UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

August 21, 2014

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: Expedited Efforts Needed to Remediate High-Risk Vulnerabilities in the Joint Polar Satellite System's Ground System—Final Memorandum

In accordance with the Federal Information Security Management Act of 2002 (FISMA), we conducted an audit of NOAA's information technology (IT) security program and have issued a final report.[1] While conducting this audit, we identified significant security concerns related to the Joint Polar Satellite System (JPSS) ground system that justified special and separate attention. We worked with NOAA to fully understand these concerns and their impact—and discussed immediate actions management could take to remediate them. NOAA has commenced some of these actions. The purpose of this memorandum is to provide our findings and recommendations specific to this system.

Background

The JPSS ground system is a high-impact IT system[2] that supports NOAA's mission by gathering and routing data from several polar-orbiting weather satellites and disseminating it to users worldwide.[3] This system also provides command, control, and data processing for the Suomi National Polar-orbiting Partnership (Suomi NPP) weather satellite[4] and in the future will provide similar functions for other planned satellites. In a partnership with NOAA, the National Aeronautics and Space Administration (NASA) manages the contract for the JPSS ground system.

---

[1] U.S. Department of Commerce, Office of Inspector General, July 15, 2014. *Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission,* OIG-14-025-A. Washington, DC: Commerce OIG.

[2] *High-impact systems* are categorized as those systems for which the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic effect on organizational operations, organizational assets, or individuals.

[3] JPSS is the nation's next-generation polar-orbiting operational environmental satellite system. It provides continuity of critical, global Earth observations—including oceans, clouds, ozone, snow, ice, vegetation, and atmosphere.

[4] Suomi NPP, the first next-generation polar-orbiting satellite, was launched in 2011.

NOAA repurposed the JPSS ground system from its original role of supporting a research and prototyping project under the National Polar-orbiting Operational Environmental Satellite System (NPOESS)[5] to one that supports operational satellites for the JPSS program. This was done due to delays with the NPOESS program. Thus, the ground system now in place was not originally intended to support operational satellites nor was it designed to meet Department of Commerce IT security requirements.[6] In 2010, NOAA began to modify the ground system to support the newly established JPSS program but, until January 2014, the program did not require the ground system contractor to begin full implementation of the majority of the security controls for the system. As a result, few security controls are fully implemented and many high-risk vulnerabilities exist within the system. Specifically,

- The JPSS program's security assessments for fiscal years (FYs) 2012 and 2013 found that only about a quarter of the Department's required National Institute of Standards and Technology (NIST) security controls had been fully implemented.

- Our analysis of the JPSS program's assessments of system vulnerabilities found that, since FY 2012, the number of high-risk vulnerabilities in the system had increased by two-thirds[7] despite recent efforts the program has taken to remediate these vulnerabilities (see figure 1). Vulnerabilities are defined as high-risk if they are relatively easy for attackers to exploit and gain control over system components. If exploited, these vulnerabilities may make it possible for attackers to significantly disrupt the JPSS mission of providing critical data used in weather forecasting and climate monitoring. Software used by the JPSS system contains vulnerabilities that have been publicly known for several years. Software tools to exploit several of these vulnerabilities are available on the Internet.

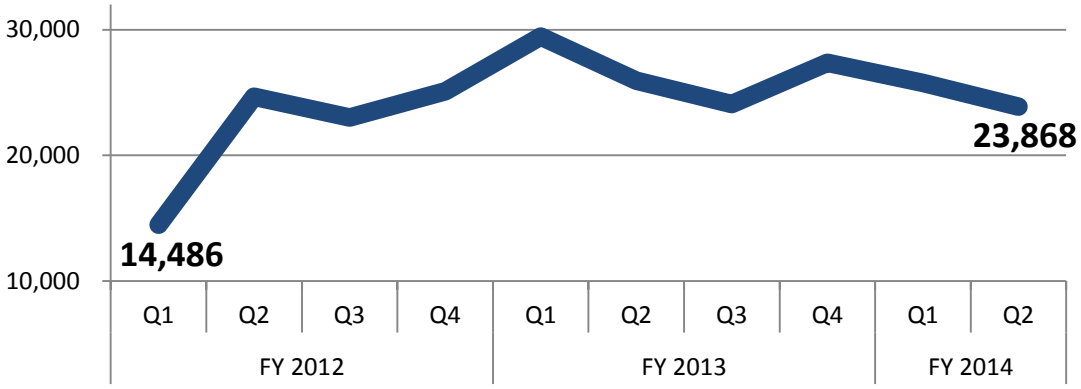
NOAA is responsible for ensuring that its IT systems have an appropriate operational security posture, which includes timely remediation of high-risk vulnerabilities in the JPSS ground system. While the program has begun implementing plans to make the necessary changes that will correct the JPSS ground system's numerous IT security weaknesses and vulnerabilities, the majority of these issues will not be remediated for another 2 years.

[5] The National Polar-orbiting Operational Environmental Satellite System (NPOESS) was created in 1994. In 2010, a portion of it was restructured as the JPSS program. The ground system supported the NPOESS Preparatory Project (NPP), which was intended to demonstrate new instruments.

[6] The NPOESS was a tri-agency program including NOAA, NASA, and the Department of Defense. The ground system was built to meet Department of Defense security requirements.

[7] The number of vulnerabilities in a system may increase because new vulnerabilities in software used by the JPSS program are constantly being uncovered and publicly reported (e.g., by software vendors, security researchers). Additionally, changes made to the existing system (for example, installing new software or operating systems) may introduce new vulnerabilities if IT security protections are not fully integrated with the changes.

Figure 1. Number of High-Risk Vulnerability Instances in the JPSS Ground System, by Quarter, FY 2012 to FY 2014 2nd Quarter



Source: JPSS Quarterly Ground System Vulnerability Assessment Analysis Reports FYs 2012–2014

Objectives, Findings, and Recommendations

The objective of our audit was to assess the effectiveness of NOAA's IT security program by determining whether key security measures adequately protect NOAA's systems. (For detailed objectives, scope, and methodology please see appendix A.) We found that the JPSS program needs to expedite its efforts to reduce the current IT security-related risks to its ability to support critical weather forecasting operations and improve the overall security posture of JPSS' ground system.

I. Expedite Remediation of High-Risk Vulnerabilities

Although full implementation of many of the missing and partially implemented security controls requires the significant changes that are planned for the next iteration of this system, there are steps the program can take now to improve its security posture. We found that there are numerous high-risk vulnerabilities that we believe can be corrected with only minor alterations to the existing system. In the past, these have taken a year or more to remediate, because the JPSS program has seldom used the expedited processes it has developed to deploy high-risk security fixes and did not direct the contractor responsible for the ground system to use these processes to remediate vulnerabilities in a timely manner.

A. Many High-Risk Vulnerabilities Are Remediable with Minor Alterations to the Existing System

We examined the JPSS ground system's vulnerabilities that were identified by the program and believe that there are high-risk vulnerabilities that could be remediated by making minor alterations to the existing system. These include:

- More than 9,100 instances of high-risk vulnerabilities identified by vulnerability scans, including (a) out-of-date software versions or missing security patches, (b) insecurely configured software, and (c) unnecessary user privileges within the operating systems and software.

- More than 3,600 instances where password and auditing settings need to be configured in accordance with JPSS policy.

- Unnecessary software applications that need to be removed or disabled.

- Three outstanding vulnerabilities identified by penetration testing conducted in June 2012.

We believe remediating these vulnerabilities should require only minor alterations to the existing system because they include simple actions, such as deploying missing security patches and updates that are compatible with the existing system and are available from vendors; correcting minor misconfigurations in applications or operating systems; or removing unneeded applications.

B. Remediation of Vulnerabilities Has Been Slow

The JPSS security policy for the ground system requires remediation of high-risk vulnerabilities within 30 days of identification and remediation on a quarterly basis for moderate- to low-risk flaws. However, it took the JPSS program 11 to 14 months to remediate high-risk vulnerabilities it identified in the ground system. We found that

- The vulnerabilities the program determined it could fix that were identified from penetration testing in June 2012 were not remediated until September 2013.

- Most of the vulnerabilities resulted from flaws in software that was running within the system. However, the time between deployments of software updates and security patches to remediate these flaws varied from 11 to 14 months during the period 2011 to 2013, meaning that remediation activities only occurred about once a year.

Remediating vulnerabilities at such intervals is not sufficient to keep up with the rapid growth in the number of vulnerabilities found in the system (see figure 1). For the last 2 years, the JPSS program had planned to address system vulnerabilities by means of two maintenance releases per year. Not only did this fall significantly short of the system's requirement for patching high-risk vulnerabilities within 30 days but, of the two maintenance releases scheduled each year, only one was actually performed. According to JPSS management, since 2011 maintenance releases to the system were suspended for 344 days to allow for the evaluation of contractor performance and conducting important operational events, such as preparation for the launch of the Suomi NPP satellite and subsequent on-orbit testing.

The remediation of high-risk vulnerabilities is critical to the continued success of the JPSS mission and should have a high priority. The more high-risk vulnerabilities that exist in the system, the higher the probability is that an attacker could compromise it. This could lead to a disruption of NOAA's ability to command and control the Suomi NPP satellite and to provide data that is used in numerical weather models that support weather predictions and climate monitoring. The importance of remediating these vulnerabilities justifies addressing them outside the regular cycle of maintenance deployments.

Processes for deploying urgent updates are in place. Using these processes would have made it possible for the JPSS program to correct many high-risk vulnerabilities in an expedited manner. Also, the vulnerability management plan for the ground system includes monitoring and prioritization of vulnerabilities by the ground system's Patch and Vulnerability Group (PVG), which is a group of system and IT security experts within the JPSS program. Since June 2012, the PVG repeatedly recommended that high-risk vulnerabilities be corrected immediately. However, the JPSS program only used the urgent update processes once during this time period, to remediate one vulnerability.

Urgent updates to the JPSS ground system were not performed because the program did not require that the ground system contractor remediate vulnerabilities in a timely manner. The contractor was required to remediate vulnerabilities identified by the JPSS program in its plans of action and milestones (POA&Ms)—a management tool used to identify, assess, prioritize, and monitor efforts to correct IT security vulnerabilities—but the POA&Ms created by the JPSS program allowed 8–13 months for correction of high-risk vulnerabilities. Thus, the JPSS program did not effectively use its POA&Ms to ensure that high-risk vulnerabilities were remediated in a timely manner.

While the fieldwork for this audit was being conducted, the JPSS program began implementation of a plan that would deploy fixes to correct vulnerabilities quarterly instead of semiannually, by adding two deployments to the two already planned each year. But even if the JPSS program is able to successfully deploy fixes quarterly, there will still be gaps of potentially up to 3 months before some high-risk vulnerabilities can be addressed.

Conclusions

It is essential that the JPSS program's existing urgent update processes be used to correct high-risk vulnerabilities in the ground system's critical components.[8] We believe that the types of high-risk vulnerabilities we have identified in finding I(a) of this memorandum can be fixed in an expedited manner and should be addressed as soon as possible. Although these measures will not address all vulnerabilities, we believe that they will improve protection of the current JPSS ground system until NOAA deploys the next iteration of its ground system. Considering that the current system's security

[8] JPSS ground system critical components include those that are associated with command, control, and communication of the satellite and that process data used in numeric weather models and forecast offices in Alaska.

posture was at a disadvantage from the outset—having not incorporated security into its development when it was transitioned into the JPSS—the program needs to ensure that the security measures planned for the next iteration of the ground system are included from the beginning and not added later or deferred.

Recommendations

To reduce the risks of compromise to the JPSS ground system, we recommend that the NOAA Assistant Administrator for Satellite and Information Services and NOAA's Chief Information Officer ensure that

1. The JPSS program review the types of vulnerabilities identified in finding 1(a) of this memorandum and, where possible, correct them as soon as feasible.

2. Urgent system update processes are used to deploy high-risk security-related software patches and updates, based on the criticality of the patches and the system components affected.

3. POA&Ms require that newly discovered, high-risk, JPSS vulnerabilities be remediated within 3 months.

We have summarized your agency's response in this memorandum and included the formal response as appendix B. The final memorandum will appear on the OIG 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 memorandum, 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
Mark Paese, Acting Assistant Administrator for Satellite and Information Services, NOAA
Zachary Goldstein, Acting Chief Information Officer, NOAA
Mike Maraya, Acting Director, Office of Cyber Security, and Chief Information Security Officer
Harry Cikanek, Director, JPSS Program, NOAA
Lawrence Reed, Director, Cyber Security Division, NOAA
Irene Parker, Acting Assistant Chief Information Officer, Satellite and Information Service, NOAA
Brian Doss, Audit Liaison, NOAA
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer

Summary of Agency Response and OIG Comments

NOAA Response

In response to our draft memorandum, NOAA concurred with our recommendations. NOAA indicated that it had already implemented recommendation 2, explaining that it remediated the Heartbleed vulnerability[9] during the third quarter of FY 2014. NOAA also requested deletion of the following sentence on page 5, paragraph 3, "Using these processes would have made it possible for the JPSS program to correct high-risk vulnerabilities in an expedited manner." NOAA requested this deletion to reflect remediation of Heartbleed in an accelerated manner. NOAA's complete formal response is included as appendix B.

OIG Comments

In preparing this final report, we thoroughly considered NOAA's formal comments and informal comments made in discussions and other communications subsequent to the issuance of our draft report.

With regard to NOAA's response concerning recommendation 2, remediating the Heartbleed vulnerability in an expedited manner is a step in the right direction, however numerous vulnerabilities remain. Going forward, we encourage NOAA, as it corrects the existing and future vulnerabilities within the JPSS ground system, to fully implement this recommendation.

In regard to NOAA's request in its response for removal of our sentence on page 5 paragraph 3, NOAA's assertion that it remediated the Heartbleed vulnerability does not change the fact that the JPSS program could have remediated many high-risk vulnerabilities using its urgent update processes, especially those recommended by its PVG group for immediate correction. As noted in our memorandum, these processes were seldom used. We have added the word "many" to this sentence to avoid misinterpretation that the JPSS program has not remediated any vulnerabilities using urgent update processes.

[9] Heartbleed is a vulnerability in commonly used versions of open-source cryptographic software that received widespread media attention in April 2014 because it could allow attackers to expose sensitive data.

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. In contribution to this objective, we reviewed the implemented security controls and known vulnerabilities of the JPSS ground system. To do so, we

- Reviewed the system-related artifacts since FY 2011, including risk, vulnerability, and security control assessments; policy and procedures; planning documents; and other material related to the current security posture of the ground system, and

- Interviewed operating unit personnel including IT security officers and organizational directors.

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

    - 800-53A Rev 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans

We conducted our field work on the JPSS ground system portion of our FISMA audit of the NOAA IT security program from October 2013 to May 2014. 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: Agency Response

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

JUL 25 2014

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

FROM: Vice Admiral Michael S. Devany

SUBJECT: Expedited Efforts Needed to Remediate High-Risk Vulnerabilities in the Joint Polar Satellite System's Ground System Draft OIG Memorandum

Thank you for the opportunity to comment on the Office of the Inspector General's draft memorandum report regarding security concerns with the Joint Polar Satellite System (JPSS) ground system. 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 requirements, and to manage IT security risk in a challenging fiscal climate.

We concur with all recommendations and are taking actions to address the issues identified. 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
"Expedited Efforts Needed to Remediate High-Risk Vulnerabilities in the Joint Polar Satellite System's Ground System"
(Draft Memorandum)

General Comments

We appreciate the effort that the Office of the Inspector General (OIG) team has put forth on this audit for the Block 1.2 operational configuration of the Joint Polar Satellite System (JPSS) ground system. The JPSS Ground Project over the last several years has been focused on sustaining the existing ground system to support the on flight assets of Suomi National Polar Partnership (SNPP) and service delivery for our partner Government Agencies and international polar orbiting missions.

We believe that completely deploying the Block 2.0 configuration and decommissioning Block 1.2 will significantly improve our security posture over the next two years. As part of this strategy we are seeking early opportunity to retire obsolete components that do not directly support the product generation, service delivery, command, control and configuration aspects of the system.

Recommended Changes for Factual/Technical Information

Page 5, Paragraph 3 "Using these processes would have made it possible for the JPSS program to correct high-risk vulnerabilities in an expedited manner."

Requested Change: Request deletion of this statement or revise to reflect that JPSS successfully used expedited processes to enable remediation of Heartbleed in an accelerated manner within FY14Q3. Beyond processes, additional computing resources and labor would be also be necessary to maintain more rapid patching cycles. Competing operational needs necessitate prioritizing security improvements along with other pressing matters.

Editorial Comments

None.

NOAA Response to OIG Recommendations

Recommendation 1: "To reduce the risks of compromise to the JPSS ground system, we recommend that the NOAA Assistant Administrator for Satellite and Information Services and NOAA's Chief Information Officer ensure that the JPSS program review the types of vulnerabilities identified in finding 1(a) of this memorandum and, where possible, correct them as soon as feasible."

NOAA Response: We concur with the recommendation.

Recommendation 2: "To reduce the risks of compromise to the JPSS ground system, we recommend that the NOAA Assistant Administrator for Satellite and Information Services and NOAA's Chief Information Officer ensure that urgent system update processes are used to deploy high-risk security-related software patches and updates, based on the criticality of the patches and the system components affected."

NOAA Response: We concur with the recommendation and in fact we are already doing this, for example, with regard to remediation of the Heartbleed vulnerability in FY2014 Quarter 3.

Recommendation 3: "To reduce the risks of compromise to the JPSS ground system, we recommend that the NOAA Assistant Administrator for Satellite and Information Services and NOAA's Chief Information Officer ensure that POA&Ms require that newly discovered, high-risk, JPSS vulnerabilities be remediated within 3 months."

NOAA Response: We concur with the recommendation. The current required remediation frequency for remediating newly discovered JPSS high-risk vulnerabilities is 30 days. Existing high-risk vulnerabilities will be remediated in accordance with approved POA&M remediation dates as tracked in the Cyber Security Assessment and Management system.