MARCH 28, 2011

AUDIT REPORT

OFFICE OF AUDITS

INADEQUATE SECURITY PRACTICES EXPOSE KEY NASA NETWORK TO CYBER ATTACK

OFFICE OF INSPECTOR GENERAL

National Aeronautics and
Space Administration

REPORT NO. IG-11-017 (ASSIGNMENT NO. A-10-011-00)

Final report released by:

Paul K. Martin
Inspector General

Acronyms

FTP	File Transfer Protocol
IP	Internet Protocol
IT	Information Technology
JPL	Jet Propulsion Laboratory
OA	Office of Audits
OIG	Office of Inspector General
VPN	Virtual Private Network

OVERVIEW

INADEQUATE SECURITY PRACTICES EXPOSE KEY NASA NETWORK TO CYBER ATTACK

The Issue

NASA relies on a series of computer networks to carry out its various missions, including controlling spacecraft like the International Space Station and conducting science missions like the Hubble Telescope. Therefore, it is imperative that NASA protect its computer networks from cyber attacks that could disrupt operations or result in the loss of sensitive data. In this audit, we evaluated whether NASA protected information technology (IT) assets on its Agency-wide mission computer network from Internet-based cyber attacks. Specifically, we assessed whether NASA adequately protected these IT assets from Internet-based attacks by regularly assessing risks and identifying and mitigating vulnerabilities. We also reviewed internal controls as appropriate. Details of the audit's scope and methodology are in Appendix A.

Results

We found that computer servers on NASA's Agency-wide mission network had high-risk vulnerabilities that were exploitable from the Internet. Specifically, six computer servers associated with IT assets that control spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable. Moreover, once inside the Agency-wide mission network, the attacker could use the compromised computers to exploit other weaknesses we identified, a situation that could severely degrade or cripple NASA's operations. We also found network servers that revealed encryption keys, encrypted passwords, and user account information to potential attackers. These data are sensitive and provide attackers additional ways to gain unauthorized access to NASA networks. These deficiencies occurred because NASA had not fully assessed and mitigated risks to its Agency-wide mission network and was slow to assign responsibility for IT security oversight to ensure the network was adequately protected. In a May 2010 audit report, we recommended that NASA immediately establish an IT security oversight program for this key network.[1] However, even though the Agency concurred with the recommendation it remained unimplemented as of February 2011. Until NASA addresses these critical deficiencies and improves its IT

[1] NASA OIG, "Review of the Information Technology Security of [a NASA Computer Network]" (IG-10-013, May 13, 2010).

security practices, the Agency is vulnerable to computer incidents that could have a severe to catastrophic effect on Agency assets, operations, and personnel.

Management Action

In order to strengthen the Agency's IT security program, we urge NASA to expedite implementation of our May 2010 recommendation to establish an IT security oversight program for NASA's Agency-wide mission network. We also recommend that NASA Mission Directorates (1) immediately identify Internet-accessible computers on their mission networks and take prompt action to mitigate identified risks and (2) continuously monitor Agency mission networks for Internet-accessible computers and take prompt action to mitigate identified risks. Finally, to help ensure that all threats and vulnerabilities to NASA's IT assets are identified and promptly addressed, we recommend that NASA's Chief Information Officer, in conjunction with the Mission Directorates, conduct an Agency-wide IT security risk assessment.

In response to a draft of this report, the Chief Information Officer and Mission Directorates concurred with our recommendations. The Chief Information Officer stated that she will work with the Mission Directorates and Centers to develop a comprehensive approach to ensure that Internet-accessible computers on NASA's mission networks are routinely identified, vulnerabilities are continually evaluated, and risks are promptly mitigated by September 30, 2011. In addition, the Chief Information Officer said she will develop and implement a strategy for conducting an Agency-wide risk assessment by August 31, 2011. The full text of NASA's comments can be found in Appendix B.

We consider the Chief Information Officer's proposed actions to be responsive to our recommendations. Therefore, the recommendations are resolved and will be closed upon verification that management has completed the corrective actions.

CONTENTS

INTRODUCTION

Background

The threat to NASA's computer networks from Internet-based intrusions is tangible and expanding in both scope and frequency. For example, in May 2009 NASA notified the Office of Inspector General (OIG) of a suspicious computer connection from a system that supports Agency space operations and space exploration activities. The subsequent OIG investigation confirmed that cybercriminals had infected a computer system that supports one of NASA's mission networks. Due to the inadequate security configurations on the system, the infection caused the computer system to make over 3,000 unauthorized connections to domestic and international Internet protocol (IP) addresses including addresses in China, the Netherlands, Saudi Arabia, and Estonia.[2] In another cyber attack in January 2009, cybercriminals stole 22 gigabytes of export-restricted data from a Jet Propulsion Laboratory (JPL) computer system. The sophistication of both of these Internet-based intrusions confirms that they were focused and sustained efforts to target assets on NASA's mission computer networks.

NASA's Agency-wide mission network is widely distributed throughout the United States and hosts more than 190 IT systems and projects run by the Agency's Mission Directorates and JPL. Included in these 190 IT assets are computer systems and projects that control the Hubble Space Telescope, the Space Shuttle, the International Space Station, the Cassini and Lunar Reconnaissance orbiters, and several ground stations and mission control centers. These IT systems and projects, categorized as moderate- and high-impact, control spacecraft, collect and process scientific data, and perform other critical Agency functions.[3] Consequently, a security breach of one of these systems or projects could have a severe to catastrophic adverse effect on NASA operations, assets, or personnel.

In order to communicate and share information with external parties, NASA's Agency-wide mission network is connected to the Internet. NASA uses firewall technology to control access to the network. A firewall is a set of IT resources that separate and protect computer systems and data on an organization's internal networks from unauthorized

[2] An IP address is a unique numerical label assigned to each device (such as a computer or printer) connected to a network that uses the Internet protocol to communicate. An information technology system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[3] In a moderate-impact system, the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. In a high-impact system, such a loss could be expected to have a severe or catastrophic adverse effect.

access from an external network, such as the Internet. Specifically, firewalls inspect incoming network traffic and permit or deny requests for access according to an organization's security policy.

Firewalls are only as effective as the rules that security personnel define for them. For example, firewall rules that allow unrestricted access from the Internet to computers on an organization's internal networks are pathways attackers can use to identify and exploit vulnerabilities on these networks. Accordingly, as part of an enterprise-wide IT security risk assessment, organizations should identify and prioritize the mitigation of vulnerabilities that can be exploited from the Internet. This is especially important when these vulnerabilities are associated with moderate- or high-impact systems because a system breach could severely degrade or even cripple an organization's ability to operate. Typically, organizations assess their network security posture from within the confines of their own organizational networks and therefore do not always identify computers that are exploitable from the Internet. Computer hackers, however, assess and evaluate potential targets from the outside. Thus, computers that are accessible from the Internet are prime targets for exploitation and are highly sought after by hackers.

Objectives

We reviewed the firewalls and related computer networking devices that control the flow of network traffic between the Internet and systems on NASA's Agency-wide mission network to determine whether they are effectively configured to protect NASA IT resources from Internet-based threats. We also reviewed internal controls as appropriate. See Appendix A for details of the audit's scope and methodology.

NASA DID NOT ADEQUATELY ASSESS AND MITIGATE RISKS TO ITS AGENCY-WIDE MISSION COMPUTER NETWORK

We performed vulnerability tests on computer servers connected to NASA's Agency-wide mission computer network and found six servers that were exploitable from the Internet. These servers were associated with IT projects that control spacecraft or contain critical NASA data. In addition to servers with high-risk vulnerabilities, we also found servers that exposed encryption keys, encrypted passwords, and user account information. These data are sensitive and provide attackers additional ways to gain unauthorized access to NASA computer networks. These deficiencies occurred because NASA had not fully assessed and mitigated risks to the network and had not assigned responsibility for IT security oversight to ensure the network was adequately protected. A security breach of a moderate- or high-impact system or project on this key network could severely disrupt NASA operations or result in the loss of sensitive data.

Computers on NASA's Agency-wide Mission Network Could Be Exploited from the Internet

NASA computers that are accessible from the Internet are prime targets for exploitation and thus are highly sought after by hackers. To determine the extent to which NASA's Agency-wide mission network was vulnerable to a cyber attack, we first conducted a test to probe the network for Internet-accessible computers.[4] The test included all IP addresses assigned to the more than 190 IT systems and projects on this network – more than 176,000 in total. At the time of our test, we found that NASA's Agency-wide mission network had 54 Internet-accessible computer servers associated with 8 IT projects. These servers were associated with moderate- and high-impact NASA IT projects used to control spacecraft or process critical data.

We contacted the owner of each project and found that two of the eight projects were scheduled for termination and were disposed of during the audit.[5] We performed vulnerability tests on the six remaining projects to determine if they included computers with high-risk vulnerabilities. Specifically, we used NESSUS®, a network vulnerability scanner, to test each computer for vulnerabilities such as running outdated or unpatched

[4] We used Nmap, a widely used software program, to identify Internet-accessible computers. Nmap discovers what hosts (computers) are present on a network and what services (applications such as e-mail or file sharing) those hosts are offering.

[5] Disposal means that all computer hardware related to the project was removed from the network and retired.

software or offering network services that have known security weaknesses. NESSUS® ranks vulnerabilities as high, medium, or low based on their potential to harm the system.

One of the IT projects we reviewed had an Internet-accessible server that was susceptible to a file transfer protocol (FTP) bounce attack – a highly effective form of cyber attack, widely known since 1998.[6] As shown in Figure 1 below, in an FTP bounce attack the attacker connects to and exploits a software flaw in the FTP server (1 and 3). Next, the attacker uses the FTP server as a middle-man to discreetly scan computers positioned behind the firewall for vulnerabilities (2). The scan results are relayed from the FTP server back through the firewall to the attacker (4), and the attacker uses the scan results to exploit other computers on the network, disrupt operations, or steal data.

Figure 1: Attacker Exploits Vulnerability to Disrupt NASA Operations or Steal Data

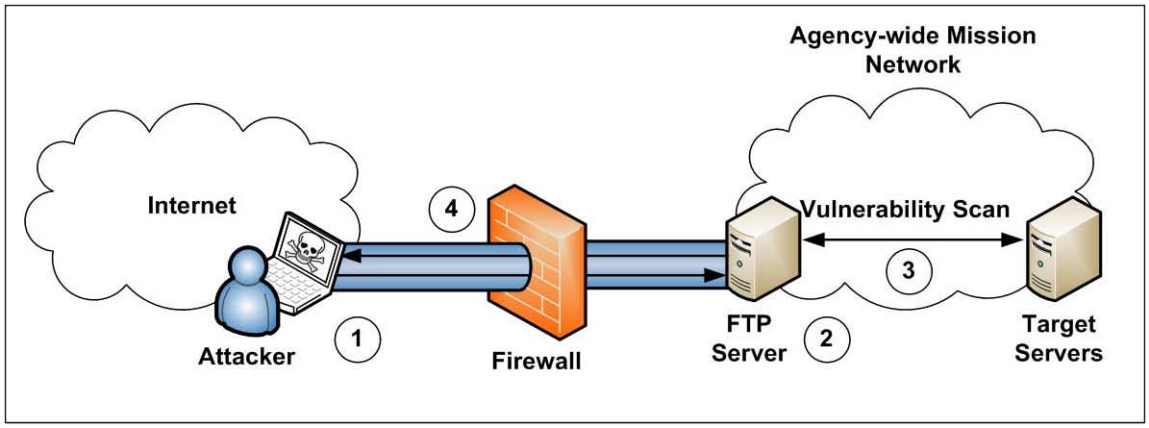

Table 1 shows the results of our vulnerability tests for the six NASA projects we evaluated. Specifically, it shows the number of Internet-accessible servers with high-risk vulnerabilities and the total number of servers with high-risk vulnerabilities. We also detected medium- and low-risk vulnerabilities and immediately provided the complete results of our tests to NASA IT security staff. NASA has since remediated all the high-risk vulnerabilities we detected. As the table shows, three of the projects and six computer servers had high-risk vulnerabilities that could allow an Internet-based attacker to take control of the computers or render them unavailable. We also found high-risk vulnerabilities on other computers that were part of these six projects.

[6] File transfer protocol is a network protocol commonly used on the Internet to copy files from one computer to another. An FTP bounce attack exploits the FTP protocol when an attacker is able to use the PORT command to request access to ports indirectly through the use of the victim machine as a middle-man for the request.

Table 1. Vulnerability Assessment Results		
Project	Number of Internet-Accessible Servers with High-Risk Vulnerabilities	Number of Servers with High-Risk Vulnerabilities
1	0	2
2	0	0
3	0	2
4	2	2
5	3	5
6	1	1
Total	**6**	**12**

Once an attacker has exploited a vulnerability on an Internet-accessible computer, the attacker could use the compromised computer as a means to exploit vulnerabilities on other mission network computers. For example, had the bounce attack vulnerability been exploited, a cybercriminal could have significantly disrupted NASA's space flight operations and stolen sensitive data.

Problems with Server Configurations Exposed Sensitive Data

We also found that servers associated with the six projects we reviewed were not securely configured and, as a result, sensitive data such as encryption keys, encrypted passwords, and user account lists were exposed to potential attackers. These data are sensitive and can be used to gain unauthorized access to NASA's Agency-wide mission network. For example, an attacker can use encryption keys to bypass security controls and remotely access a mission network server.[7] Although encrypting passwords prevents the true password from being disclosed in a legible form, an attacker can use one of the many tools available on the Internet to decipher the password through a technique called brute-forcing.[8] After cracking the password, the attacker can then bypass the login mechanism on the related server's password-protected website and gain access to NASA's Agency-wide mission network. Finally, one server we reviewed disclosed sensitive account data for all its authorized users. This information could be used by attackers for phishing or sending Agency personnel e-mails containing malicious code to their official NASA e-mail accounts. When the recipient accessed the e-mail, their computer and any sensitive data on it could be compromised.

[7] The encryption keys are files used as part of the authentication process for tunneling into an internal network using a VPN (virtual private network) to remotely administer computer servers in the network.

[8] Brute-force password cracking is a technique that involves an automated script or program that attempts every possible password combination or uses a dictionary of words until the encrypted password is discovered.

NASA Needs to Conduct an Agency-Wide IT Security Risk Assessment

Although NASA regularly conducts risk assessments of individual IT systems, the Agency has never completed an Agency-wide risk assessment for its portfolio of IT assets. Agency-wide risk assessments are important because they help ensure that all threats and vulnerabilities are identified and that the greatest risks are promptly addressed. In our judgment, the deficiencies noted above occurred because NASA (1) was unaware of critical risks to its Agency-wide mission network that a comprehensive risk assessment would have brought to light and (2) had not implemented an agreed-upon recommendation to establish an IT security oversight program to ensure that Agency mission networks were adequately protected. As a result, NASA's Agency-wide mission network was vulnerable to a variety of cyber attacks with the potential for devastating adverse effects on the mission operations the network supports. Until NASA improves its IT security practices by completing a comprehensive IT security risk assessment and implementing our previous recommendation to establish an IT security oversight program, the Agency is vulnerable to computer incidents that could have a severe to catastrophic adverse effect on Agency assets, operations, or personnel.

Recommendations, Management's Response, and Evaluation of Management's Response

To strengthen the Agency's IT security program, we urged NASA to expedite implementation of our May 2010 recommendation to establish an IT security oversight program for NASA's Agency-wide mission network. We also recommended that NASA Mission Directorates take the following actions:

Recommendation 1. Immediately identify Internet-accessible computers on their mission computer networks and take prompt action to mitigate identified risks.

Recommendation 2. Add as a security control continuous monitoring of their mission computer networks for Internet-accessible computers and take prompt action to mitigate identified risks.

Management's Response. The NASA CIO and Mission Directorates combined Recommendations 1 and 2 and stated that by September 30, 2011, the CIO will work with the Mission Directorates and Centers to develop a comprehensive approach to ensure that Internet-accessible computers on NASA's mission networks are routinely identified, vulnerabilities are continually evaluated, and risks are promptly mitigated. NASA's proposed corrective action is an Agency-wide solution and will include analyses of the root cause or causes underlying the findings in this and prior audits; identification of short-term steps that NASA will take to address the audit findings; identification of long-term initiatives to address any identified root cause; and identification of the costs and

resources, tools, procedures, and oversight needed to implement the plan, along with specific milestones and assignments of responsibility and methods for accountability.

Evaluation of Management's Response. We consider the CIO and Mission Directorate proposed actions to be responsive to our recommendations. Further, we commend NASA for extending the corrective actions beyond NASA's mission networks. The recommendations are resolved and will be closed upon verification that the proposed actions have been completed.

The CIO also requested that we reevaluate the security of Internet-accessible computers on NASA's mission networks within 1 year of the development of NASA's remediation plan. We agreed and plan to perform a vulnerability assessment of NASA's mission networks in October 2012 to evaluate the security status of the Agency's Internet-accessible computers.

Finally, we recommended that NASA's Chief Information Officer in conjunction with the Mission Directorates:

Recommendation 3. Conduct an Agency-wide IT security risk assessment of NASA's mission-related networks and systems in accordance with Federal guidelines and industry best practices.

Management's Response. The CIO and Mission Directorates concurred with our recommendation, stating that NASA will develop and implement a strategy for conducting such a risk assessment with the goals of (1) providing an overall view of the Agency's information security risk posture and effectiveness of ongoing information security initiatives, particularly on NASA's mission-related networks and systems, and (2) producing actionable recommendations for improving information security, prioritized by level of risk to the Agency, by August 31, 2011.

Evaluation of Management's Response. We consider the proposed actions to be responsive to our recommendation. Therefore, the recommendation is resolved and will be closed upon verification that the proposed actions have been completed.

APPENDIX A

Scope and Methodology

We performed our audit from July through February 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform our work 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.

To evaluate processes NASA used to control the flow of network traffic between the Internet and systems on NASA's Agency-wide mission network, we inspected configurations of the firewalls and network gears that control network traffic between the Internet and agency-wide mission network.

To identify Internet-accessible servers on 100 percent of the Agency-wide mission network, we used Nmap, a widely used software program, that can be used to discover IT assets that are accessible from the Internet. Based on the results of Nmap scans, we identified eight mission projects (two of which were decommissioned prior to the completion of our audit fieldwork) that had computer servers that were accessible from the Internet. We selected these projects for detailed review.

Specifically, we assessed whether NASA has effective processes in place to

- protect internal IT assets from external threats,
- resume post-disaster operations, and
- identify and remediate technical vulnerabilities.

We interviewed NASA and contractor staff responsible for the different areas for each project reviewed. We evaluated processes, controls, and tools they used to secure their IT mission assets and mitigate risk. We conducted vulnerability assessments on each of the six IT projects identified to assess NASA's ability to mitigate technical vulnerabilities. Additionally, we inspected and validated the configurations of the devices that control the flow of network traffic between the Internet and NASA's mission projects against NASA's recommended configurations.

To evaluate processes NASA used for contingency planning for the Agency-wide mission network, we assessed whether there are effective processes in place to not only restore the network following a disruption but also to maintain network operations throughout the occurrence of a disaster. We also developed questionnaires to interview NASA and

contractor staff responsible for the restoration of the Agency-wide mission network. We inspected the contingency plans and contingency plan tests for the Agency-wide mission network.

Use of Computer-Processed Data. We relied on data produced from a software program to perform discovery scans on the Agency-wide mission network. We used Nmap, a widely accepted open source port scanner, to determine what hosts (computers) are active and which ports on these computers are open or may be open and available on a given network and what services and applications those hosts are offering. We validated the data produced by Nmap by manually connecting to the hosts identified by Nmap as open.

We also relied on data produced from a software program to perform vulnerability tests on samples of mission projects connected to the Agency-wide mission network. We used NESSUS®, a commercial network-based vulnerability scanner, to test computers for technical vulnerabilities. We did not validate the data produced by NESSUS® because NESSUS® is widely accepted as a reliable source for providing information related to the presence of technical vulnerabilities in information systems.

Review of Internal Controls

We reviewed internal controls related to the flow of network traffic between the Internet and systems on NASA's Agency-wide mission network and contingency planning audit objectives. These included determining whether NASA has policies and procedures in place for performing risk assessments, configuration and vulnerability management, and contingency planning.

Prior Coverage

During the last 5 years, the NASA Office of Inspector General (OIG) and the Government Accountability Office (GAO) have issued two reports of particular relevance to the subject of this report. Unrestricted reports can be accessed over the Internet at http://oig.nasa.gov/audits/reports/FY11 (NASA OIG) and http://www.gao.gov (GAO).

NASA Office of Inspector General

"Review of the Information Technology Security of [a NASA Computer Network]" (IG-10-013, May 13, 2010).

Government Accountability Office

"NASA Needs to Remedy Vulnerabilities in Key Networks" (GAO-10-4, October 15, 2009)

MANAGEMENT COMMENTS

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

Reply to Attn of: Office of Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Response to OIG Draft Audit Report, "Inadequate Security Practices Expose Key NASA Network to Cyber Attack" (Assignment No. A-10-011-00)

The NASA Chief Information Officer (CIO) is pleased to provide the following consolidated Agency response, which was developed in cooperation with the NASA Mission Directorates, regarding the subject draft report for Assignment No. A-10-011-00. This response addresses all three of the Office of Inspector General (OIG) recommendations for improving the security of Internet-accessible computers on NASA mission networks. In addition, we request that the OIG consider merging two of the recommendations. We have provided suggested wording for a consolidated recommendation below.

OIG Recommendations for Corrective Action:

Recommendation 1: *NASA Mission Directorates should immediately identify Internet-accessible computers on their mission computer networks and take prompt action to mitigate identified risks.*

Recommendation 2: *NASA Mission Directorates should add as a security control continuous monitoring of their mission computer networks for Internet-accessible computers and take prompt action to mitigate identified risks.*

NASA Management Response: Commensurate with discussion with the OIG, NASA requests that the OIG consider consolidating Recommendations 1 and 2. We believe that any effective response must be developed and implemented across the enterprise and must include actions to address the identified concerns in both the short term and the long term. We therefore suggest the OIG replace these existing recommendations with a single, new recommendation with wording similar to:

> "The NASA CIO, in collaboration with the Mission Directorates and NASA Centers, should develop and implement a plan to ensure that: a) Internet-accessible computers on NASA's mission computer networks are routinely identified, b) vulnerabilities on

Internet-accessible computers are continuously evaluated, and c) identified risks are promptly mitigated."

NASA's response to such a consolidated recommendation would be as follows:

Concur. The NASA CIO will work with the Mission Directorates and Centers to develop a comprehensive approach to ensure that Internet-accessible computers on NASA's mission networks are routinely identified, vulnerabilities are continually evaluated, and risks are promptly mitigated. In addition, we will ensure that the above procedures will be applied across the entire enterprise.

Although this audit only evaluated computers that are part of NASA's mission networks, we believe that the findings apply across NASA and that our response must encompass the entire enterprise. NASA's plan will include the following elements:

- Analysis of the root cause or causes underlying the findings in this and prior audits. We will evaluate the vulnerabilities identified in this audit and in other activities to determine how they came about and why, in each case, they were not found, or not mitigated promptly. For example, we will examine whether vulnerability scans were performed by the relevant organizations, whether scan results were available to and used by system administrators, and whether existing scanning capabilities are sufficient, along with other prudent measures.

- Identification of short-term steps that NASA will take to address the audit findings. For example, NASA is currently conducting Agency-wide Web application vulnerability scans to identify NASA Web applications that are accessible from the Internet and vulnerabilities in these applications. The results of this scan will be used to help application owners mitigate vulnerabilities in mission and non-mission applications and to establish a regular scanning and followup activity. Also, NASA will consider the feasibility of providing additional scanning tools, procedures, and guidance to systems owners, as an Agency capability or service, so that technical staff can be more proactive in identifying and mitigating vulnerabilities.

- Identification of long-term initiatives to address the identified root cause(s). Some possible actions include:

    - NASA may expand its capability to collect data from all vulnerability scans, using multiple scanning tools, and to improve the availability of this data to systems owners so they can more effectively track vulnerabilities and mitigations on their systems on a real-time basis.
    - NASA may institute an external network vulnerability scanning activity that regularly identifies NASA computers that are accessible from the Internet. This information could be used to focus remediation efforts on systems with the greatest risk of exposure.

- Identification of the costs and resources, tools, procedures, and oversight needed to implement the plan, along with specific milestones and assignments of responsibility and methods for accountability.

Management Corrective Action Date: A strategy to ensure the development of an implementation plan to continuously identify and mitigate vulnerabilities on Internet-accessible computers will be developed by September 30, 2011.

Recommendation 3: *NASA's Chief Information Officer, in conjunction with the Mission Directorates, should conduct an Agency-wide IT security risk assessment of NASA's mission-related networks and systems in accordance with Federal guidelines and industry best practices.*

NASA Management Response: Concur. Although risk assessments of individual information systems are regularly conducted, NASA management strongly agrees that only an Agency-wide security risk assessment can provide insight into risks that are systemic or widespread across the enterprise. NASA will, therefore, develop and implement a strategy for conducting such a risk assessment, with the goals of: 1) providing an overall view of the Agency's information security risk posture and effectiveness of ongoing information security initiatives, particularly on NASA's mission-related networks and systems, and 2) producing actionable recommendations for improving information security, prioritized by level of risk to the Agency.

The NASA CIO, working with several NASA Centers and Mission Directorates, has already begun developing goals, tools, and procedures for conducting an Agency-wide information security risk assessment. Because of the dispersed nature of NASA's systems and information security resources, the assessment will likely be conducted by staff local to each NASA Center. However, the assessment will utilize a consistent and standardized methodology to evaluate compliance with Federal and Agency information security standards and directives, and will be overseen by Agency-level personnel. Local data will be aggregated to ensure a comprehensive enterprise-wide result. Lessons learned and best practices will be provided back to Mission Directorate and Center management and staff.

Management Corrective Action Date: NASA will complete the strategy for conducting an Agency-wide information security risk assessment and begin a pilot assessment at one NASA Center, using the standard methodology, by August 31, 2011.

As noted in the OIG's report, NASA has remediated all the high-risk vulnerabilities detected during this audit. NASA management is committed to protecting the Agency's computers and networks from Internet-based attacks and appreciates the OIG's efforts in this area. To verify the effectiveness of NASA's strategy for identifying and addressing vulnerabilities, we request that the OIG re-evaluate the security of Internet-accessible computers on NASA's mission networks in one year from the date the remediation plan is implemented.

Any questions concerning this memorandum may be directed to Valarie Burks, Deputy Chief Information Officer for Information Technology Security, at 202-358-3716 or valarie.j.burks@nasa.gov.

Linda Y. Cureton

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief of Staff
Chief Information Officer
Associate Administrator Aeronautics Research Mission Directorate
Associate Administrator Science Mission Directorate
Associate Administrator Exploration Systems Mission Directorate
Associate Administrator Space Operations Mission Directorate

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, NASA Financial Management, Office of Financial Management and Assurance
    Director, NASA Issues, 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 Organization, Efficiency, and Financial Management
House Committee on Science, Space, and Technology
    Subcommittee on Investigations and Oversight
    Subcommittee on Space and Aeronautics

Major Contributors to the Report:

Wen Song, Director, Information Technology Directorate
Jefferson Gilkeson, Project Manager
Eric Jeanmaire, Auditor
Morgan Reynolds, Auditor

MARCH 28, 2011

REPORT No. IG-11-017

OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit http://oig.nasa.gov/audits/reports/FY11/ 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.