National Aeronautics and Space Administration

OFFICE OF INSPECTOR GENERAL

Security of NASA's Publicly Accessible Web Applications

OFFICE OF AUDITS

AUDIT REPORT
JULY 10, 2014

IG-14-023

(A-13-018-00)

Final report released by:

Paul K. Martin
Inspector General

Acronyms

FY	Fiscal Year
ID	Identifier
IP	Internet Protocol
IT	Information Technology
IPAM	Internet Protocol Asset Management
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
SQL	Structured Language Query
URI	Uniform Resource Indicator
WASP	Web Application Security Program

OVERVIEW

SECURITY OF NASA'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

The Issue

NASA manages approximately 1,200 publicly accessible web applications – or about half of all publicly accessible non-military Federal Government websites – to share scientific information with the public, collaborate with research partners, and provide Agency civil servant and contractor employees with remote access to NASA networks. Hundreds of these web applications are part of information technology (IT) systems NASA characterizes as high- or moderate-impact, meaning that a security breach could result in the loss of sensitive data or seriously impair Agency operations. NASA's publicly accessible web applications consist mainly of websites, but also include web-based login portals and administrative systems that provide authorized personnel remote access to Agency IT resources.

NASA is a regular target of cyber attacks both because of the large size of Agency networks and because those networks contain technical and other sensitive information highly sought after by criminals. The Agency's substantial connectivity with outside organizations – in particular nongovernmental educational institutions and research facilities – presents cybercriminals with a larger target than most other Government agencies. In fiscal year (FY) 2013, NASA reported that exploitation of vulnerable web applications accounted for one-third (61 of 183) of the Agency's total IT security breaches, with several resulting in the loss of sensitive information and disruption to Agency operations. For example, in July 2013, hackers compromised a NASA Shared Services Center website containing personally identifiable information of Agency civil servants and contractors. Further, several NASA websites hosted by the Ames Research Center had to be taken offline in September 2013 after an international hacker posted political statements opposing U.S. policy.

The frequency and sophistication of attacks directed at NASA's publicly accessible web applications has increased dramatically over the past several years. For example, between FYs 2012 and 2013, NASA experienced an 850 percent increase (from 42 to 359) in structured query language (SQL) injection attacks that attempted to compromise Agency web applications to steal data or gain a foothold into its networks for future exploitations.[1]

[1] SQL is an industry standard computer language used to query, operate, and administer many databases, including Microsoft and Oracle databases. In a SQL injection attack, the attacker appends (injects) instructions onto the end of a valid SQL statement in an attempt to gain unauthorized access to the system and its data.

In response to this growing cyber threat and a prior NASA Office of Inspector General recommendation, NASA established an Agency-wide initiative in 2012 – the Web Application Security Program (WASP) – to identify and assess vulnerabilities on all of its publicly accessible web applications and mitigate the most severe vulnerabilities before hackers exploit them.[2] Reducing the Agency's extensive web "footprint" is one of the more effective ways NASA can counter the threat of cyber attacks on its publicly accessible web applications. To this end, the Office of the Chief Information Officer (OCIO) and NASA Center IT security officials are working to reduce NASA's web presence by eliminating unused and duplicative web applications and moving Agency websites to a public cloud-computing environment.[3]

Results

NASA's ongoing efforts to reduce its web presence and to identify and scan for vulnerabilities on its publicly accessible web applications have improved Agency IT security. However, NASA needs to close remaining security gaps, strengthen program oversight, and further reduce the number of publicly accessible web applications. We found that WASP developed a complete inventory of all publically available web applications maintained by NASA Headquarters and Centers and, consistent with best practices, identified vulnerabilities through automated scanning coupled with manual testing. In addition, during the 15-month period ending March 2014, NASA reduced by 15 percent (from 1,500 to 1,200) the number of its publicly accessible web applications. Despite this progress, we found deficiencies in WASP's design and implementation that leaves NASA's publicly accessible web applications at risk of compromise. These deficiencies occurred because WASP did not prioritize identification of security vulnerabilities by seriousness of potential impact, identify the underlying cause of vulnerabilities, identify weaknesses associated with unsound IT security practices, or implement an effective process to ensure timely mitigation of identified vulnerabilities. Finally, while NASA has made strides in reducing the scope of its web presence, the Agency's remaining 1,200 publicly accessible web applications continue to present a large target for hackers.

Vulnerability Discovery Not Prioritized by System Impact Level. Effectively managing risk dictates NASA identify and address vulnerabilities in high- and moderate-impact systems before those in other systems.[4] Experience has shown that detecting vulnerabilities in web applications requires a combination of automated and manual testing, with WASP identifying 90 percent of the vulnerabilities in NASA

[2] NASA OIG, "Inadequate Security Practices Expose Key NASA Network to Cyber Attack" (IG-11-17, March 28, 2011).

[3] A public cloud-computing provider is a third-party IT service provider (e.g., Amazon) that delivers services, such as website hosting or data storage, to consumers over the Internet.

[4] According to the National Institute of Standards and Technology, the loss of confidentiality, integrity, or availability in a moderate-impact system could have serious adverse effects on an organization's operations, assets, or individuals, while in a high-impact system, such a loss could have severe or catastrophic effects.

systems from manual testing and only 10 percent from automated scanning. Because manual testing requires a significant amount of time and resources, efficient use of such testing requires focusing on high- and moderate-impact systems before examining low-impact systems.

We found that WASP has not mapped NASA's web applications back to their information systems using the Agency's security categorization data to determine their security impact level. Accordingly, WASP is unable to prioritize manual scanning by risk level, which increases the risk that vulnerabilities in critical publicly accessible web applications may go undetected and unmitigated.

WASP did not Address Root Cause of Vulnerabilities. Identifying and addressing the root cause of a system's security weaknesses helps prevent vulnerabilities from recurring and is a recognized best practice in IT security. We noted that WASP identified a repeating pattern of high-severity vulnerabilities associated with certain publicly accessible web applications that allowed NASA personnel to access Agency systems and network resources remotely. For security purposes, since 2008 NASA policy has required public websites originating from the Agency be registered, approved, and tested for vulnerabilities before deployment. However, this policy does not apply to other types of web applications, such as login portals and management consoles. In our judgment, the root cause of the recurring vulnerabilities associated with these other types of web applications is a control deficiency that allowed them to be deployed without undergoing the type of oversight and testing required for NASA's public websites.

WASP did not Identify Weaknesses Associated with Unsound IT Security Practices. Hackers target publicly accessible web applications that are under development or in the testing phase because such applications often lack security controls common to production applications. We reviewed the uniform resource indicators associated with NASA's publicly accessible web applications and identified 15 web applications that were under development or in testing.[5] Two of the 15 were preproduction versions of a moderate-impact Agency-wide system used to manage IT system access privileges and credentials that contained usernames and passwords for more than 55,000 NASA civil servant and contractor employees. A remote attacker who accessed these applications could have extracted thousands of user identifiers (ID) and, using an automated tool to guess the corresponding passwords, attempt to log into NASA systems. In FY 2013, such "brute force" attacks accounted for 6 percent (11 of 183) of NASA's total system breaches.

Allowing Internet access to preproduction Agency web applications is a significant security deficiency. WASP did not detect this weakness because it focused too narrowly on finding technical vulnerabilities and overlooked weaknesses related to unsound IT security practices.

[5] Uniform resource indicator – also referred to as uniform resource locator (URL) – is a string of characters used to identify a web resource. For example, www.nasa.gov is the URL for NASA's public website. Typically, web-based applications under development or in the test phase have a URL that contains strings such as ".dev," ".test," or ".tst."

Untimely Mitigation of Vulnerabilities Puts NASA's Publicly Accessible Web Applications at Risk of Compromise. Prompt mitigation of vulnerabilities in NASA's publicly accessible web applications is essential to ensuring the confidentiality, integrity, and availability of Agency systems and data. Accordingly, NASA policy requires all critical and high-severity vulnerabilities be mitigated within 10 days of discovery.

We reviewed the status of web application vulnerabilities in the Agency's information system and found that as of January 2014, 93 percent (26 of 28) of confirmed critical and high-severity vulnerabilities remained unmitigated 6 months after notification to the affected Center. We determined this occurred because OCIO staff did not have access to the Agency's vulnerability tracking system to check the status of outstanding vulnerabilities and follow up, as necessary, with the responsible NASA organization. According to OCIO officials, a lack of resources has prevented them from monitoring the real-time status of these vulnerabilities. Moreover, Center IT staff told us they could not determine the status of their Center's vulnerabilities because they did not have access to the vulnerability tracking system. Finally, we found that WASP generally used a 45-day rather than the NASA-mandated 10-day timeframe to validate whether critical and high-severity vulnerabilities had been mitigated.

Management Action

NASA's websites and publicly accessible web applications are under constant attack by hackers, and the frequency and sophistication of these cyber attacks is increasing. Thus, it is imperative that NASA find and mitigate vulnerabilities in Agency web applications before hackers exploit them. In addition, NASA should identify the root cause of security weaknesses to prevent vulnerabilities from recurring and improve oversight of WASP to ensure identified deficiencies are addressed promptly. Finally, while NASA has made progress by reducing its web presence by more than 300 applications, the 1,200 remaining publicly accessible web applications provide multiple potential entry points for remote attackers to gain unauthorized access to Agency systems and data. Accordingly, we recommend that the Agency Chief Information Officer (CIO) ensure vulnerability discovery and mitigation are prioritized by system impact level, require all publicly accessible web applications be registered and scanned for vulnerabilities before deployment, require Centers to remove or secure publicly accessible applications under development or testing, and implement an oversight process to ensure that all critical and high-severity vulnerabilities are mitigated within 10 days of discovery.

In response to a draft of this report, NASA's CIO concurred with our recommendations and proposed actions to improve the security of NASA's publicly accessible web applications. We consider the CIO's planned actions responsive and will close the recommendations upon verification that the Agency has completed them. We also reviewed management's comments for technical accuracy and report sensitivity and incorporated those as appropriate. Management's full response to the draft report is reprinted in Appendix B.

CONTENTS

INTRODUCTION

RESULTS

APPENDIX A

APPENDIX B

APPENDIX C

INTRODUCTION

Background

The Internet has grown over the past 15 years from a simple collection of static websites to a vast conglomeration of sophisticated web applications that include websites, administrative consoles, and web login portals.[6] Many of these web applications are publicly accessible, which means that anyone with an Internet connection can access them. Hackers routinely exploit vulnerabilities in these applications to gain unauthorized access to computer networks in order to steal sensitive information and data, disrupt operations, or attain public notoriety. In 2011, one information technology (IT) advisory firm estimated that more than 70 percent of all cyber attacks target vulnerabilities in an organization's publicly accessible web applications.[7] Moreover, hackers can use a minor flaw in a web application as an entryway to an organization's entire network.

NASA has a significant Internet presence with approximately 1,200 publicly accessible web applications – a total that represents about half of all non-military Federal Government websites. Through its websites, the Agency shares information on its aeronautics, science, and space programs with the public and research community. For example, the Landsat mission – a program that began in the 1970s to gather satellite imagery of the Earth – maintains a website containing publicly available data on water quality, glacier recession, sea ice movement, invasive species encroachment, coral reef health, land use change, deforestation rates, and population growth. In addition, NASA has numerous administrative consoles and web login portals that enable Agency civil servants and contractors to access data and services remotely through a single point of entry from any computer or mobile device at virtually any location anywhere in the world.

NASA is a regular target of cyber attacks both because of the large size of its networks and because of the sensitive nature of the information it maintains. Moreover, the Agency's substantial connectivity with many nongovernmental educational and research institutions presents cybercriminals with a larger target than most other Government agencies.

[6] Administrative consoles and web login portals are web applications that allow users to remotely manage or access an organization's IT devices or data.

[7] WhiteHat Security, Website Security Whitepaper Top 5 Myths of Website Security, Revised December 2011.

Hackers have improperly gained access to NASA computer systems on numerous occasions. These incidents run the gamut from individuals testing their skills, to well-organized criminal enterprises hacking for profit, to intrusions likely sponsored by foreign intelligence services. Although some of these intrusions were minor incidents that caused no real damage, others affected thousands of NASA computers, caused significant disruption to mission operations, and resulted in the theft of sensitive data. For example, in July 2013 hackers compromised a NASA Shared Services Center website containing personally identifiable information for Agency civil servants and contractors. Additionally, in September 2013, several NASA websites hosted by the Ames Research Center were taken offline after a hacker posted political statements opposing U.S. policy. Because of NASA's status as a "target rich" environment, the NASA Office of Inspector General (OIG) devotes substantial resources to overseeing the Agency's efforts to protect its IT systems.[8]

According to NASA policy, Agency websites created after 2008 must be registered, approved, and managed through the Agency's Internet Protocol Asset Management (IPAM) system. To be registered and approved, websites must undergo a vulnerability scan and receive approval from the cognizant Center Chief Information Security Officer. Upon approval, NASA assigns the website an internet protocol (IP) address through IPAM and authorizes connection to the Internet.[9]

Web Application Vulnerabilities. According to the Open Web Application Security Project, secure websites incorporate measures to protect against the following types of attacks and vulnerabilities:[10]

1. **Injection.** Structured query language (SQL) injection attacks represent the greatest security threat to web applications. SQL is an industry standard computer language used to query, operate, and administer many databases, including Microsoft and Oracle products. In a SQL injection attack, the attacker injects instructions onto the end of a valid SQL statement in an attempt to gain unauthorized access to a computer system. Failure to fully validate user input by removing potentially malicious instructions exposes web applications to SQL

[8] Since 2011, the OIG has issued five reports addressing this issue: "NASA's Adoption of Cloud-Computing Technologies" (IG-13-021, July 29, 2013); "NASA's Information Technology (IT) Governance" (IG-13-015, June 5, 2013); "Review of NASA's Computer Security Incident Detection and Handling Capability" (IG-12-017, August 8, 2012); "NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems" (IG-12-006, December 5, 2011); and "Inadequate Security Practices Expose Key NASA Network to Cyber Attack" (IG-11-17, March 28, 2011).

[9] An IP address is a numerical communications protocol or set of standard rules used to transmit data over the Internet. The most widely used protocol on the Internet today is IP Version 4, which provides about 4.3 billion IP addresses for use worldwide

[10] The Open Web Application Security Project is an international nonprofit organization that focuses on improving software security. The Project has identified the most widely exploited web application vulnerabilities and published best practices to help organizations avoid exploitation.

injection attacks. A vulnerable web application passes the attacker's commands along with the valid SQL statement to the application and system's back-end database. The results of a successful injection attack may include:

- *unauthorized information disclosure,* in which the attacker steals sensitive information from databases connected to the web application;
- *authentication bypass,* in which the attacker is able to log in to a web application without a valid username and password; and
- *compromising host computer*, in which the attacker executes a command that enables control of the computer operating the application and uses the compromised computer to exploit other computers on the network to obtain user account information, steal sensitive data, or disrupt operations.

2. **Cross-site scripting.** Cross-site scripting flaws occur when an application takes data entered by an outside user and sends it to a web browser without proper validation. These flaws allow attackers to execute scripts in the victim's computer browser that can hijack user sessions, deface websites, or redirect the user to malicious sites.

3. **Broken authentication and session management.** Improper user authentication can enable attackers to compromise passwords or exploit other system weaknesses in order to assume an authorized user's identity.

4. **Security misconfiguration.** Failure to implement and maintain a secure configuration for web applications, frameworks, application servers, web servers, databases, and up-to-date software can result in unauthorized access.

In a March 2011 audit report, we recommended that NASA implement a program to continuously monitor Agency networks and take prompt action to mitigate identified vulnerabilities.[11] In response, NASA established the Web Application Security Program (WASP) to identify and assess vulnerabilities on the Agency's publicly accessible web applications and to mitigate the most significant of those vulnerabilities. As part of WASP, NASA's Office of the Chief Information Officer (OCIO) collaborated with the Langley and Ames Research Centers to scan Agency public IP addresses on a regular basis. Since the end of 2012, NASA has regularly scanned its IP addresses to identify the universe of publicly accessible computers connected to Agency networks.[12] Moreover, as part of its WASP initiative NASA hired the consulting firm Booz Allen Hamilton (Booz Allen) to conduct both automated scans and manual testing of Agency web applications to identify, categorize, and track vulnerabilities. Two contractor employees

[11] NASA OIG, "Inadequate Security Practices Expose Key NASA Network to Cyber Attack" (IG-11-17, March 28, 2011).

[12] NASA uses Nmap, a software program that can identify hosts (computers) present on a network and the services, including applications such as e-mail or file sharing, those hosts offer.

working full time perform automated scans to search for vulnerabilities on identified active devices running web-based services and manually test publicly accessible NASA applications to identify vulnerabilities not detected by the automated scanning. The contractors refer "critical" or "high-severity" vulnerabilities to the OCIO and the affected Center, which are responsible for mitigating the problem.[13]

In fiscal year (FY) 2013, the OCIO initiated the NASA Web Enterprise Services Technology (WestPrime) contract to support the Agency's transition from an IT environment that relies on storing data and applications at multiple data centers to one that increasingly relies on storing information and applications in the public cloud. The OCIO strongly encourages but does not mandate NASA Centers, programs, and projects use WestPrime when acquiring web-based, cloud-computing services. As of April 2014, the OCIO and the WestPrime contractor managed approximately 140 internal and public NASA websites. NASA expects significant increases in use of the cloud over the next 5 years, estimating that up to 75 percent of new IT programs could begin in the cloud and nearly 100 percent of the Agency's public data could be stored there.

Objectives

Our overall objective was to assess the effectiveness of NASA's efforts to secure its publicly accessible web applications. To do this we evaluated (1) the efficacy of WASP and (2) NASA's efforts to reduce its publicly accessible web applications. Details of the audit's scope and methodology are set forth in Appendix A.

[13] Critical vulnerabilities are those that if exploited could result in severe impact to the Agency. High-severity vulnerabilities are those that are of high concern due to ease of exploitation or the severity of impact if exploited.

NASA HAS IMPROVED THE SECURITY OF ITS PUBLIC WEB APPLICATIONS BUT NEEDS TO ADDRESS REMAINING VULNERABILITIES, STRENGTHEN PROGRAM OVERSIGHT, AND FURTHER REDUCE ITS EXTENSIVE WEB PRESENCE

NASA has improved the security of the Agency's publicly accessible web applications using an enterprise-wide approach to identify and assess vulnerabilities and mitigate identified vulnerabilities. In addition, over a 15-month period ending in March 2014, NASA reduced by 15 percent its publicly accessible web applications, from approximately 1,500 to 1,200. Despite this progress, we found deficiencies in the design and implementation of NASA's approach that leaves the Agency's publicly accessible web applications at risk of compromise. Specifically, NASA did not prioritize the identification of vulnerabilities by seriousness of impact, identify the underlying cause of the vulnerabilities, address identified weaknesses in Agency IT security practices, and implement an effective process to ensure timely mitigation of vulnerabilities. In addition, while NASA has reduced its publicly accessible web presence, the Agency's remaining 1,200 publicly accessible web applications continue to present a large number of potential entry points for attackers.

NASA Has Reduced its Web Presence and Improved Security of its Public Web Applications

NASA has improved the security of publicly accessible web applications by developing a complete inventory of such applications. Since April 2012, NASA IT officials have used Nmap, a widely accepted open-source software program, to perform annual and quarterly Agency-wide scans to identify all NASA IP addresses accessible from the Internet. Nmap identifies active computers on NASA's networks and the services they run, such as e-mail and file sharing.

The SANS Institute and other security experts recommend a hybrid approach to identifying Internet security weaknesses, including both automated vulnerability scanning and manual testing.[14] We found that NASA followed this best practice and that Booz Allen conducted both automated scans and manual testing to identify, categorize, and track web application vulnerabilities. In addition, since March 2014 new publicly accessible Agency websites may be launched only with approval from the Agency Chief Information Officer (CIO) and after an automated vulnerability scan. Any high-risk vulnerabilities detected must be mitigated before the websites are permitted to go live.

[14] The SANS Institute is a private company recognized for expertise in IT and Internet security training.

We reviewed NASA's Agency-wide Nmap scans from late 2012 through the first quarter of 2014 and found NASA had reduced its publicly accessible web applications by 15 percent, from approximately 1,500 to 1,200. As part of an ongoing effort, NASA IT security officials told us that they targeted obsolete or duplicative applications for elimination. In addition, the Agency CIO has encouraged Centers and Mission Directorates to utilize the WestPrime contract when moving web applications from NASA data centers to the public cloud. According to the Agency Web Services Executive, one of the goals of these initiatives is to reduce NASA's web presence by encouraging adoption of cloud computing services and by limiting the growth of new publicly accessible web applications. Moving applications off NASA's networks and into the cloud reduces the total number of entry points attackers can exploit.

Despite this progress, we found that deficiencies in the design and implementation of WASP, combined with the Agency's extensive Internet presence, continue to place NASA's systems and data at risk of compromise.

Vulnerabilities Not Prioritized by System Impact

Effectively managing risk dictates NASA identify and address vulnerabilities in high- and moderate-impact systems before those in low-impact systems.[15] Accordingly, as part of our audit we sought to determine the number of publicly accessible Agency web applications associated with high- and moderate-impact systems and whether WASP prioritized vulnerability detection according to security impact level.

We used the quarterly Nmap scans to identify IP addresses associated with NASA's publicly accessible web applications and linked those addresses to their system security plans in order to determine the security impact level.[16] According to information in NASA's IT security database at the time of our audit, 1,464 IP addresses were associated with NASA's publicly accessible web applications. As we have noted in prior audit work, NASA systems have been properly categorized.[17] However, not all of the system categorization information on NASA's publicly accessible web applications has been entered into the IT security asset database. In fact, of those addresses associated with public website applications, 429 (29 percent) were

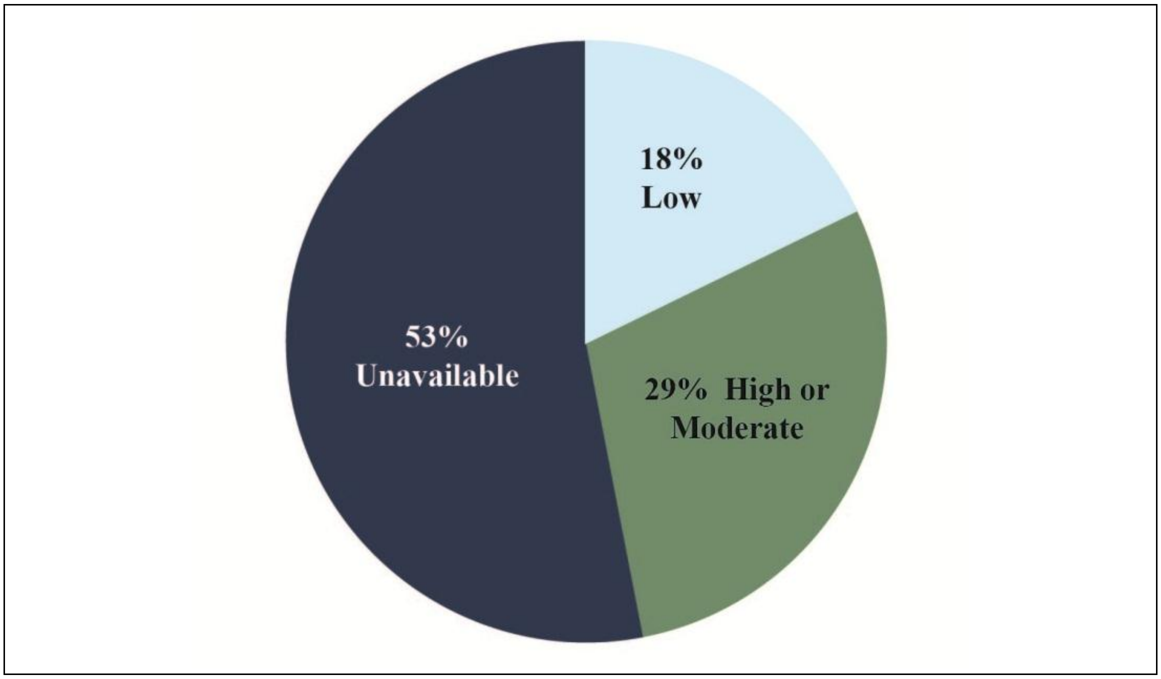
[15] According to the National Institute of Standards and Technology, the loss of confidentiality, integrity, or availability in a moderate-impact system could have serious adverse effects on an organization's operations, assets, or individuals. Such a loss in a high-impact system could result in severe or catastrophic effects.

[16] According to the National Institute of Standards and Technology (NIST), a system security plan is a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The security impact level (high, moderate, low) is a required element of a NIST-compliant system security plan.

[17] NASA OIG, "Federal Information Security Management Act: Fiscal Year 2008 Report from the Office of Inspector General" (IG-08-031, September 30, 2008).

categorized as either high- or moderate-impact, 256 (18 percent) as low impact, and the remaining 775 (53 percent) had no categorization available in the IT security asset database (Figure 1).[18]

Figure 1. NASA's Internet-accessible Web Applications by Security Categorization



Source: NASA OIG.

Experience has shown that detecting vulnerabilities in web applications requires a combination of automated and manual testing, with WASP identifying 90 percent of the vulnerabilities in NASA systems using manual testing and 10 percent from automated scanning. Automated scanning has the ability to identify certain categories of vulnerabilities, including some SQL injection and cross-site scripting; however, complex vulnerabilities such as flaws in security functionality design (e.g., designs related to authentication and authorization) are not readily identified using automated techniques and require manual testing. Because manual testing requires a significant amount of time and resources, efficient use of such testing requires focusing on high- and moderate-impact systems before turning to low-impact systems.

We found that WASP has not mapped NASA's publicly accessible web applications back to their information systems using the Agency's security categorization data to determine their security impact level. Accordingly, WASP is unable to prioritize manual scanning by risk level, which increases the risk that vulnerabilities in critical publicly accessible web applications may go undetected and unmitigated.

[18] Although NASA has categorized these systems, this information has not been entered in its IT security asset database.

WASP did not Address Root Cause of Vulnerabilities

Identifying and addressing the root cause of a system's security vulnerabilities helps prevent them from recurring and is a recognized best IT security practice. We noted that WASP identified a repeating pattern of high-severity vulnerabilities associated with certain publicly accessible web applications that allow NASA personnel to access Agency systems and network resources remotely. Specifically, these web applications support login portals and management consoles NASA civil servants and contractors use to remotely manage IT resources such as telecommunications devices, multifunction printers, and networking equipment. We found significant security weaknesses with these login portals and management consoles. For example, we identified usernames and passwords written directly into source code, credentials sent unencrypted over the Internet, and management consoles that permitted nonauthenticated access to NASA IT resources.

In addition, we found that these login portals and management consoles often were not registered in the Agency's IPAM system. Since 2008, NASA policy has required that new publicly accessible websites originating from the Agency be registered, approved, and managed through the IPAM process and tested for vulnerabilities before deployment. However, this policy does not apply to other types of web applications such as login portals and management consoles. In our judgment, the root cause of the recurring vulnerabilities associated with these web applications is a control deficiency that allowed the applications to be deployed without undergoing the type of oversight and testing required for public websites. While WASP identified and tracked vulnerabilities associated with these web applications, it did not address the root cause of the vulnerabilities by not taking action to remedy missing controls in business processes that allowed the applications to be deployed in the first place.

WASP did not Identify Weaknesses Associated with Unsound IT Security Practices

Hackers may target publicly accessible web applications under development or undergoing testing because these applications often lack security controls common on production applications. If these preproduction applications contain "live" test data, a system breach could result in loss of sensitive data. For these reasons, best practices dictate that development and testing of web applications take place in an environment isolated from the Internet and separate from the organization's production databases. In addition, this testing and development process should never use or connect to databases containing live data. Center Chief Information Security Officers we spoke with agreed that enabling Internet access to preproduction web applications is a poor security practice and should be avoided.

We reviewed the registered name or uniform resource indicator (URI) of NASA's publicly accessible web applications to determine if any were under development or in the testing phase.[19] Typically, these web applications will have a URI that contains strings such as ".dev," ".test," or ".tst." Hackers often develop a list of the intended target's public web applications and first attack any applications under development or in testing.

We identified 15 URIs associated with NASA's publicly accessible web applications that were under development or in a test phase. Two of the 15 were pre-production applications of a moderate-impact system used to manage IT system access privileges that contained usernames and passwords for more than 55,000 NASA civil servants and contractors. We also confirmed that both of these preproduction web applications were connected to databases containing actual NASA user credentials. We immediately reported these vulnerabilities to Center security officials.

An attacker who accessed either of the two applications could have easily extracted thousands of user identifiers (ID). Using these IDs, the attacker could attempt to log in to NASA systems using an automated tool that repeatedly "guesses" the corresponding password, a technique known as a brute force attack. If successful in gaining unauthorized access to an Agency network, the attacker would possess the same access privileges as the NASA civil servant or contractor whose identity the hacker had assumed. If that employee was a systems administrator, the hacker could (1) modify, copy, or delete sensitive files; (2) add, modify, or delete user accounts for NASA systems; (3) upload hacking tools to steal user credentials and compromise other NASA systems; and (4) modify system logs to conceal their actions. In FY 2013, brute force attacks accounted for 6 percent (11 of 183) of breaches into Agency systems.

In our judgment, WASP did not identify this significant security vulnerability because it focused too narrowly on identifying technical vulnerabilities, such as SQL injection flaws, and did not identify weaknesses associated with broader, unsound IT security practices.

Untimely Mitigation of Vulnerabilities Puts NASA's Public Web Applications at Risk of Compromise

Prompt mitigation of vulnerabilities in NASA's publicly accessible web applications is essential to ensure the confidentiality, integrity, and availability of Agency systems and data. We examined the status of documented web application vulnerabilities and found that in January 2014, 93 percent (26 of 28) of confirmed critical and high-severity vulnerabilities remained unmitigated more than 6 months after notification to the affected Center.

[19] Uniform Resource Indicator (also referred to as Uniform Resource Locator or URL) is a string of characters used to identify a website or web resource. For example, www.nasa.gov is the URL for NASA's primary public website.

WASP ranks identified vulnerabilities as critical, high, moderate, low, and informational based on their potential to disrupt Agency operations. NASA requires prompt mitigation of all critical and high-severity vulnerabilities due to the potentially adverse effect they could have on Agency operations if exploited. Specifically, NASA's IT security policy requires WASP to notify Center Chief Information Security Officers about all critical and high-severity vulnerabilities within 5 business days of discovery and Centers are expected to complete corrective actions to mitigate the vulnerabilities within 5 business days of notification. Consequently, Agency policy requires that all critical and high-severity vulnerabilities should be mitigated no later than 10 business days from discovery.

Corrective actions may include mitigating the vulnerability by modifying the web application's code, isolating the application by removing it from the Internet and moving it to an Agency internal or private network, or decommissioning the application. To verify mitigation of vulnerabilities, WASP manually checks for removal of the vulnerability or validates the system when performing quarterly vulnerability scans. After confirmation of mitigation, the vulnerability is deleted from the Agency's vulnerability tracking system – a system managed by Booz Allen and one to which the OCIO and Centers do not have access.

In our judgment, critical and high-severity vulnerabilities in NASA web applications went unmitigated because OCIO staff do not have access to the Agency's vulnerability tracking system to monitor the status of vulnerabilities and corrective actions. OCIO officials said a lack of resources prevent them from monitoring the real-time status of all vulnerabilities in the system. Moreover, Center IT staff told us they could not determine the status of their Center's vulnerabilities because they did not have access to the system. Finally, we found that WASP generally used a 45-day rather than the required 10-day timeframe for validating whether critical and high- severity vulnerabilities had been mitigated.

Conclusion

NASA's publicly accessible web applications are under constant attack by hackers and the frequency and sophistication of these attacks is increasing. Thus, it is imperative that the Agency find and mitigate vulnerabilities in NASA web applications before attackers can exploit them. In addition, NASA should identify the root cause of security weaknesses to prevent vulnerabilities from recurring. The Agency also needs to improve oversight of its vulnerability mitigation program to ensure identified deficiencies are addressed promptly. Finally, while the Agency has made progress in reducing its publicly accessible web presence by more than 300 applications, the 1,200 remaining publicly accessible web applications provide multiple potential entry points for attackers seeking to gain unauthorized access to Agency systems and data.

Recommendations

To improve the effectiveness of NASA's Web Application Security Program, we recommend that the Agency Chief Information Officer:

Recommendation 1. Modify WASP protocols to prioritize vulnerability discovery and mitigation resources on the highest impact systems first.

Management's Response. The Agency CIO concurred with our recommendation, stating the WASP protocol will be adjusted to prioritize vulnerability discovery and mitigation based on risk, impact, and data set sensitivity by October 31, 2014.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

Recommendation 2. Require that all publicly accessible web applications, including login portals and management consoles, be registered in the Agency's IPAM System and pass a vulnerability test prior to deployment.

Management's Response. The Agency CIO concurred with our recommendation, stating the WASP protocol will be modified to address the issues identified in this report starting with the quarterly scan cycle beginning no later than October 1, 2014. This quarterly cycle will be evaluated with the January 1, 2015 scan and complete the evaluation by January 31, 2015.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

Recommendation 3. Remove from the Internet or secure with a web application firewall all Agency web applications in development or testing mode.

Management's Response. The Agency CIO concurred with our recommendation, stating that by January 1, 2015, the OCIO will work with stakeholders to ensure that policies and processes are in place to identify and secure web applications that are in development or testing mode.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

Recommendation 4. Ensure that critical and high-severity web application vulnerabilities are mitigated within 10 business days of discovery, as required by Agency policy.

> **Management's Response.** The Agency CIO concurred with our recommendation, stating that by January 1, 2015, the WASP team's governance processes and procedures will be updated to ensure that findings are mitigated in accordance with Agency policy. Furthermore, processes will be updated to ensure stakeholders are notified of outstanding critical and high-risk findings that need to be addressed or remediated, "deferred" as a Plan of Action and Milestones, or accepted as a risk.
>
> **Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

Recommendation 5. Grant Center Chief Information Security Officers and OCIO officials access to the Agency vulnerability tracking system to ensure adequate monitoring of the status of vulnerabilities.

> **Management's Response.** The Agency CIO concurred with our recommendation and stated that by December 5, 2014, the WASP team will develop procedures to grant officials user accounts in the Agency's vulnerability tracking system.
>
> **Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

APPENDIX A

Scope and Methodology

We performed this audit from July 2013 through June 2014 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.

In order to determine whether NASA implemented adequate security measures over its publicly accessible web applications to reduce the risk of compromise as required by Federal and Agency guidance and industry best practices, we interviewed OCIO officials, Center IT security personnel, and Booz Allen contractors in charge of WASP. We reviewed the Agency's WASP handbook. We used the Agency's quarterly Nmap scans to identify development systems, test systems, and management consoles on NASA's network that are publicly accessible. In addition, we used the quarterly Nmap scans to quantify the number of Agency IP addresses associated with its publicly accessible web applications. Then, we linked the IP addresses for NASA's publicly accessible web applications back to their related system security plans as noted in the Agency's IPAM system to determine their Federal Information Processing Standard 199 system impact level. Finally, we reviewed the status of web application vulnerabilities in the Agency tracking system to determine the number of vulnerabilities that have not been mitigated within 6 months.

In order to determine the status of NASA initiatives to reduce the Agency's number of publicly accessible web applications, we interviewed NASA officials to determine the progress made and barriers encountered. We also obtained the Agency's quarterly Nmap scans and identified the total number of IP addresses associated with publicly accessible web applications for each quarter in order to determine whether there was a reduction in the total web applications exposed.

Use of Computer-Processed Data. We reviewed the Agency Nmap scans. We verified the completeness of this listing by reviewing the script used to run the scans and comparing the IP addresses in the scan to those in the inventory system, IPAM. In addition, we reviewed the Agency's vulnerability tracking system. While we did not verify the accuracy of the vulnerabilities, this did not impact our findings or conclusions.

Review of Internal Controls

We identified and evaluated the effectiveness of internal controls in place for NASA's WASP program related to the identification of all publicly accessible web applications, assessment of these web applications for vulnerabilities, and mitigation of the most severe vulnerabilities before they can be exploited. The control weaknesses we identified are discussed in the Results section of this report. Our recommendations, if implemented, should correct the identified weaknesses.

Prior Coverage

During the last 5 years, the Department of Commerce Office of Inspector General, Department of Homeland Security Office of Inspector General, Department of Transportation Office of Inspector General, and the Office of Personnel Management Office of Inspector General have issued four reports of particular relevance to the subject of this report/audit. Unrestricted reports can be accessed over the Internet at http://www.oig.doc.gov (Department of Commerce Office of Inspector General), http://www.oig.dhs.gov/ (Department of Homeland Security Office of Inspector General), https://www.oig.dot.gov/ (Department of Transportation Office of Inspector General), and http://www.opm.gov/our-inspector-general/ (Office of Personnel Management Office of Inspector General).

Department of Commerce Office of Inspector General

"Improvements are Needed for Effective Web Security Management" (OIG-12-002-A, October 21, 2011)

Department of Homeland Security Office of Inspector General

"Vulnerabilities Highlight the Need for More Effective Web Security Management" (OIG-09-101, September 2009)

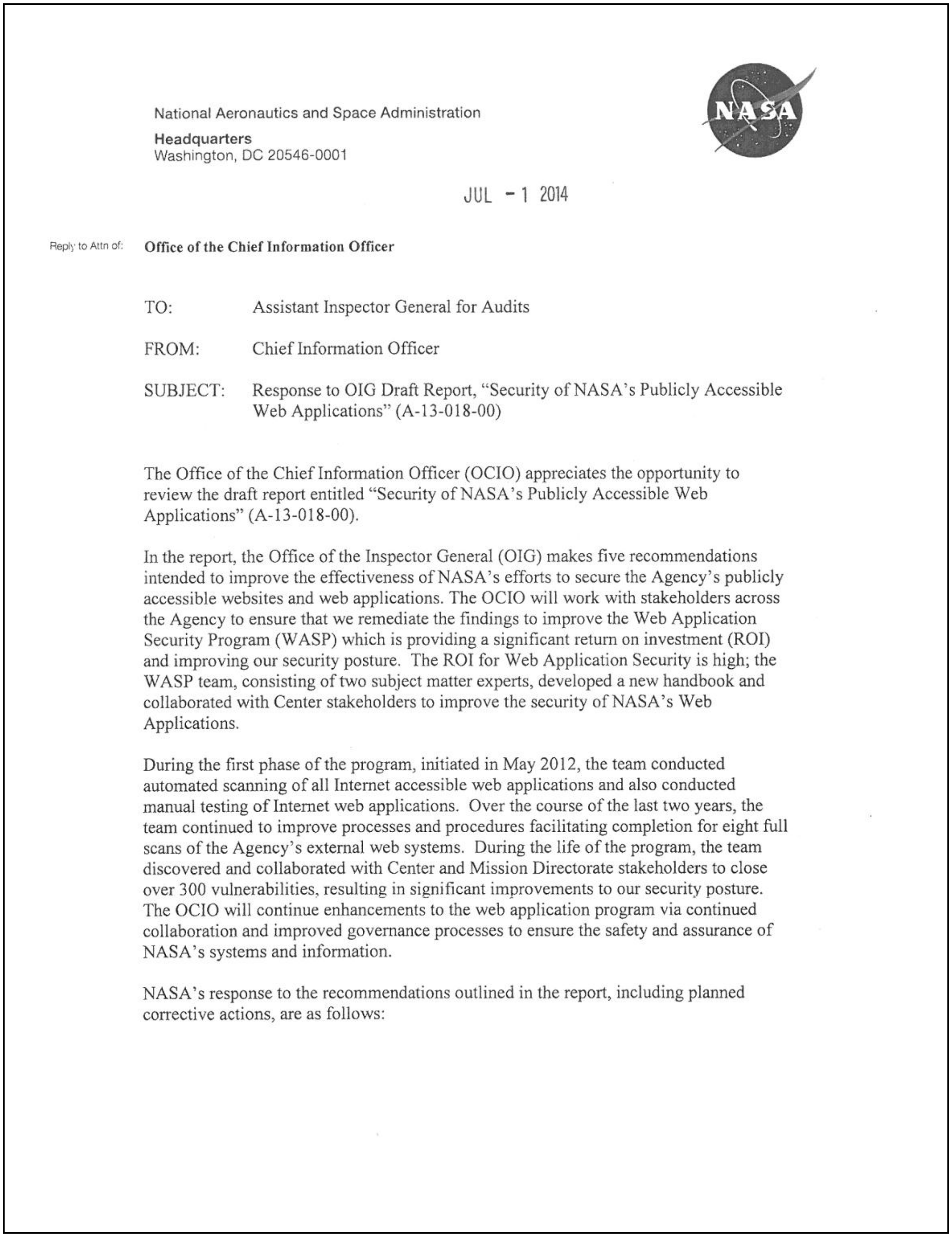
Department of Transportation Office of Inspector General

"Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems" (FI-2009-049, May 4, 2009)

Office of Personnel Management Office of Inspector General

OPM OIG "Audit of the Information Security Posture of the U.S. Office of Personnel Management's USAJOBS System FY2012" (4A-HR-00-12-037, July 26, 2012)

MANAGEMENT COMMENTS



National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001

JUL - 1 2014

Reply to Attn of: **Office of the Chief Information Officer**

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

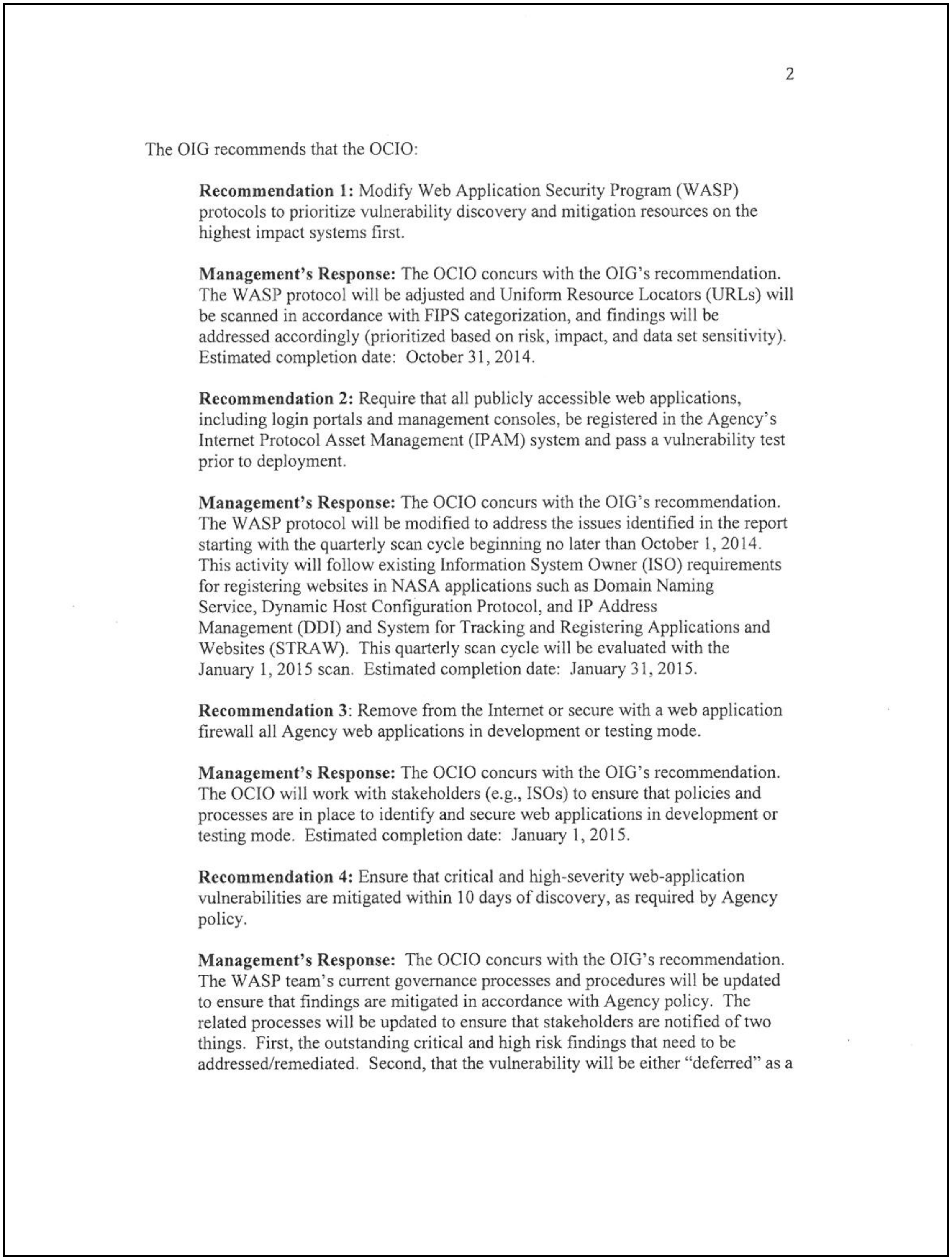
SUBJECT: Response to OIG Draft Report, "Security of NASA's Publicly Accessible Web Applications" (A-13-018-00)

The Office of the Chief Information Officer (OCIO) appreciates the opportunity to review the draft report entitled "Security of NASA's Publicly Accessible Web Applications" (A-13-018-00).

In the report, the Office of the Inspector General (OIG) makes five recommendations intended to improve the effectiveness of NASA's efforts to secure the Agency's publicly accessible websites and web applications. The OCIO will work with stakeholders across the Agency to ensure that we remediate the findings to improve the Web Application Security Program (WASP) which is providing a significant return on investment (ROI) and improving our security posture. The ROI for Web Application Security is high; the WASP team, consisting of two subject matter experts, developed a new handbook and collaborated with Center stakeholders to improve the security of NASA's Web Applications.

During the first phase of the program, initiated in May 2012, the team conducted automated scanning of all Internet accessible web applications and also conducted manual testing of Internet web applications. Over the course of the last two years, the team continued to improve processes and procedures facilitating completion for eight full scans of the Agency's external web systems. During the life of the program, the team discovered and collaborated with Center and Mission Directorate stakeholders to close over 300 vulnerabilities, resulting in significant improvements to our security posture. The OCIO will continue enhancements to the web application program via continued collaboration and improved governance processes to ensure the safety and assurance of NASA's systems and information.

NASA's response to the recommendations outlined in the report, including planned corrective actions, are as follows:



The OIG recommends that the OCIO:

Recommendation 1: Modify Web Application Security Program (WASP) protocols to prioritize vulnerability discovery and mitigation resources on the highest impact systems first.

Management's Response: The OCIO concurs with the OIG's recommendation. The WASP protocol will be adjusted and Uniform Resource Locators (URLs) will be scanned in accordance with FIPS categorization, and findings will be addressed accordingly (prioritized based on risk, impact, and data set sensitivity). Estimated completion date: October 31, 2014.

Recommendation 2: Require that all publicly accessible web applications, including login portals and management consoles, be registered in the Agency's Internet Protocol Asset Management (IPAM) system and pass a vulnerability test prior to deployment.

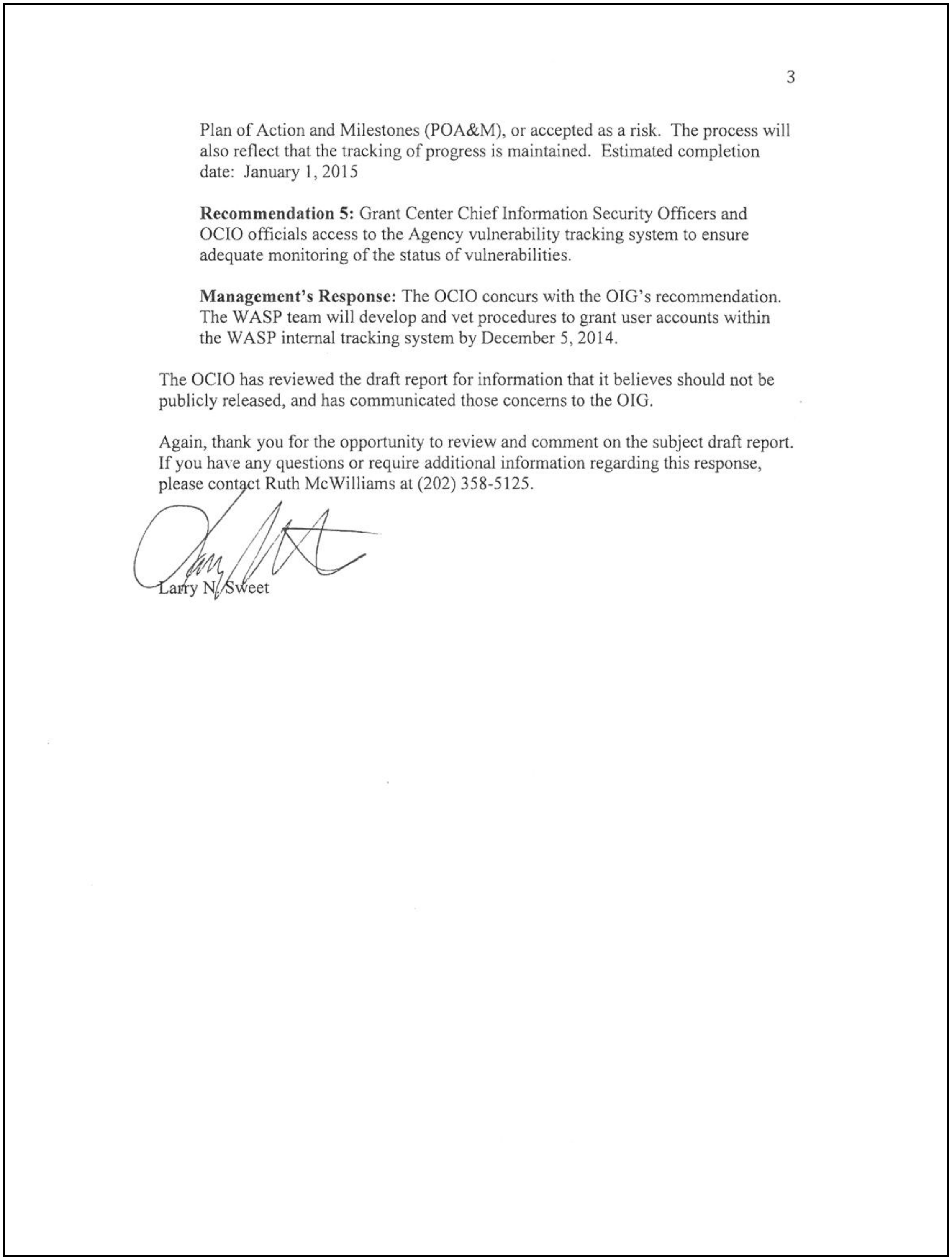
Management's Response: The OCIO concurs with the OIG's recommendation. The WASP protocol will be modified to address the issues identified in the report starting with the quarterly scan cycle beginning no later than October 1, 2014. This activity will follow existing Information System Owner (ISO) requirements for registering websites in NASA applications such as Domain Naming Service, Dynamic Host Configuration Protocol, and IP Address Management (DDI) and System for Tracking and Registering Applications and Websites (STRAW). This quarterly scan cycle will be evaluated with the January 1, 2015 scan. Estimated completion date: January 31, 2015.

Recommendation 3: Remove from the Internet or secure with a web application firewall all Agency web applications in development or testing mode.

Management's Response: The OCIO concurs with the OIG's recommendation. The OCIO will work with stakeholders (e.g., ISOs) to ensure that policies and processes are in place to identify and secure web applications in development or testing mode. Estimated completion date: January 1, 2015.

Recommendation 4: Ensure that critical and high-severity web-application vulnerabilities are mitigated within 10 days of discovery, as required by Agency policy.

Management's Response: The OCIO concurs with the OIG's recommendation. The WASP team's current governance processes and procedures will be updated to ensure that findings are mitigated in accordance with Agency policy. The related processes will be updated to ensure that stakeholders are notified of two things. First, the outstanding critical and high risk findings that need to be addressed/remediated. Second, that the vulnerability will be either "deferred" as a



Plan of Action and Milestones (POA&M), or accepted as a risk. The process will also reflect that the tracking of progress is maintained. Estimated completion date: January 1, 2015

Recommendation 5: Grant Center Chief Information Security Officers and OCIO officials access to the Agency vulnerability tracking system to ensure adequate monitoring of the status of vulnerabilities.

Management's Response: The OCIO concurs with the OIG's recommendation. The WASP team will develop and vet procedures to grant user accounts within the WASP internal tracking system by December 5, 2014.

The OCIO has reviewed the draft report for information that it believes should not be publicly released, and has communicated those concerns to the OIG.

Again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Ruth McWilliams at (202) 358-5125.

Larry N. Sweet

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief of Staff
Chief Information Officer

Non-NASA Organizations and Individuals

Office of Management and Budget
  Deputy Associate Director, Energy and Science Division
    Branch Chief, Science and Space Programs Branch
Government Accountability Office
  Director, Office of Acquisition and Sourcing Management

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
  Subcommittee on Commerce, Justice, Science, and Related Agencies
Senate Committee on Commerce, Science, and Transportation
  Subcommittee on Science and Space
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
  Subcommittee on Commerce, Justice, Science, and Related Agencies
House Committee on Oversight and Government Reform
  Subcommittee on Government Operations
House Committee on Science, Space, and Technology
  Subcommittee on Oversight
  Subcommittee on Space

Major Contributors to the Report:
Wen Song, Director Information Technology Audit
Jefferson Gilkeson, Program Manager
Morgan Reynolds, Audit Team Lead

JULY 10, 2014

REPORT NO. IG-14-023

OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit http://oig.nasa.gov/audits/reports/FY14/ to obtain additional copies of this report, or contact the Assistant Inspector General for Audits at 202-358-1232.

COMMENTS ON THIS REPORT

In order to help us improve the quality of our products, if you wish to comment on the quality or usefulness of this report, please send your comments to Mr. Laurence Hawkins, Audit Operations and Quality Assurance Director, at Laurence.B.Hawkins@nasa.gov or call 202-358-1543.

SUGGESTIONS FOR FUTURE AUDITS

To suggest ideas for or to request future audits, contact the Assistant Inspector General for Audits. Ideas and requests can also be mailed to:

Assistant Inspector General for Audits
NASA Headquarters
Washington, DC 20546-0001

NASA HOTLINE

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD). You may also write to the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026, or use http://oig.nasa.gov/hotline.html#form. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.