



# NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

## Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT Security Program

FINAL REPORT NO. OIG-16-043-A  
AUGUST 26, 2016

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

**FOR PUBLIC RELEASE**





August 26, 2016

**MEMORANDUM FOR:** Dr. Kathryn D. 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:** *Successful Cyber Attack Highlights Longstanding Deficiencies  
in NOAA's IT Security Program*  
Final Report No. OIG-16-043-A

Attached is our final report on OIG's audit of NOAA's IT systems in response to a significant cyber attack that took place in September 2014. We conducted this audit to (1) determine the significant factors that contributed to the successful cyber attack on NOAA information systems and (2) evaluate NOAA's handling of the detection, analysis, eradication, and reporting of the attack, as well as recovery from it.

Regarding our first objective, we found that NESDIS systems were vulnerable because the office had not addressed weaknesses in the information security practices applied to the compromised system components. Specifically, we found that (1) deficiencies in risk management left an application exposed to attack, (2) practices for detecting web application vulnerabilities were inadequate, and (3) the attacker obtained unauthorized access to additional systems because NOAA deferred implementation of additional access controls which had been required since 2006.

We limited our review of the second objective to NOAA's containment and recovery efforts, specifically focusing on the issues that prolonged the disruption of disseminating weather satellite data. We focused on these issues because they resulted in the greatest impact to NESDIS operations. We found that inadequate firewall management practices prolonged the disruption.

We have summarized NOAA's response to our draft report and included its entire formal response as appendix B. The final report will be posted on 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 your action plan within 60 days of this memorandum. The plan should outline the actions you propose to take to address each recommendation.

We appreciate the cooperation and courtesies extended to us by your staff during this audit. If you have any questions or concerns about this report, please 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, OS  
Ben Friedman, Deputy Under Secretary for Operations, NOAA  
Stephen Volz, Assistant Administrator for Satellite and Information Services, NOAA  
Mark S. Paese, Deputy Assistant Administrator and Acting Assistant Chief Information Officer for Satellite and Information Services, NOAA  
Rod Turk, Director, Office of Cyber Security, and Chief Information Security Officer  
Zachary G. Goldstein, Chief Information Officer, NOAA  
Robert Hembrook, Acting Director, Cyber Security Division, NOAA  
Mack Cato, Audit Liaison, NOAA  
Joselyn Bingham, Audit Liaison, Office of the Chief Information Officer  
Maria Stanton-Dumas, Audit Liaison, Office of the Chief Information Officer  
MaryAnn Mausser, Audit Liaison, OS



# Report in Brief

AUGUST 26, 2016

## Background

In early September 2014, NOAA experienced a significant cyber attack. An attacker exploited vulnerabilities in Internet accessible web applications and eventually compromised important internal NOAA systems operated by the National Environmental Satellite, Data, and Information Service (NESDIS). NESDIS is responsible for providing global environmental data from satellites and other sources to promote, protect, and enhance the nation's economy, security, environment, and quality of life.

The attacker compromised three NESDIS systems and gained complete control of system components within one of them. The attacker was also able to use usernames and passwords gathered from one of these systems to obtain unauthorized access to another three NOAA systems.

## Why We Did This Review

We conducted this audit to (1) determine the significant factors that contributed to the successful cyber attack on NOAA information systems and (2) evaluate NOAA's handling of the detection, analysis, eradication, and reporting of the attack, as well as recovery from it.

## NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

### Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT Security Program

OIG-16-043-A

#### WHAT WE FOUND

Regarding our first objective, we found that NESDIS systems were vulnerable because the office had not addressed weaknesses in the information security practices applied to the compromised system components. Specifically, we found that (1) deficiencies in risk management left an application exposed to attack, (2) practices for detecting web application vulnerabilities were inadequate, and (3) the attacker obtained unauthorized access to additional systems because NOAA deferred implementation of additional access controls which had been required since 2006.

We limited our review of the second objective to NOAA's containment and recovery efforts, specifically focusing on the issues that prolonged the disruption of disseminating weather satellite data. We focused on these issues because they resulted in the greatest impact to NESDIS operations. We found that inadequate firewall management practices prolonged the disruption.

#### WHAT WE RECOMMEND

We recommend that NESDIS' Assistant Administrator do the following:

1. Improve risk management practices to reduce the exposure of web application vulnerabilities when decisions are made to not remediate known issues.
2. Formally review Internet exposed web applications and determine if access from the Internet is justified.
3. Deploy the specialized web application vulnerability scanning tool and an updated assessment process that requires more than one assessment tool; especially on web applications.
4. Ensure that all web applications are scanned for vulnerabilities on a quarterly basis.
5. Ensure that the same methodology used to identify a vulnerability is also used to validate its remediation.
6. Establish and implement procedures to periodically review firewall rules.
7. Develop an improved practice for managing plans of action and milestones (POA&Ms) to ensure that evidence showing actual remediation of a weakness identified in the POA&M is submitted, reviewed, and approved before the POA&M is closed.

We recommend that NOAA's Chief Information Officer do the following:

8. Ensure that adequate measures are taken to implement mechanisms for multifactor authentication in a timely manner for all applicable users and applications.

# Contents

- Introduction ..... 1
- Objectives, Findings, and Recommendations ..... 3
  - I. Deficiencies in Risk Management Left an Application Exposed to Attack..... 3
  - II. Web Application Vulnerability Assessments Were Not Conducted Routinely and Missed Hundreds of High-Risk Vulnerabilities ..... 4
    - A. Web application vulnerability assessments should be conducted routinely..... 4
    - B. Using multiple vulnerability assessment tools may improve detection of critical vulnerabilities ..... 5
  - III. Deferred Implementation of Multifactor Authentication Allowed Unauthorized Access to Additional Systems ..... 5
  - IV. Inadequate Firewall Management Practices Prolonged the Disruption of Disseminating Weather Satellite Data..... 6
    - A. The ESPC firewall ruleset was not regularly reviewed and interconnections were not properly documented..... 7
    - B. ESPC firewall management weaknesses were not resolved because remediation plans were inadequate ..... 7
    - C. The number and complexity of the ESPC firewall rules and inadequate interconnection documentation prolonged efforts to resume dissemination of weather satellite data..... 8
- Recommendations ..... 9
- Summary of Agency Response and OIG Comments..... 10
- Appendix A: Objectives, Scope, and Methodology ..... 11
- Appendix B: Agency Response ..... 13

*COVER: Detail of fisheries pediment,  
U.S. Department of Commerce headquarters,  
by sculptor James Earle Fraser, 1934*

## Introduction

In early September 2014, the National Oceanic and Atmospheric Administration (NOAA) experienced a significant cyber attack. An attacker exploited vulnerabilities in Internet accessible web applications and eventually compromised important internal NOAA systems operated by the National Environmental Satellite, Data, and Information Service (NESDIS). NESDIS is responsible for providing global environmental data from satellites and other sources to promote, protect, and enhance the nation's economy, security, environment, and quality of life.

The attacker compromised three NESDIS systems and gained complete control of system components<sup>1</sup> within one of them. The systems compromised include:

- (1) *The Environmental Satellite Processing Center (ESPC)*. The ESPC is a high-impact system which is the most critical system compromised because it is responsible for disseminating critical weather satellite data to NESDIS customers.<sup>2</sup>
- (2) *The NOAA Satellite Operations Facility Administrative Local Area Network (NSOF Admin LAN)*. The NSOF Admin LAN is a moderate-impact system which provides office automation for the Satellite Operations Facility and public information via the Internet. The attacker gained complete control over system components within this system.
- (3) *The National Geophysical Data Center (NGDC) Data Archive Management and User System*. The NGDC Data Archive Management and User System is a moderate-impact system which provides access to archived weather data and supports NGDC office automation.

The attacker was also able to use usernames and passwords gathered from the NSOF system to obtain unauthorized access to:

- NESDIS' Headquarters Information Technology Support Local Area Network (HQ ITS LAN)—a moderate impact system;
- NOAA's Web Operation Center (WOC)—a high-impact system; and
- NOAA's Cyber Security Center (NCSC)—a high-impact system.

---

<sup>1</sup> Examples of system components include servers and workstations.

<sup>2</sup> Examples of weather satellite data customers include the National Weather Service, the United States Navy's and the United States Air Force's primary forecast centers, international forecast centers, academia, and the private sector.



NOAA investigated the attack and determined that the attacker, at the very least, obtained sensitive information including usernames and passwords (including those of system administrators) and system configuration information. The attacker was also able to gain access to NOAA's cyber incident tracking system and obtain records documenting NOAA's efforts to analyze the attack. However, NOAA was unable to determine the full extent of the data obtained from NOAA systems<sup>3</sup> so the full impact of the compromise is still unknown.

NOAA discovered that NESDIS systems had been compromised during the first week of September 2014 and NOAA's Computer Incident Response Team (N-CIRT) began an investigation that included (1) analyzing malware found on the compromised system components, (2) searching for other system components that may be infected by malware, and (3) reviewing network traffic.

On October 20, 2014, one of NESDIS' public websites was defaced in an unrelated attack on one of its already compromised systems and NOAA officials determined that they could no longer wait to implement full containment efforts, which included disconnecting NESDIS systems from the Internet. ESPC was included in the disconnected systems, resulting in the disruption of disseminating weather satellite data during that period. Officials from the National Weather Service's National Centers for Environmental Prediction (NCEP) assert that this satellite data is critical to the weather prediction models used by forecasters. Weather forecasters rely on NESDIS systems such as ESPC to provide weather satellite data to enhance forecasts and increase the accuracy of severe weather warnings.

By October 22, 2014, containment and recovery efforts enabled NESDIS to resume distributing critical weather satellite data from ESPC. Unfortunately, NESDIS was unable to recover the satellite data gathered from October 20–22. While this loss of data was noteworthy, NCEP could not fully determine the impact on the weather prediction models during the disruption. But, according to NCEP officials, a longer period of data loss could increase the impact on the models over time. Therefore, longer disruptions could lead to a degradation of weather forecasting, which may also affect the accuracy of predicting severe weather events in the future.

### *Information Obtained During the Attack*

- Usernames and passwords
- System configuration information
- Incident tracking records concerning the attack

---

<sup>3</sup> According to NOAA, the unavailability of logs and the attacker's use of encryption when exfiltrating data limited its ability to determine the full extent of the compromise.

# Objectives, Findings, and Recommendations

We conducted this audit to (1) determine the significant factors that contributed to the successful cyber attack on NOAA's information systems, and (2) evaluate NOAA's handling of the detection, analysis, eradication, and reporting of the attack, as well as recovery from it.

In regards to our first objective, we found that NESDIS systems were vulnerable because the office had not addressed weaknesses in the information security practices applied to the compromised system components. Specifically, we found that (1) deficiencies in risk management left an application exposed to attack, (2) practices for detecting web application vulnerabilities were inadequate, and (3) the attacker obtained unauthorized access to additional systems because NOAA deferred implementation of additional access controls which had been required since 2006.

We limited our review of the second objective to NOAA's containment and recovery efforts, specifically focusing on the issues that prolonged the disruption of disseminating weather satellite data. We focused on these issues because they resulted in the greatest impact to NESDIS operations. We found that inadequate firewall management practices prolonged the disruption.

## I. Deficiencies in Risk Management Left an Application Exposed to Attack

The attacker initially compromised the NESDIS NSOF Admin LAN system through a publicly accessible web application that supported only internal NOAA users. NOAA believes that the attacker compromised this application by exploiting a high-risk web application input validation vulnerability.<sup>4</sup> We found that NESDIS had previously learned, during penetration testing conducted in February 2013, that this application was vulnerable to such exploits. However, NESDIS officials explained that they did not take steps to mitigate this risk because the web developer support needed to correct such vulnerabilities had been discontinued. Even though NESDIS had previously identified the vulnerability, they did not take sufficient action to remediate the vulnerability or mitigate the risk it posed.

According to N-CIRT, the functions compromised by the attacker were only used by internal NOAA users and did not need to be publicly accessible. Department policy requires that NESDIS follow security control requirements defined by the National Institute of Standards and Technology (NIST) which include a requirement to limit information systems to the least functionality necessary.<sup>5</sup> In addition, NIST risk management guidance suggests that when assessing risks it is useful to consider the possibility of attackers

---

<sup>4</sup> An example of such vulnerabilities is structured query language (SQL) injection, which allows an attacker to execute a command via a web form to extract, modify, or destroy the data stored in the back-end database.

<sup>5</sup> U.S. Department of Commerce National Institute of Standards and Technology, August 2009. *Recommended Security Controls for Federal Information Systems*, NIST Special Publication 800-53, Rev. 3. Gaithersburg, MD: NIST, F-43. See also NIST, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Rev. 4. Gaithersburg, MD: NIST, F-71.



exploiting unauthorized or poorly configured information systems exposed to the Internet.<sup>6</sup> Had NIST's requirement been fully implemented or the risk of the vulnerability been properly managed, NESDIS would have limited the vulnerable functions to internal use only. Doing so would have reduced the exposure of the vulnerability and the related risk of compromise.

## II. Web Application Vulnerability Assessments Were Not Conducted Routinely and Missed Hundreds of High-Risk Vulnerabilities

In addition to the web application in the NSOF Admin LAN, the attacker also compromised web applications in the NGDC and ESPC systems. Prior to the attack, NESDIS had performed web application vulnerability assessments on these applications; however, these assessments were not effective in identifying vulnerabilities. First, NESDIS did not always assess web application vulnerabilities for the ESPC and NSOF Admin LAN web applications. In addition, prior to the attack, NESDIS only used a single assessment tool when assessing all three applications that were breached—but, after the attack, found hundreds of high-risk vulnerabilities in the NSOF Admin LAN and NGDC applications by using a different assessment tool. NESDIS may be able to improve vulnerability detection by conducting regular assessments and using multiple assessment tools.

### A. *Web application vulnerability assessments should be conducted routinely*

According to Department policy,<sup>7</sup> all IT assets on a system's network must be assessed for vulnerabilities at least quarterly. NESDIS conducted quarterly assessments on the web server compromised within ESPC, but the assessment tool was not always configured to check for web application vulnerabilities. We examined assessments for the five consecutive quarters preceding the attack and found that only the assessment for the last quarter included web application vulnerability assessments.

During the last quarter's assessment, NESDIS identified the vulnerability it believes the attacker used to compromise the system; however, this identification occurred only 15 days prior to the attack, leaving little time for corrective action and no room for delay. Efforts to remediate the vulnerability were delayed because of staffing changes and an ongoing upgrade to the server hosting the vulnerable application. If the assessments for the previous quarters had included assessments for web application vulnerabilities it is very likely that NESDIS would have identified this vulnerability earlier when it could have been addressed long before the attack.

In addition, failure to run a web application assessment on the NSOF Admin LAN application—previously mentioned in finding one—led to a false sense of security. Although NESDIS did not take actions to mitigate or remediate the input validation vulnerability in its web application identified in February 2013, as discussed in finding I, it

<sup>6</sup> NIST, September 2012. *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30, Rev. 1. Gaithersburg, MD: NIST, E-3.

<sup>7</sup> DOC, January 25, 2012. *Commerce Information Technology Requirement, Vulnerability Scanning and Patch Management*, CITR-016. Washington, DC: DOC, 2.

conducted an assessment almost 15 months later to determine if the vulnerability was still present. However, that assessment did not include checks for web application vulnerabilities so the vulnerability was not identified during the assessment, even though it was still present. Based on these results, NESDIS incorrectly concluded that the vulnerability had been remediated. In the future, when conducting vulnerability assessments on servers that host web applications, NESDIS needs to ensure that its assessments always include steps to check for web application vulnerabilities.

*B. Using multiple vulnerability assessment tools may improve detection of critical vulnerabilities*

NIST's guide for conducting information security assessments explains that vulnerabilities that are undetected by one assessment tool can potentially be identified by another and that it is a common practice to use multiple vulnerability assessment tools to improve identification of vulnerabilities.<sup>8</sup> However, NESDIS only used a single assessment tool to identify web application vulnerabilities for the ESPC, NSOF Admin LAN, and NGDC web applications compromised by the attacker.

Following the attack, NESDIS used an additional assessment tool specialized for web application assessments to evaluate the NGDC and NSOF Admin LAN applications and found hundreds of high-risk vulnerabilities that had not been previously identified. In May 2014, the Department had provided NOAA with licenses for this specialized tool, at no cost to NOAA. However, prior to the attack, NESDIS did not use the tool. In December 2015, NOAA began a project to determine whether to use it as part of their regular assessments. NESDIS should use additional vulnerability assessment tools to increase the likelihood that it can reduce the number of unknown vulnerabilities as much as is practicable, especially considering that the attacker compromised the NGDC application using a vulnerability that NESDIS had previously not identified.

### III. Deferred Implementation of Multifactor Authentication Allowed Unauthorized Access to Additional Systems

The attacker was able to gain unauthorized access to web applications within the NESDIS HQ ITS LAN, the NCSC, and WOC systems and obtain sensitive information from the NCSC. The attacker was able to gain access to these systems by reusing usernames and passwords it had obtained from its initial compromise because multifactor authentication was not fully implemented for these systems. Although multifactor authentication was required for these systems and known to not be in place, NOAA accepted the risk of not implementing or of deferring implementation of this control.

Multifactor authentication provides additional security beyond traditional username/password authentication because it requires that more than one authentication method is used—such as a combination of password, token (i.e., a hardware device used for authentication, such as an identification card or key fob), fingerprint, or other means. This

---

<sup>8</sup> NIST, September 2008. *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115. Gaithersburg, MD: NIST, 4–6.

control has been required since 2006 for NOAA's high-impact systems and since 2010 for its moderate-impact systems.

However, we found that NOAA did not fully implement this control for the three systems where the attacker obtained unauthorized access: the HQ ITS LAN, the NCSC system, and a restricted website within the WOC system. NOAA either accepted the risks associated with not fully implementing this control or deferred full implementation of this control for these systems. As a result, multifactor authentication was not in place for these systems when the attack occurred.

Without this control in place, the attacker was able to use usernames and passwords obtained from its initial compromise of the NSOF Admin LAN to obtain unauthorized access to information within the NCSC, HQ ITS LAN, and WOC systems. From the NCSC system, the attacker obtained the sensitive report NOAA was using to coordinate its response to the attack and from the NESDIS HQ ITS LAN, the attacker obtained non-sensitive NOAA policy documentation. Although the attacker gained unauthorized access to the WOC system, the data it exfiltrated was already publicly accessible, and therefore not considered sensitive.

One and a half months prior to this attack, we reported that two other NESDIS systems—ESPC and the Search and Rescue Satellite Aided Tracking (SARSAT) system—also lacked multifactor authentication because, again, NESDIS deferred implementation of this control.<sup>9</sup> The attacker's successful use of previously obtained credentials during this attack demonstrates why we recommended multifactor authentication should be implemented for ESPC and SARSAT and why it is required and should be implemented for all of NOAA's high- and moderate-impact systems. According to NOAA officials, a planned update to the NCSC application will support multifactor authentication.

#### IV. Inadequate Firewall Management Practices Prolonged the Disruption of Disseminating Weather Satellite Data

As a standard security practice, ESPC uses firewalls to control access to and from its network entry points, including the Internet. Firewalls control access by enforcing specific rules, which allow or deny connections between computers and networks. However, the ESPC firewall ruleset was not periodically reviewed and its interconnections were not properly documented, resulting in an overly complex ruleset and confusion concerning what systems interconnected with ESPC. These issues had previously been identified, but were not corrected because remediation plans were inadequate. These issues also prolonged NESDIS' efforts to resume dissemination of weather satellite data through ESPC after it had been disconnected as part of NOAA's strategy to contain and recover from the attack.

---

<sup>9</sup> DOC OIG, July 15, 2014. *Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission*, OIG-14-025-A. Washington, DC: OIG, 12. As of August 22, 2016, 9 of the 13 recommendations agreed to in the report were still unimplemented.

A. *The ESPC firewall ruleset was not regularly reviewed and interconnections were not properly documented*

Firewall rulesets should be actively managed and regularly reviewed as specified in NIST's guide for managing firewalls and firewall policies, which states:

Firewall rulesets and policies should be managed by a formal change management control process because of their potential to impact security and business operations, with ruleset reviews or tests performed periodically to ensure compliance with the organization's policies.<sup>10</sup>

However, NESDIS did not periodically review the ESPC firewall ruleset, and its operating procedures for the firewall do not require any such reviews. As a result, the firewall was not properly managed and over a 10-year period it accumulated an overly complex and lengthy ruleset, with more than 16,000 rules. In addition, the firewall's interconnections with other systems were not properly documented, making it difficult to determine which rules were appropriate and what systems should be permitted to connect to ESPC.

B. *ESPC firewall management weaknesses were not resolved because remediation plans were inadequate*

In 2012, NESDIS found that the ESPC firewall's rules had not been maintained and that its interconnections had not been properly documented, even noting that some rules slated for removal in 2007 were still present. However, these weaknesses were not resolved because NESDIS lost track of them after incorrectly concluding they had been resolved without validating remediation efforts.

NESDIS IT security weaknesses are tracked in remediation plans known as plans of action and milestones (POA&Ms). According to the Office of Management and Budget (OMB), a POA&M should only be considered completed when a weakness has been fully resolved, including testing corrective actions.<sup>11</sup> However, NESDIS' POA&M addressing these weaknesses did not meet the OMB requirement. The weaknesses were grouped together into a single POA&M with completion criteria that only required a plan be developed to remediate the weaknesses. Instead, NESDIS should have required evidence showing that the weaknesses were actually remediated.

NESDIS did develop a plan associated with the firewall weaknesses and closed the POA&M, but the plan did not adequately address those weaknesses and no evidence was provided showing that they had been addressed. Since NESDIS did not ensure the weaknesses were resolved, they were still present by the time it began efforts to contain and recover from the attack. This is not a new issue with ESPC; in 2010, we

<sup>10</sup> NIST, September 2009. *Guidelines on Firewalls and Firewall Policy*, NIST Special Publication 800-41, Rev. 1. Gaithersburg, MD: NIST, ES-2.

<sup>11</sup> U.S. Executive Office of the President Office of Management and Budget, October 17, 2001. *Guidance for Preparing and Submitting Security Plans of Actions and Milestones*, Memorandum M-02-01. Washington, DC: OMB.

previously reported that POA&Ms for ESPC had similar deficiencies in that they also did not provide adequate evidence that weaknesses had been addressed.<sup>12</sup>

*C. The number and complexity of the ESPC firewall rules and inadequate interconnection documentation prolonged efforts to resume dissemination of weather satellite data*

ESPC was disconnected from the Internet on October 20, 2014, as part of NESDIS' strategy to contain and recover from the attack. As a result, the dissemination of weather satellite data was disrupted. NESDIS determined that to reduce the risk of further compromise and prevent the attacker from getting back into the system, it needed to review and rebuild the firewall ruleset rule-by-rule before ESPC could be reconnected to the Internet.

Because the weaknesses in maintaining the ESPC firewall ruleset had never been addressed, there were over 16,000 rules to review and rebuild. After determining it would take significant time to rebuild the entire set of firewall rules, NESDIS decided to rebuild just the subset of over 3,100 rules that controlled access to the Internet. Efforts to review the rules and implement and validate changes were prolonged because of the complexity of the ruleset<sup>13</sup> and the improperly documented interconnections, which made it challenging to determine what rules were appropriate and if all the systems requiring interconnection with ESPC were able to connect. ESPC was reconnected to the Internet on October 22, 2014, and resumed dissemination of weather satellite data. As previously explained, NCEP was unable to determine how much the outage impacted weather forecasting, but has asserted that weather satellite data is critical to weather forecasting operations. According to NOAA officials, NESDIS had completed its efforts to review and clean up the entire ruleset for the firewall.

The findings presented in this report raise our concerns about NOAA's commitment to properly managing security risks to minimize the likelihood of falling victim to cyber attacks. We are especially concerned that—particularly within NESDIS systems—NOAA continues to accept the risks of not remediating identified vulnerabilities, delay corrective action when it is planned, and not adequately track the significant high-risk vulnerabilities that have been identified in its systems. For example, in addition to our previous findings already cited in this report, in 2014 we reported that NESDIS was deferring the remediation of thousands of critical vulnerabilities for 2 years in the Joint Polar Satellite System ground system,<sup>14</sup> and that it also was not following its own vulnerability remediation processes for its other satellite ground systems, leaving thousands of high-risk vulnerabilities unremediated.<sup>15</sup> NOAA leadership needs

---

<sup>12</sup> DOC OIG, January 2010. *FY2009 FISMA Assessment of the Environmental Satellite Processing Center (NOAA5045)*, OAE-19730. Washington, DC: OIG, 10–11.

<sup>13</sup> As an example of the complexity of the ruleset, we found that following the attack NESDIS was able to reduce the firewall ruleset for Internet connections from over 3,100 rules down to a much simpler set of 154 rules.

<sup>14</sup> DOC OIG, August 21, 2014. *Expedited Efforts Needed to Remediate High-Risk Vulnerabilities in the Joint Polar Satellite System's Ground System—Final Memorandum*, OIG-14-027-M. Washington, DC: OIG, 2–3.

<sup>15</sup> DOC OIG, July 15, 2014. *Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission*, OIG-14-025-A. Washington, DC: OIG, 10–14.

to provide serious attention to these issues to reduce the risks of cyber attacks that could harm NOAA's ability to complete its missions and perform its critical functions.

### *Recommendations*

We recommend that NESDIS' Assistant Administrator do the following:

1. Improve risk management practices to reduce the exposure of web application vulnerabilities when decisions are made to not remediate known issues.
2. Formally review Internet exposed web applications and determine if access from the Internet is justified.
3. Deploy the specialized web application vulnerability scanning tool and an updated assessment process that requires more than one assessment tool; especially on web applications.
4. Ensure that all web applications are scanned for vulnerabilities on a quarterly basis.
5. Ensure that the same methodology used to identify a vulnerability is also used to validate its remediation.
6. Establish and implement procedures to periodically review firewall rules.
7. Develop an improved practice for managing POA&Ms to ensure that evidence showing actual remediation of a weakness identified in the POA&M is submitted, reviewed, and approved before the POA&M is closed.

We recommend that NOAA's Chief Information Officer do the following:

8. Ensure that adequate measures are taken to implement mechanisms for multifactor authentication in a timely manner for all applicable users and applications.



# Summary of Agency Response and OIG Comments

## NOAA Response

In response to our draft report, NOAA concurred with all recommendations and described both completed and planned actions to address each recommendation. NOAA also included suggested factual and technical changes to our findings, mainly related to the issue with multi-factor authentication on NESDIS HQ ITS LAN in finding III. NOAA's response is reproduced in its entirety in appendix B of this report.

## OIG Comments

While we made some modifications to our report based on NOAA's response—including clarification related to a web application within NESDIS HQ ITS LAN—we stand by our statement that multi-factor authentication was not fully implemented on NESDIS HQ ITS LAN system because not all NESDIS users who accessed HQ ITS LAN were authenticated through multi-factor authentication. Our finding III primarily illustrated that fully implementing multi-factor authentication could reduce the risk of unauthorized access to NOAA systems.

# Appendix A: Objectives, Scope, and Methodology

Our audit objectives were to (1) determine the significant factors that contributed to the successful cyber attack on NOAA's information systems, and (2) evaluate NOAA's handling of the detection, analysis, eradication, and reporting of the attack, as well as recovery from it. We limited the scope of our second objective to specifically focus on issues that prolonged the disruption of disseminating weather satellite data. We concentrated on these issues because they had the greatest impact to NESDIS operations. To accomplish our objectives, we

- reviewed NOAA's internal documents, email correspondence, presentations and memoranda related to the attack;
- reviewed the attack-related artifacts, including security testing results, firewall rules, and network logs;
- interviewed operating unit personnel, including system owners, meteorologists, IT security officers, IT administrators, and organizational directors and administrators; and
- reviewed vulnerability management documentation, including POA&Ms and vulnerability scans.

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

- The Federal Information Security Modernization Act of 2014
- IT Security Program Policy, U.S. Department of Commerce, introduced by the Chief Information Officer on September 12, 2014, 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:
  - 800-30, Rev. 1, *Guide for Conducting Risk Assessments*
  - 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - 800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy*
  - 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*
  - 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

- 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
- 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans*
- 800-115, *Technical Guide to Information Security Testing and Assessment*

We conducted our field work from January 2015 to December 2015. 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 based on our audit objectives.


# Appendix B: Agency Response



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

**AUG 12 2016**

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

FROM: Benjamin Friedman   
Deputy Under Secretary for Operations

SUBJECT: *National Oceanic and Atmospheric Administration : Successful  
Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT  
Security Program*  
Draft OIG Audit Report

Thank you for the opportunity to comment on the Office of the Inspector General's draft audit report evaluating the National Oceanic and Atmospheric Administration's information technology systems. We concur with all recommendations and our attached response describes both completed and planned actions to address each recommendation. We will continue our efforts to complete actions and work with the Department to close the recommendations.

If you have questions, please contact Mack Cato, Director, Audit, Internal Control and Information Management on (301) 628-0949.

Attachment



**Department of Commerce  
National Oceanic and Atmospheric Administration  
Comments to the OIG Draft Report Entitled  
“Successful Cyber Attack Highlights Longstanding Deficiencies in  
NOAA’s IT Security Program”  
(July 2016)**

**General Comments**

The National Oceanic and Atmospheric Administration (NOAA) appreciates the opportunity to review and comment on the Office of the Inspector General (OIG) draft report on NOAA’s information technology (IT) systems.

NOAA concurs with the findings and recommendations in the report. NOAA is committed to implementing cost-effective IT security controls to manage risk at an acceptable level and to ensure IT system components are resistant to attack and resilient if a defense fails. We acknowledge that additional protections are necessary for our legacy system components to keep pace with the ever-increasing number of software vulnerabilities and are deploying new and improved enterprise continuous monitoring tools and other countermeasures to protect these systems against the growing sophistication of attack techniques.

The response to each recommendation is provided below. NOAA recommends factual and technical changes to the report, which are provided below to ensure that the information presented is complete, accurate, and up-to-date.

**Recommended Changes for Factual/Technical Information**

*Page 1, 3rd paragraph:*

Please include the following additional information to clarify that the stolen credentials from the National Satellite Operations Facility (NSOF) Admin Local Area Network (LAN) did not allow the attacker to log in to the National Environmental Satellite, Data, and Information Service (NESDIS) Headquarters (HQ) LAN, but rather the access was limited to an internal LAN object only -- a website that is accessible by all of NESDIS by design (and therefore is accessible only by NESDIS users who have a NOAA Lightweight Directory Access Protocol (LDAP) account (UserID and password) for login).

*Page 2, 2nd paragraph:*

Please revise the statement “NOAA discovered...” to reflect that information system security personnel from the NESDIS Office of Satellite Products and Operations (OSPO) and NCEI/National Geophysical Data Center (NGDC) first discovered the event in September 2014. The OSPO personnel informed NOAA’s Computer Incident Response Team (N-CIRT) via the incident reporting system after users complained about access problems to the website and log files had shown compromised accounts on the website. Similarly, with respect to the NGDC event, an NCEI system administrator detected the compromise and created an incident report to inform NOAA. Upon receipt of these incident reports, N-CIRT then initiated an investigation that identified suspicious traffic, which triggered the action to install Mandiant Intelligent Response (MIR) agents on components of affected systems.

*Bottom of page 2 - last paragraph:*

Please revise the statement “But, according to NCEP [National Centers for Environmental Prediction] officials,...” to articulate the possible effect in a less speculative tone. A suggested revision is “But, according to NCEP [National Centers for Environmental Prediction] officials, extended periods of data loss could have a possible impact on the models over time, leading to a degradation of weather forecasting that could in turn affect the accuracy of predicting severe weather events in the future.”

*Section I, sentence starting at bottom of page 3 to top of page 4:*

Please clarify the sentence “... attackers exploiting unauthorized information systems...” to reflect that no “unauthorized” systems were attacked. The full text of the National Institutes for Standards and Technology (NIST) threat event scenario cited by the OIG in the draft report states “poorly configured *or* unauthorized” (emphasis added on “or”) system components. We request to replace “unauthorized” in this sentence to “poorly configured” for accuracy.

*Page 4 last paragraph:*

Please revise the statement, “In addition, failure to run a web application assessment on the NSOF Admin LAN application—previously mentioned in finding one—led to a false sense of security,” to reflect this is a possible effect rather than a conclusion of fact. Suggested revision is “In addition, failure to run a web application assessment on the NSOF Admin LAN application—previously mentioned in finding one—led to a possibly impaired assessment of risk due to incomplete vulnerability information.”

*Page 5, Section III, 1st paragraph:*

Please include the following additional information to clarify that the stolen credentials from the NSOF Admin LAN did not allow the attacker to log in to the NESDIS HQ LAN, but rather the access was limited to an internal LAN object only -- a website that is accessible by all of NESDIS by design (and therefore is accessible only by NESDIS users who have a NOAA LDAP account (UserID and password) for login).

*Page 5, Section III, 1st paragraph:*

Please include additional information with regard to the NESDIS HQ ITS LAN in reference to “these systems” in the statements “...because multifactor authentication was not fully implemented for these systems. Although multi-factor authentication was required for these systems and known to not be in place...”. All NESDIS HQ ITS LAN users at the time of the incident were and still are required to, and do, log in to the network and to local privileged accounts using Common Access Card (CAC) Homeland Security Presidential Directive 12 (HSPD-12) authentication. Please also specify in the report the source/policy for the requirement to implement multifactor authentication for access by users already on the internal network to internal objects on the network such as website applications.

*Page 6, Section III, 1st paragraph on page 6:*

Please consider the following information to clarify the use of “these systems” with respect to the HQ ITS LAN in the statements “...we found that NOAA did not fully implement this control for the three systems where the attacker obtained unauthorized access: the HQ ITS LAN, ... NOAA either accepted the risks associated with not fully implementing this control or deferred



full implementation of this control for these systems. As a result, multifactor authentication was not in place for these systems when the attack occurred.” We ask that mention of the NESDIS HQ ITS LAN be removed from this finding because it had implemented multi-factor authentication as required by HSPD-12 at the time of the incident and all NESDIS HQ LAN network users at the time of the incident were and still are required to, and do, login to the LAN using CAC authentication. Monthly Balanced Scorecard Metrics for Strong Authentication submitted to NOAA show that NESDIS HQ ITS LAN reported 100% implementation for Privileged, Unprivileged, and Remote network users as of the report dated September 30, 2014. NESDIS also reported that the system was compliant in the data call response submitted to OIG for this audit on September 18, 2015.

*Page 6, Section III, 2nd paragraph on page 6:*

Please include in the report that the data exfiltrated from the NESDIS HQ ITS LAN was not sensitive. In our response to a data call submitted to OIG for this audit on March 24, 2016, we noted that “As listed in the embedded spreadsheet ..., none of the documents are considered sensitive FOUO [For Official Use Only] or SBU [Sensitive but Unclassified]; therefore, NESDIS considers these documents as “Public”.”

#### **Editorial Comments**

We have no editorial comments.

#### **NOAA Response to OIG Recommendations**

**Recommendation 1:** “We recommend that NESDIS’ Assistant Administrator improve risk management practices to reduce the exposure of web application vulnerabilities when decisions are made to not remediate known issues.”

**NOAA Response:** We concur. We will ensure that requests for exceptions to flaw remediation requirements require identification of the host as internal or public-facing, that Authorizing Officials take this information into consideration when deciding whether to accept the risk to not remediate vulnerabilities. Notably, to improve the security posture of these components, the NESDIS Enterprise Security Remediation Advancement (ESRA) Program was established specifically to address systemic enterprise weaknesses contributing to the October 2014 incident including implementation of modernized IT solutions and secure re-coding of vulnerable web applications.

**Recommendation 2:** “We recommend that NESDIS’ Assistant Administrator formally review Internet exposed web applications and determine if access from the Internet is justified.”

**NOAA Response:** We concur. As part of the annually required DOC data call for public-facing web site inventories and certification (online at [http://www.osec.doc.gov/webresources/policies/policy8\\_annual\\_website\\_certifications.html](http://www.osec.doc.gov/webresources/policies/policy8_annual_website_certifications.html)), NESDIS will conduct and document a formal review of its web sites for proper justification. The NOAA Web Committee is drafting a similar policy for an annual Web Asset Certification and Inventory (WACI).

**Recommendation 3:** “We recommend that NESDIS’ Assistant Administrator deploy the specialized web application vulnerability scanning tool and an updated assessment process that requires more than one assessment tool; especially on web applications.”

**NOAA Response:** We concur. NESDIS and OCIO will coordinate the use of the WebInspect scanning services in addition to configuring the Nessus vulnerability scanning of web sites for web application vulnerabilities. In addition, to identify and remediate web application vulnerabilities before they become costly to fix, NOAA will identify local level tools for proactive detection of vulnerabilities during code development. It should be noted that the sophistication of some of the tools such as WebInspect require specialized expertise to administer, so NOAA will provide specialized training and tools to fill this gap.

**Recommendation 4:** “We recommend that NESDIS’ Assistant Administrator ensure that all web applications are scanned for vulnerabilities on a quarterly basis.”

**NOAA Response:** We concur. NESDIS will comply with the recently issued NOAA IT Security Manual v5.6 requirement that “all NOAA website applications must be scanned for vulnerabilities at least every 90 days (every 30 days for any websites within FISMA high impact systems).” In addition, to identify and remediate web application vulnerabilities before they become costly to fix, NOAA will identify feasible local level tools for proactive detection of vulnerabilities during code development.

**Recommendation 5:** “We recommend that NESDIS’ Assistant Administrator ensure that the same methodology used to identify a vulnerability is also used to validate its remediation.”

**NOAA Response:** We concur. NESDIS procedures for Plan of Action and Milestones (POA&M) Management require assessment of POA&Ms using the same NIST SP 800-53A procedures that were used in weakness discovery. We currently require our independent security controls assessors to perform pre-closure reviews of high-risk POA&Ms for high-impact systems while all other POA&Ms are reviewed for closure by the system personnel and then independently reviewed post-closure as part of the next annual assessment. We will consider updating procedures to require pre-closure independent review of all POA&Ms.

**Recommendation 6:** “We recommend that NESDIS’ Assistant Administrator establish and implement procedures to periodically review firewall rules.”

**NOAA Response:** We concur. While rulesets are reviewed as part of the annual security controls assessment procedures, NOAA will implement procedures to require system personnel to review the rulesets at least annually or upon processing a configuration change request that affects the ruleset.

**Recommendation 7:** “We recommend that NESDIS’ Assistant Administrator develop an improved practice for managing POA&Ms to ensure that evidence showing actual remediation of a weakness identified in the POA&M is submitted, reviewed, and approved before the POA&M is closed.”

**NOAA Response:** We concur. NESDIS procedures for POA&M Management require adequate POA&M closure evidence using the NIST SP 800-53A procedures. We currently require our independent security controls assessors to perform pre-closure reviews of evidence for closure of high-impact system high-risk POA&Ms. Evidence for closure of all other POA&Ms are reviewed for closure by the system personnel and then independently reviewed post-closure as part of the next annual assessment. In conjunction with our response to recommendation 5, we will consider updating the procedures to require pre-closure independent review of all POA&M evidence for adequacy.

**Recommendation 8:** “We recommend that NOAA’s Chief Information Officer ensure that adequate measures are taken to implement mechanisms for multi-factor authentication in a timely manner for all applicable users and applications.”

**NOAA Response:** NOAA concurs, and is continuing its implementation of its multi-factor authentication program. NOAA Office of the Chief Information Officer (OCIO) has put in place the Identity Credential Access Management Program (ICAM), which provides enterprise-wide services for two-factor authentication. It is currently in production and has already been adopted by many of NOAA’s line offices. The goal is to get 100% of privileged users and as close to 100% of users on ICAM as soon as possible, given available resources.

The program provides the following core capabilities:

- Identity: authoritative data source to uniquely identify all NOAA Personnel.
- Credential: HSPD-12 vetted smart card such as CAC, Alt Token to support 2FA.
- Access Manager: engine to provide authentication for NOAA Applications. Fully supports 2FA.
- Federation: Capability to work with other Government agencies to share vetted identities and trusts between NOAA systems.

NOAA OCIO is working closely with its line offices on the modernization requirements necessary on furthering the implementation for standardized multi-factor authentication solutions for all non-compliant systems.

01120000203