Ineffective Vulnerability Remediation Activities Leaves Its Mission-Critical Assets Vulnerable to Compromise

Numerous high-risk vulnerabilities remain in NESDIS' systems because of its deficient vulnerability remediation practices. High-risk vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing remote execution of malicious commands.

Three of the four systems reviewed (POES, GOES, and ESPC) have a significant number of vulnerabilities that have not been remediated. Specifically, our review of each system's vulnerability scans<sup>6</sup> found that:

- POES, GOES, and ESPC have thousands of vulnerabilities, where some of the vulnerabilities in the software have been publicly disclosed for as long as 13 years (see table 4). The older the vulnerability, the more likely exploits have been incorporated into common hacking toolkits, making it much easier for even an unskilled attacker to compromise a system.
- ESPC and POES have not remediated 24 percent and 50 percent, respectively, of the high-risk vulnerabilities<sup>7</sup> identified by the OIG's FY 2010 vulnerability scans.<sup>8</sup>

Timely vulnerability management has been a security requirement for many years.<sup>9</sup> NESDIS asserted that, to meet this requirement, its staff follows a vulnerability management process wherein they perform credentialed, quarterly scans of each system and extensively test patches for software flaws (i.e., ensuring that the patch will not

<sup>6</sup> At the time of our analysis, we selected each system's most recent vulnerability scan to determine the system's current vulnerabilities.

<sup>7</sup> The percentage of unremediated vulnerabilities references unique vulnerabilities within the environment, not specific to a system component.

<sup>8</sup> U.S. Department of Commerce, Office of Inspector General, November 15, 2010. *Office of the Secretary: Federal Information Security Management Act Audit Identified Significant Issues Requiring Management Attention*, final report no. OIG-11-012-A. Washington, DC: Commerce OIG.

<sup>9</sup> National Institute of Standards and Technology, February 2005. *Recommended Security Controls for Federal Information Systems*, NIST Special Publications 800-53 Rev. 3. Gaithersburg, MD.

**Table 4: Unremediated High-Risk Vulnerabilities Identified on NESDIS' Systems**

Time frame <sup>a</sup>	NESDIS Systems Reviewed							
	POES		GOES		ESPC		SARSAT	
	Unique Vul. <sup>b</sup>	Instances <sup>c</sup>	Unique Vul.	Instances	Unique Vul.	Instances	Unique Vul.	Instances
1990–1999	9	36	0	0	12	139	2	2
2000–2009	203	1,576	47	1,221	548	7,368	0	0
2010–2012 <sup>d</sup>	697	5,639	251	4,080	2,063	42,968	94	197
<b>Total</b>	<b>909</b>	<b>7,251</b>	<b>298</b>	<b>5,301</b>	<b>2,623</b>	<b>50,475</b>	<b>96</b>	<b>199</b>

Source: OIG analysis

<sup>a</sup> Time frame is when the vulnerability was identified in the software.

<sup>b</sup> Unique vulnerabilities is a total number of the distinct vulnerabilities for a specified timeframe on the system.

<sup>c</sup> Instances are the total number of vulnerabilities on a system for a specified timeframe.

<sup>d</sup> Since the scans we reviewed occurred at the beginning of 2013, the vulnerabilities related to 2013 were not included.

cause software to crash) before applying them. However, NESDIS staff admitted that they do not follow their own vulnerability remediation process. Specifically,

- Staff claimed that they are unable to deploy software and operating system security patches to POES, GOES, and ESPC within the approved patch cycle.<sup>10</sup>
- Staff from three of four NESDIS systems (POES, GOES, and ESPC) indicated that they do not track patches that cannot be applied to system components. This not only results in unpatched components, but it also leaves NESDIS with an inaccurate understanding of security risks within each system.<sup>11</sup>

As identified in findings I and II, NESDIS' systems are vulnerable to external attacks via unauthorized USB devices and system interconnections. Further, the presence of numerous high-risk vulnerabilities increases the risk that these systems could be successfully compromised.

#### B. NESDIS' Remote Access Deficiencies Leave Its Information Systems Vulnerable to Cyber Attacks

Both ESPC and SARSAT—the two systems we reviewed that allow remote access—lack two-factor authentication and do not have sufficient mechanisms to restrict the use of personal computers.

<sup>10</sup> NESDIS increased the remediation timeframe for GOES from the Department's required 30 days to 120 days to allow for more rigorous testing of software patches.

<sup>11</sup> In some instances, applying patches to fix a software flaw can affect a system's operations (such as rendering custom software inoperable) or have other adverse effects. If a patch cannot be applied, compensating controls are identified that will mitigate the risks of operating with the vulnerability. However, NESDIS did not have evidence of this process being applied in its remediation activities.

***NESDIS' information systems lack the required two-factor authentication necessary to secure remote access to its critical assets.*** We found that ESPC and SARSAT<sup>12</sup> have not implemented two-factor authentication for remote access. Without two-factor authentication, stolen credentials with administrative privileges could allow an attacker full access to the information system. For example, use of a secure token (e.g., a physical form of identification that is more difficult for an attacker to acquire) provides a second, stronger authentication element—in addition to basic authentication mechanisms such as a username and password—to the remote access process. As introduced in finding I, an attacker with access to one system poses a threat to other interconnected systems.

Implementation of two-factor authentication is a government-wide requirement for high-impact systems. Owing to resource constraints, NESDIS has chosen to forgo this requirement at this time. Further, NESDIS has not developed plans to implement the requirement, nor is it clear when NESDIS will comply.

***NESDIS did not follow the Department's requirement to restrict the use of personal computers for remote access.*** As personal computers are not required to adhere to Department policy, there is a distinct lack of assurance that these computers have the security necessary to protect the Department's information systems and data. Accordingly, the Department has expressly prohibited the use of personal computers for remotely accessing information systems for several years.<sup>13</sup> However, NESDIS does not restrict personal computer use; instead allowing personal computer use based on operational need, including remote administration of an information system. Specifically, we found:

- *NESDIS information systems lack the necessary security mechanisms to prohibit personal computer use.* ESPC and SARSAT asserted that appropriate remote access security mechanisms, including restricting personal computers, are implemented. However, we found the systems lack the necessary technical enforcement mechanisms to monitor for and stop personal computers from remotely accessing the information systems (e.g., checking remote connections to identify and restrict to authorized computers only).
- *NESDIS has experience with the perils of allowing personally owned devices access to its systems.* In a FY 2013 cyber incident, an attacker exfiltrated data from a NESDIS system to a suspicious external IP address via the remote connection established with a personal computer. The NOAA Computer Incident Response Team determined that the personal computer was likely infected with malware, but NOAA could not pursue the investigation because it involved a personal device, not government equipment (i.e., the owner of the personal computer, even though a NESDIS contractor, did not give NOAA permission to perform forensic activities on the personal computer). This incident highlights the risk of

<sup>12</sup> SARSAT has a waiver for two-factor authentication as it applies to its public user base. However, we are concerned with its system administrators, contractors, and other local users remotely accessing the system, for which that requirement still applies.

<sup>13</sup> Department policy specifies that personal computers are only allowed to access Web-based email services and select secure Web portals. U.S. Department of Commerce, February 2013, "Telework Program."

using personal computers to remotely access government information systems, as well as hindrances to incident response efforts.

- *NESDIS' current telework policy does not provide critical guidance on the appropriate use of personal computers.* Although NESDIS asserts that its policies and staff follow the Department's policies, we found that NESDIS' telework policy is ambiguous and contradicts the Department's telework policy. Specifically, NESDIS' policy does not specify under what circumstances personal computers are authorized to remotely access NESDIS' information systems, nor who may do so. Consequently, NESDIS' staff does not have clear guidance on this matter. By allowing access by personal computers, NESDIS is jeopardizing the security of its information systems.

### C. *NESDIS' Critical Mission Support Systems Continue to Lack Secure Configuration Settings*

We found that NESDIS has not implemented the secure configuration settings control, an essential aspect of securing an information system that, when appropriately implemented, can effectively minimize cyber attacks. For example, attackers look for easily exploitable default (unsecured) system configurations (e.g., extraneous software installed and default passwords) that are often set for ease-of-deployment and ease-of-use.

In order to implement secure configuration settings, each information system must (1) define a set of secure configuration settings for each IT product, (2) implement the configuration settings on all system components, (3) document approved deviations from the mandatory configuration settings, and (4) monitor components for changes to the established configuration settings.<sup>14</sup> Despite secure configuration settings being a required security control for more than six years, NESDIS' systems are only in the beginning stages of implementing this critical control's requirements.

We found that

- *None of the systems have successfully fulfilled these requirements, and the secure configuration settings remain unimplemented.* POES and GOES are in the process of defining secure baselines for the IT products in each system (the first requirement). SARSAT and ESPC are implementing the selected baselines and documenting deviations (the second and third requirements).
- *NESDIS has acquired an enterprise configuration settings monitoring tool (to meet the fourth implementation requirement), but its systems have not yet implemented secure configuration settings.* NESDIS intends to deploy the tool enterprise-wide to monitor baselines within all systems' components. However, each system (and NESDIS as a whole) cannot effectively use the tool to monitor for changes until secure baselines are selected and implemented, and deviations are documented.

---

<sup>14</sup> National Institute of Standards and Technology, Computer Security Division Information Technology Laboratory, August 2009. *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Rev. 3. Gaithersburg, MD.



Until NESDIS completely implements this critical control, assets central to its mission will continue to operate in an unsecure, vulnerable state.

### *Recommendations*

We recommend that NESDIS' Assistant Administrator and NOAA's Chief Information Officer:

7. Determine a feasible remediation timeframe for applying patches to POES, GOES, and ESPC.
8. Ensure that management gives appropriate priority to remediation of high-risk vulnerabilities in the required timeframe. If remediation is not feasible, ensure that vulnerabilities are documented and that compensating controls are implemented.
9. Ensure that information systems are compliant with all applicable remote access and telework policies and that two-factor authentication is implemented.
10. Ensure that NESDIS' telework policy complies with Department policy concerning the use of personal devices for remote access.
11. Implement the 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 by: (1) establishing and documenting mandatory configuration settings; (2) implementing these settings; (3) identifying, documenting, and approving deviations from mandatory settings; and (4) monitoring components for changes to the implemented settings.

#### IV. Improvements Are Needed to Provide Assurance That Independent Security Control Assessments Are Sufficiently Rigorous

An independent security control assessor must evaluate the security controls implemented on an information system prior to the organization placing the system into operation. These independent assessments provide the authorizing official (AO)<sup>15</sup> with an unbiased accounting of the system's security posture, such as the implementation status of security controls. The AO uses this information to ensure that the risks identified during the assessments are of an acceptable level to allow the system to operate. Inadequate security control assessments could misrepresent a system's security posture, giving the AO an inaccurate understanding of the risks when granting an authorization to operate.

To meet the requirement for independent security assessments of its information systems, NOAA procured the services of the FAA Enterprise Service Center, which is designated by OMB as a certification and accreditation shared-services provider. We evaluated 12 critical security control assessments<sup>16</sup> on each of the five NWS systems, for a total of 60 controls, to determine the quality of FAA's assessments. We found that 28 of 60 (47 percent) of the control assessments have deficiencies and may not have provided the AO with an accurate implementation status of the system's security controls.

***Independent assessors did not conduct sufficiently rigorous assessments of critical security controls.*** NOAA selected a designated certification and accreditation shared-services provider with the expectation that the assessments would be sufficiently rigorous. However, our review identified the following types of assessment deficiencies:

- *Assessment results lacked supporting evidence.* Although the FAA assessors reported that they performed appropriate tests of the security controls, there was no evidence to support the assessment results. For example, assessors claimed that components were configured to require appropriate password protections, but the assessors did not provide any evidence that an assessment was conducted.
- *Evidence collected during the assessments contradicted the assessor's conclusion.* The FAA assessors asserted that controls were appropriately implemented, despite evidence that directly contradicted these assertions. For example, the assessors concluded that there was an established baseline of authorized software enforced on the system, despite evidence collected by the assessors showing the presence of unauthorized software.
- *Not all requirements of the security control were assessed.* Regularly scanning system components for vulnerabilities is a key security requirement. Scans must be conducted with the appropriate credentials, which provide more complete vulnerability information. For example, the FAA assessors concluded the control was

<sup>15</sup> The *authorizing official* is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and the nation. Authorizing officials typically have budgetary oversight for an information system or are responsible for the mission and/or business operations supported by the system.

<sup>16</sup> These 12 security controls are a sub-set of the NIST 800-53 controls, which we selected as critical to securing an information system.

implemented, but they had an insufficient basis for reaching this conclusion, as they had not verified that NWS staff had conducted credentialed scans.

- *Not all types of IT products in a system were assessed.* To ensure that security controls are appropriately implemented on a system, assessors should assess each type of IT product in the information system. The FAA assessors, however, only reviewed certain IT products in a given NWS system—such as Microsoft Windows and Red Hat Linux—and did not assess others, such as Cisco IOS or databases. Thus, the assessors gained an incomplete picture of the risks within each system, and the implementation status of controls on these IT products remains unknown.

***NOAA would benefit from incorporating quality control measures into its review process.*** Currently, to ensure that authorization packages are complete and accurate prior to the AO's review, NOAA's OCIO staff conducts a compliance review. However, the review does not check the quality of the independent security control assessments; instead, it only ensures that the package has the required documents.

While NOAA's selection of a designated shared-service provider should have ensured its independent assessments were sufficiently rigorous, our findings indicate that NOAA would benefit from incorporating quality control measures into its review process. With these measures, the authorizing official has more assurance that the authorization package received is sufficient for an informed, risk-based decision.

### *Recommendation*

We recommend that NOAA's Chief Information Officer:

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

# Summary of Agency and OIG Comments

## NOAA Response

In response to our draft report, NOAA generally concurred with the findings and recommendations. NOAA indicated that it had already implemented recommendation 3, and partially implemented recommendation 7. NOAA also included suggested factual and technical changes to our findings.

NOAA stated that it implemented recommendation 3 by requiring that all NESDIS systems annually complete an authorization with independent security controls and risk assessments, and that both interconnected systems have a current authorization. NOAA also stated it has implemented recommendation 7 for GOES, and planned to implement for POES and ESPC.

NOAA took issue with some of the statements in findings I and III of the report, asking those to be revised. The specific issues NOAA highlighted are as follows:

- Issue 1: The statement that NOAA management did not factor risks associated with the POES-DMSP interconnection, when making the decision to authorize POES.
- Issue 2: The statement that DMSP is operating with significant deficiencies because the assessments referenced by the OIG occurred in 2013.
- Issue 3: The use of the statement “will immediately” inferred that NOAA was deliberately choosing not to correct significant deficiencies.
- Issue 4: The statement that NOAA could not appropriately characterize the POES-DMSP interconnection as a medium risk.
- Issue 5: The 2013 incident discussed in the finding III. B. was out of the scope of this audit because it was not directly related to the systems we assessed.

NOAA’s response is reproduced in its entirety in appendix C of this report.

## OIG Comments

With regard to recommendation 3, NOAA’s implementation is partially responsive to our recommendation. Our recommendation asks NOAA to require that all systems, even those owned by other agencies, complete control assessments and be authorized to operate, before establishing a connection.

While we made some modifications to our report based on NOAA’s response in issues 2 and 3, we stand by the statements regarding issues 1, 4, and 5, and explain our rationale accordingly:

- Issue 1: The statement was referencing the risk associated with DMSP’s interconnection with another high-impact NESDIS system that is connected to the Internet. This risk was not specifically conveyed in POES’s authorization package to NOAA management.

The authorization package is used by authorizing officials to make the risk-based decision in allowing a system to operate. Considering the close interweaving of POES and DMSP, the risk of interconnection between DMSP and the other NESDIS information system, which has a connection to the Internet, should have been specifically included in the authorization package.

- Issue 4: Regarding the POES-DMSP interconnection, NOAA did not consider the security risks within DMSP when determining the risk level for the interconnection, because the security posture of DMSP is unknown.

Currently, DMSP and POES continue to share domain controllers, which provide central account management and authentication services for these two systems. Sharing these critical services provide an easy way for malicious attackers to attack POES through DMSP, by bypassing nearly all internal protection mechanisms such as firewalls and user access controls.

We also believe that current security controls in place within POES will not effectively protect POES from attacks originating from DMSP. NOAA's own risk assessment report on POES, dated March 18, 2014, stated "there is no protection between DMSP and POES and the boundary is not properly documented."

- Issue 5: The incident mentioned in the report is very relevant to our finding related to remote access. As stated in the report, "this incident highlights the risk of using personal computers to remotely access government information systems, as well as hindrances to incident response efforts." However, we acknowledge that the incident did not occur on one of the systems that we focused on for our review.



# Appendix A: Objectives, Scope, and Methodology

Our audit objective was to assess the effectiveness of NOAA's information security program by determining whether key security measures adequately protect NOAA's systems. To do so, we:

- Assessed a subset of security controls on information system components
- Reviewed system-related artifacts, including policy and procedures, planning documents, and other material supporting the security authorization process
- Interviewed operating unit personnel, including system owners, IT security officers, IT administrators, and organizational directors and administrators

We reviewed NOAA's compliance with the following applicable internal controls, provisions of law, regulation, and mandatory guidance:

- The Federal Information Security Management Act of 2002
- IT Security Program Policy and Minimum Implementation Standards, U.S. Department of Commerce, introduced by the Chief Information Officer on January 9, 2009, and applicable Commerce Information Technology Requirements
- NIST Federal Information Processing Standards Publications:
  - 199, Standards for Security Categorization of Federal Information and Information Systems
  - 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Special Publications:
  - 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  - 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations
  - 800-53 A Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans

We conducted our field work from March 2013 to December 2013. We performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated April 26, 2013, and in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

## Appendix B: List of Acronyms and Abbreviations

Acronym	Definition
AO	Authorizing Official
ATO	Authorization to Operate
AWC	Aviation Weather Center
Cisco IOS	Cisco Internetwork Operating System
DMSP	Defense Meteorological Satellite Program
ESPC	Environmental Satellite Processing Center
FAA	Federal Aviation Administration
FISMA	The Federal Information Security Management Act of 2002
GOES	Geostationary Operational Environmental Satellites
GSLEP	Ground Service Life Extension Program
IT	Information Technology
NCEP	National Centers for Environmental Prediction
NESDIS	National Environmental Satellite, Data, and Information Service
NHC	National Hurricane Center
NIST	National Institute for Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NWS	National Weather Service
OCIO	Office of the Chief Information Officer
POES	Polar-orbiting Operational Environmental Satellites
SARSAT	Search and Rescue Satellite Aided Tracking
SPC	Storm Prediction Center
SWPC	Space Weather Prediction Center
USAF	U.S. Air Force
USB	Universal Serial Bus
Vul	Vulnerabilities

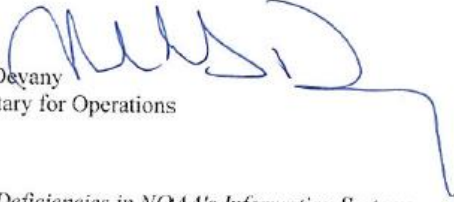
# Appendix C: Agency Response



UNITED STATES DEPARTMENT OF COMMERCE  
The Deputy Under Secretary for Operations  
Washington, D.C. 20230

6/6/2014

MEMORANDUM FOR: Allen Crawley  
Assistant Inspector General for Systems Acquisition  
and IT Security

FROM: VADM Michael S. Deyany   
Deputy Under Secretary for Operations

SUBJECT: *Significant Security Deficiencies in NOAA's Information Systems  
Place Its National Critical Mission at Risk*  
Draft OIG Audit Report

Thank you for the opportunity to comment on the Office of the Inspector General's draft audit report evaluating selected NOAA information systems. We recognize the need to maintain a strong but cost-effective security posture to support our critical mission responsibilities, to keep pace with growing environmental data and product needs, and to manage IT security risk in a challenging fiscal climate.

Our specific comments on the report's findings and recommendations are attached.

Attachment



**Department of Commerce  
National Oceanic and Atmospheric Administration  
Comments on the Draft OIG Report Entitled  
“Significant Security Deficiencies in NOAA’s Information Systems Place Its National  
Critical Mission at Risk”  
(Draft Report – May 9, 2014)**

**General Comments**

NOAA generally concurs with the findings and recommendations in the report. NOAA is committed to maintaining a cost-effective IT security program that manages risk at an acceptable level. We had already identified most of the concerns cited by the OIG in the report and have been implementing remediation efforts as documented in the Plans of Action and Milestones (POA&M) tracking system used by the Department of Commerce.

**Recommended Changes for Factual/Technical Information**

*Page 4, first bulleted paragraph, last sentence, to top of page 5:*

The statement “Consequently NOAA management did not factor this significant risk into its subsequent risk-based authorization decision” is not accurate. The security assessment report and briefing to NOAA management highlighted the “key boundary” findings regarding POES and DMSP, the status of the existing high-risk POA&M to track deficiency remediation, as well as ongoing efforts to engage USAF for a security and risk assessment of DMSP. To claim that they “did not factor” this into an informed risk determination is without basis. Request this statement be removed from the report as unsupported considering the facts present in the briefing and reports from the independent security controls assessment.

*Page 5, first bulleted paragraph:*

There is no evidence presented to support the statement that “DMSP is operating with significant deficiencies.” While the security posture of specific shared components may have been scanned at a point in time in 2013, there is no support for a statement as to whether the deficiencies discovered at that time reflected, or continue to reflect, the overall DMSP security posture to state that DMSP is or is not currently still operating “with significant deficiencies.” Request this section be deleted from the report. The reference to scan results from one point in time in 2013 has no bearing on the current state of DMSP’s security posture to state as if a fact that it “is” currently operating with a security posture. This statement is supposition that has no basis in evidence presented.

*Page 5, second bulleted paragraph, second sentence:*

Change “will immediately” to “are able at this time to”. The statement “Neither NESDIS nor USAF will immediately address the deficiencies” implies that these agencies are able to

“immediately” address them but conscientiously choose not to address them. That is not the case. We must operate within limited resources and remediate these deficiencies in accordance with the established POA&M.

*Page 5, last paragraph, through the first full paragraph at the top of page 6:*

This narrative seems to imply that the designation of risk as “medium” was inappropriate; however, no facts are provided to refute this determination or contest the risk analysis performed and documented as the basis for this determination. The independent risk assessment, performed in accordance with the methodology of NIST Special Publication 800-30 Revision 1, considered the potential threats to the system, safeguards in place to mitigate exploitation of vulnerabilities, the high-risk POA&M tracked for remediating the acknowledged boundary separation deficiency, and the results of independent tests of security controls including penetration testing. Furthermore, the assertion that the existing firewall configuration, user account controls, intrusion detection monitoring, anti-virus software, and audit logging, “will not protect POES” is inaccurate. These countermeasures, while they may not reduce residual risk to a low level, they do serve to prevent and detect harmful actions by internal and external threat-sources, and in so doing, mitigate risk. We request this narrative to be revised.

*Page 12, last paragraph:*

The 2013 incident mentioned was not associated with any of the NESDIS systems identified as included in the audit scope or in the scope of this finding as described at the top of page 12. This paragraph leads the reader to assume that the incident referenced pertains to one of these systems but it does not. The system affected was not even a high-impact system, and was subject to a different security controls baseline than the high-impact systems that were in the scope of this audit. Request deletion of this paragraph from the report as misleading and out of scope of the FY2013 FISMA audit as announced and as described in the Introduction section of the draft report.

#### Editorial Comments

None.

#### NOAA Response to OIG Recommendations

**Recommendation 1:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer conduct a review to determine the risks posed by NESDIS’ restricted systems” interconnections with other information systems.”

**NOAA Response:** NOAA concurs. Implementation of this recommendation is already under way. We are tracking POA&Ms to review and improve POES interconnection security agreements as well as to evaluate the risk associated with the comingled POES and DMSP system boundaries so that we can design a feasible solution to securely separate the systems. In



addition, our annual independent security assessments include comprehensive tests of mechanisms that monitor events on shared system components to ensure that anomalous system behavior is detected, logged, and investigated.

**Recommendation 2:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer document and convey to NOAA senior management the risks identified with these interconnections.”

**NOAA Response:** NOAA concurs and will inform NOAA senior management regarding the risk as briefed to the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer for the FY2014 security assessment report and system re-authorization.

**Recommendation 3:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer require that interconnected systems have completed control assessments and are authorized to operate before establishing an interconnection.”

**NOAA Response:** NOAA concurs and already does this. All NESDIS systems are subjected annually to independent security controls and risk assessments, which support the Authorizing Official’s annual written determination of risk acceptance and decision to continue the system’s authorization to operate. Interconnection security agreements require that both systems involved in an interconnection have a current authorization to operate before the Authorizing Officials will approve the interconnection by signing the agreement.

**Recommendation 4:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer pursue USAF’s commitment that DMSP meets Department of Commerce’s security requirements and conduct security assessments as outlined in a memorandum from the USAF to NOAA on May 13, 2010.”

**NOAA Response:** NOAA concurs. We will engage USAF regarding its efforts to meet the terms of our agreement with regard to DMSP.

**Recommendation 5:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer prevent components from moving between the GOES network and SWPC network for maintenance activities.”

**NOAA Response:** NOAA concurs. We are reviewing the Interconnection Security Agreement between GOES and SWPC to clarify maintenance responsibilities and restrictions on maintenance practices regarding GOES components.



**Recommendation 6:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer implement security mechanisms to protect against the use of unauthorized mobile devices.”

**NOAA Response:** NOAA concurs. System Security Plans for ESPC, POES, and GOES will be updated to enhance the Mobile Device policy to specify devices authorized for use within the system environment. In addition, NESDIS will procure tools appropriate for these systems to automate monitoring of USB device use. We have already processed a Change Control Request to disable *AutoRun* on the GOES system through Group Policy (CCR2707) and the *AutoRun* feature for ESPC components has been disabled as a part of the quarterly preventive maintenance Change Control Request.

**Recommendation 7:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer determine a feasible remediation timeframe for applying patches to POES, GOES, and ESPC.”

**NOAA Response:** NOAA concurs. We have already completed this determination for GOES. On April 14, 2014, the Authorizing Officials approved that due to operational availability and integrity requirements, critical and high priority patches cannot be installed within Commerce, NOAA and NESDIS defined time frames because of the need to thoroughly test the patches prior to deployment within the operations capability. The sensitivity of the GOES Ground System components and the requirement for extensive patch testing and burn-in periods precludes remediation of critical and high flaws as required by CTR-016. In lieu of the CTR-016’s 30-day time frame for patching, OSPO has implemented a 120-day flaw remediation cycle for the GOES Ground System to address all flaws identified through vulnerability scanning. POA&M #59980 has been established with a scheduled completion date of February 28, 2015, to complete this determination for POES and POA&M #60301 with a scheduled completion date of March 27, 2015, for ESPC.

**Recommendation 8:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer ensure that management gives appropriate priority to remediation of high-risk vulnerabilities in the required timeframe. If remediation is not feasible, ensure that vulnerabilities are documented and that compensating controls are implemented.”

**NOAA Response:** NOAA concurs. We employ a rigorous independent security controls assessment and continuous monitoring process that identifies and documents vulnerabilities, identifies and tests the ability of mitigating and compensating controls to reduce risk, quantifies and explains the residual risk to Authorizing Officials, and tracks corrective actions to reduce risk to an acceptable level. NESDIS has implemented a quarterly IT security status review in which system owners discuss their system’s security posture with the NESDIS Deputy Assistant

Administrator, and IT security status is presented monthly to the Assistant Administrator by the NESDIS Assistant Chief Information Officer.

**Recommendation 9:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer ensure that information systems are compliant with all applicable remote access and telework policies and that two-factor authentication is implemented.”

**NOAA Response:** NOAA concurs. We assess system compliance with Remote Access and Alternate Work Site controls requirements (controls AC-17 and PE-17) as part of our independent security controls assessment process. NOAA has established a group to design a feasible solution to implement multi-factor authentication on high-impact systems. These systems have unique challenges with new technology initiatives, and involve designs that are costly to implement.

**Recommendation 10:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer ensure that NESDIS’ telework policy complies with Department policy concerning the use of personal devices for remote access.”

**NOAA Response:** NOAA concurs. We will review the NESDIS telework policy for compliant use of personal computers in accordance with the Commerce Information Technology Requirement (CITR) 008 for *Remote Access*.

**Recommendation 11:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer implement the necessary security mechanisms to secure against remote access via personal computers.”

**NOAA Response:** NOAA concurs. NESDIS will evaluate, select, and implement a feasible solution to secure ESPC and SARSAT against remote access via personal computers.

**Recommendation 12:** “We recommend that the NESDIS’ Assistant Administrator and NOAA’s Chief Information Officer ensure that appropriate attention is given to implementing required secure configuration settings in a timely manner and continue the implementation by: (1) establishing and documenting mandatory configuration settings; (2) implementing these settings; (3) identifying, documenting, and approving deviations from mandatory settings; and (4) monitoring components for changes to the implemented settings.”

**NOAA Response:** NOAA concurs. Implementation of this recommendation is already underway. POA&Ms exist for non-compliant systems to track remediation of these deficiencies.

**Recommendation 13:** “We recommend that NOAA’s Chief Information Officer develop a quality control process that provides better assurance that security controls are appropriately assessed before the authorization package is assembled and submitted to the authorizing official.”

**NOAA Response:** NOAA concurs. NOAA has established a process to evaluate security authorization packages for compliance and quality prior to issuance of the annual risk acceptance and authorization to operate decision by the Authorizing Officials. NOAA will revise, expand, or replace this process to address control assessment quality.