SEPTEMBER 9, 2010

AUDIT REPORT

OFFICE OF AUDITS

STATUS OF NASA'S TRANSITION TO INTERNET PROTOCOL VERSION 6 (IPV6)

OFFICE OF INSPECTOR GENERAL

National Aeronautics and
Space Administration

REPORT NO. IG-10-022 (ASSIGNMENT NO. A-09-017-00)

Final report released by:

Paul K. Martin
Inspector General

Acronyms

ARPANET	Advanced Research Projects Agency Network
CIO	Chief Information Officer
DNS	Domain Name System
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IT	Information Technology
LAN	Local Area Network
NISN	NASA Integrated Services Network
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget

OVERVIEW

STATUS OF NASA'S TRANSITION TO INTERNET PROTOCOL VERSION 6 (IPV6)

The Issue

Throughout its history, NASA has been at the forefront of Federal Government information technology (IT) innovation. This includes early adoption of leading-edge technologies such as cloud computing. Moreover, NASA is a leader in using the Internet to communicate the importance of its programs to the public, and its Web environment has evolved to become a cornerstone of the Agency's business processes.

Internet protocol (IP) is a communications protocol, or set of standard rules, used to transmit data over the Internet. The most widely used protocol supporting the Internet today is IP Version 4 (IPv4), which provides about 4.3 billion IP addresses for use worldwide. Over the last 6 years, the demand for IP addresses has been steadily accelerating due to the expansion of Internet usage worldwide and the advent of Internet-capable devices such as mobile phones, car navigation systems, home appliances, and industrial equipment. In May 2009, the Architecture and Infrastructure Committee of the Federal Chief Information Officers Council reported that the IPv4 pool of addresses would be exhausted by 2011 or 2012. In anticipation of the exhaustion of IPv4 addresses, in late 1990 the Internet Engineering Task Force selected IP Version 6 (IPv6) as the successor to IPv4. IPv6 allows for an exponentially larger pool of addresses and is seen as the only practical and readily available long-term solution to the impending exhaustion of IPv4 addresses.[1] However, without adaptations, communications between devices using IPv4 and IPv6 are not compatible. In addition, successful transition to the new system is complex and requires detailed planning.

In 2005, the Office of Management and Budget (OMB) began issuing guidance to Federal agencies relating to the transition to IPv6 so that they would be in a position to

- take advantage of the expanded IP address space and embrace future-oriented networking capabilities, such as converged communications, IP-aware medical devices, and remote sensors and

[1] IPv4 allows for approximately 4.3×10^9 addresses. IPv6 allows for approximately 3.4×10^{38} addresses.

- lead by example in U.S. enterprise IPv6 transformation.[2]

The "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government," which defines the Federal Government's IPv6 plan and builds on requirements set forth in OMB's guidance (M-05-22), was released in May 2009. Our objective in this audit was to evaluate the status of NASA's efforts to plan for IPv6 transition and integration to ensure appropriate implementation. Details of the audit's scope and methodology are in Appendix A.

Results

NASA has taken preliminary steps to meet OMB requirements for IPv6 transition and integration, including assigning a lead official in November 2005 to coordinate NASA's efforts, developing inventories of IP-aware devices and an impact analysis, and in June 2008 demonstrating IPv6 capability of one NASA network. However, as of March 2010 the Agency did not have an updated or complete IPv6 transition plan as required by OMB. This occurred, in part, because the Agency has ample IPv4 addresses to meet its current and future requirements and because the individual who was leading the IPv6 transition effort left NASA in November 2006 and no one has been assigned to replace him. As a result, the Agency does not have adequate assurance that it has considered all necessary transition elements or that the security and interoperability of its systems will not be affected as other Government agencies and entities transition to IPv6. Accordingly, even if NASA can continue meeting its communication needs using IPv4 addresses, it should ensure that its systems are prepared as other Internet users transition to IPv6.

Management Action

We recommended that the NASA Chief Information Officer appoint an Agency official to lead and reinvigorate its IPv6 transition planning efforts and ensure that it implements key OMB planning requirements. In response to a draft of this report, the Chief Information Officer concurred with our recommendation and stated that her office will appoint an IPv6 lead to develop an IPv6 transition plan as required by OMB by March 31, 2011 (see NASA's comments in Appendix F).

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

[2] From "Federal Government Transition Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6), Frequently Asked Questions," February 15, 2006, available online at http://www.cio.gov/documents/IPv6_FAQs.pdf (accessed May 19, 2010). This document provides clarification to OMB Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005, which advised agencies to take specific actions to ensure an orderly and secure transition to IPv6.

CONTENTS

INTRODUCTION

Background

The Internet is a network consisting of millions of private, public, academic, business, and Government networks of local to global scope that are linked by a broad array of electronic and optical networking technologies. NASA's Internet environment is a mechanism for providing information about NASA to the public and a cornerstone of the Agency's business processes. Recently, the NASA Chief Information Officer (CIO) stated: "Information technology at NASA has been, and will remain, a critical enabling capability for the Agency, whether in NASA's main themes of Space Flight, Exploration, Science, Aeronautics, and Mission Support, or any iteration thereof for the foreseeable future." This linkage between information technology (IT) and various aspects of the Agency's mission underscores the importance of IT across the Agency.

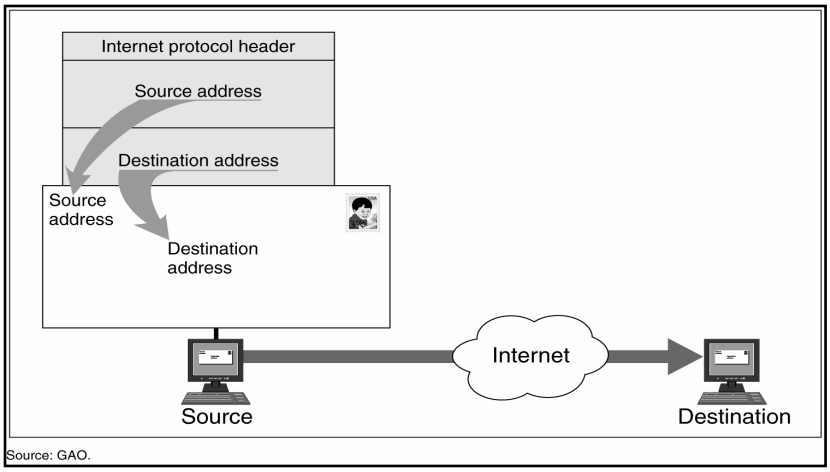
The Internet began when a small research team, including the Defense Department's Advanced Research Projects Agency and the Massachusetts Institute of Technology, created the Advanced Research Projects Agency Network (ARPANET), the world's first operational packet-switching network. Packet switching, the rapid store-and-forward networking design, divides messages up into packets.[3] Routing decisions are made per packet, making it possible for separate physical computer networks to form one logical network.

The communications protocol, or set of standard rules, used to transmit data over the Internet has evolved through the years. The Network Control Program was developed to provide connections between processes running on different ARPANET host computers. Application services, like e-mail or file transfer, were built on top of the Network Control Program to handle connections to other host computers. In 1983, Transmission Control Protocol and the Internet protocol (IP) replaced the Network Control Program and made possible the connection of almost any computer network to ARPANET.

Addressing is a basic IP capability. The Internet, including NASA's Internet environment, currently relies on IP Version 4 (IPv4) addresses to uniquely identify devices on the network so that information can be transmitted from one device, such as a computer, to another as illustrated in Figure 1.

[3] A packet is a formatted unit of data, including source and destination addresses, which can be carried over the Internet.

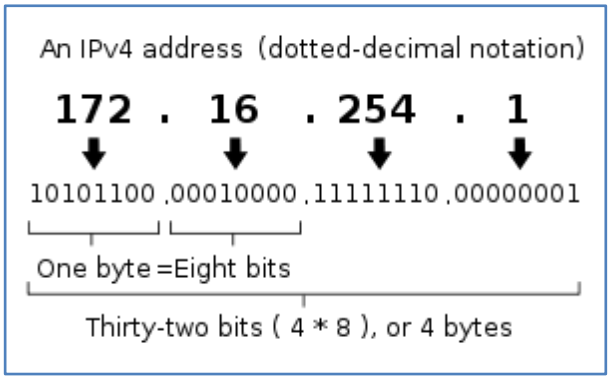
Figure 1. IP Source/Destination Example



Source: GAO Report, "Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks" (GAO-05-471, May 20, 2005).

IPv4 provides for a finite number of addresses ranging from 0.0.0.0 to 255.255.255.255. See Figure 2 for an illustration of an IPv4 address.

Figure 2. An Illustration of an IPv4 Address



Source: *TCP/IP Fundamentals for Microsoft Windows* (2006).

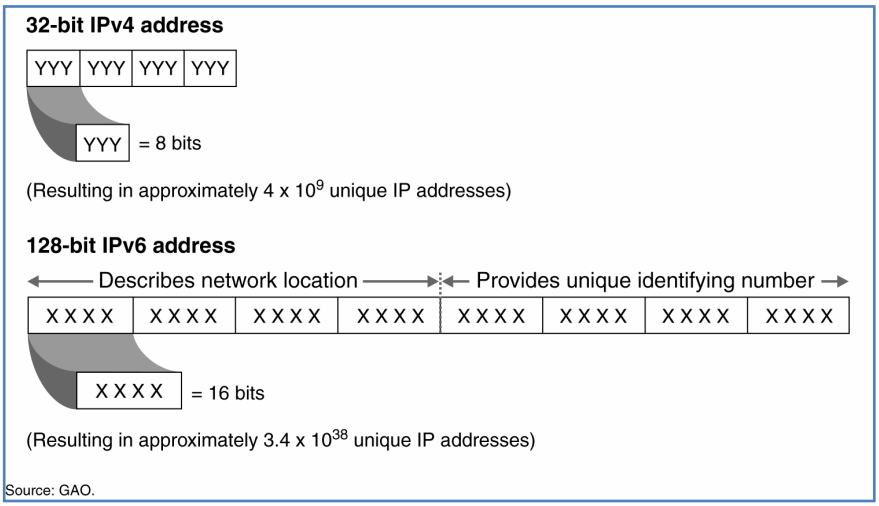
Due to rapid population growth, mass-market broadband deployment, applications such as Voice over Internet Protocol, the addition of network addressable devices such as mobile phones and sensors to the Internet, and continuing cost reductions in technology that have brought the Internet to large populations in developing economies, demand for IPv4 addresses has been steadily accelerating. In light of this rapid worldwide growth, the Architecture and Infrastructure Committee of the Federal Chief Information Officers Council reported in May 2009 that the pool of IPv4 addresses would be exhausted by 2011 or 2012.

Foreseeing the eventual depletion of IPv4 addresses, the Internet technical community took action to manage IPv4 addresses as a finite resource and to plan for the future by

developing a new addressing protocol, IP Version 6 (IPv6), also referred to as IP Next Generation (IPng).[4]

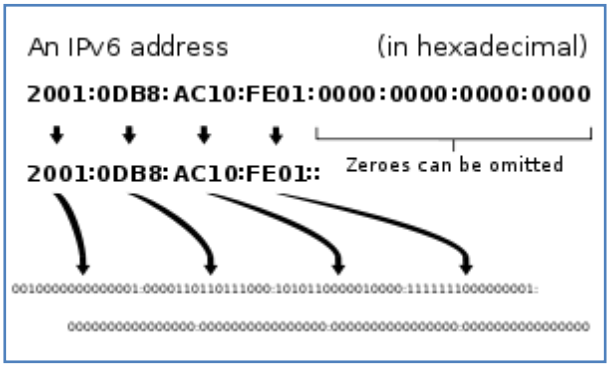
While IPv4 allows for 2^{32} or 4,294,967,296 possible addresses, IPv6 allows for 2^{128} or 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses (see Figure 3). An example of an IPv6 address is 3FFE:2900:D005:0000:02AA:00FF:FE28:9C5A. See Figure 4 for an illustration of an IPv6 address.

Figure 3. Comparison of IPv4 and IPv6 Addresses



Source: GAO Report, "Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks" (GAO-05-471, May 20, 2005).

Figure 4. An Illustration of an IPv6 Address



Source: *TCP/IP Fundamentals for Microsoft Windows* (2006).

[4] The Internet Assigned Numbers Authority assigned version number 6 to IPng since version 5 was reserved for an experimental protocol, "Internet Stream Protocol, Version 2 (ST2)" (see Appendix B for details).

Several organizations manage and distribute IPv4 and IPv6 addresses:

- The Internet Assigned Numbers Authority coordinates the global pool of IPv4 and IPv6 addresses and provides them to five Regional Internet Registries. The Internet Assigned Numbers Authority is one of the Internet's oldest institutions, dating back to the 1970s. Today, the Internet Assigned Numbers Authority is operated by the Internet Corporation for Assigned Names and Numbers.

- The Regional Internet Registries manage and distribute public IPv4 and IPv6 addresses within their respective regions. The five Regional Internet Registries are the African Network Information Center, Asia Pacific Network Information Centre, American Registry for Internet Numbers, Latin American and Caribbean Internet Addresses Registry, and Réseaux IP Européens Network Coordination Centre.

- The American Registry for Internet Numbers, a Regional Internet Registry, is a non-profit membership organization established for the administration and distribution of IP addresses in the United States, Canada, and many Caribbean and North Atlantic islands.

NASA officials estimate that the American Registry for Internet Numbers assigned about 4 million IPv4 addresses to NASA. In March 2010, NASA was using approximately 203,000 IPv4 addresses and holding in reserve approximately 434,000 IPv4 addresses for network design, network configuration, and other needs. As a result, with more than 3.3 million unused IPv4 addresses, NASA officials said they do not believe that the Agency will exhaust its supply of IPv4 addresses or need to begin using IPv6 addresses in the near future.

However, the Internet Assigned Numbers Authority and the American Registry for Internet Numbers have warned that many new Internet computing devices will have IPv6 addresses by the end of 2011. Therefore, it is vital that the networks used to transfer data over the Internet, including NASA's systems, are capable of supporting IPv6.

OMB Requirements and Guidance. Office of Management and Budget (OMB) Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005, was OMB's first policy memorandum to agencies to ensure an orderly and secure transition to IPv6. The OMB policy included the following deadlines for required agency actions:[5]

November 15, 2005

- Assign an official to lead and coordinate agency planning efforts for IPv6 transition.
- Complete an inventory of existing routers, switches, and hardware firewalls (IP-aware hardware devices in the agency's infrastructure, also called the network backbone).

February 2006

- Using guidance to be issued by the Architecture and Infrastructure Committee of the Federal Chief Information Officers Council,[6] address each of the actions identified in Attachment C of the OMB policy (including conducting a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements) and provide the completed IPv6 transition plan as part of the agency's enterprise architecture submission to OMB.

June 30, 2006

- Complete an inventory of existing IP-aware devices and technologies that are components of the agency infrastructure but were not included in the first inventory.
- Complete an impact analysis of fiscal and operational impacts and risks related to the transition to IPv6.

June 30, 2008

- All agency infrastructures must be capable of successfully passing IPv6 data traffic and supporting IPv6 addresses. Agency networks also must be able to communicate with this infrastructure.

In addition, the OMB policy recommended that all new IT procurements be IPv6 compliant – that is, able to receive, process, and transmit or forward (as appropriate)

[5] See M-05-22 in Appendix E for the original language of the required actions. We reworded the requirements in this report for clarity based on information subsequently issued by OMB and the Architecture and Infrastructure Committee of the Federal Chief Information Officers Council.

[6] The Architecture and Infrastructure Committee of the Federal Chief Information Officers Council issued "IPv6 Transition Guidance" in February 2006. In May 2009, it issued "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government."

packets of IPv6 data – to the maximum extent practicable to avoid additional costs in the future. The OMB memorandum also recommended that agency products or systems be able to interoperate with systems using either the IPv4 or IPv6 addressing convention.

To address the many questions concerning IPv6 generated by its August 2005 policy, in February 2006, OMB published "Federal Government Transition Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6), Frequently Asked Questions."[7] The document addressed questions about the scope of agencies' IPv6 efforts, the inventory submissions, and the transition plan each agency was to submit to OMB in February 2006.

In May 2009, OMB released the "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government" (the IPv6 Planning Guide), which sets out the Federal Government's movement toward adopting IPv6 and builds on the requirements in the August 2005 OMB policy. In OMB's memorandum announcing the release of the Planning Guide, OMB recommends that agencies

- use their enterprise architecture and capital planning activities to plan for the deployment of IPv6-enabled[8] network services, show how they intend to use these services to power IPv6-enabled applications, commit to specific measureable improvements in agency performance, and reflect these improvements in their investment proposals;
- leverage the guidance milestones provided in the IPv6 Planning Guide to develop an effective transition plan;
- set up test laboratories and prototype networks to acquire IPv6 experience and expertise; and
- deploy secure IPv6-enabled network services during regular technology upgrade cycles.

Objective

Our objective was to evaluate NASA's efforts and plans for IPv6 transition and integration. We reviewed the Agency's implementation of planning requirements for IPv6 transition in accordance with the August 2005 OMB policy and the status of NASA's progress with IPv6 integration since the May 2009 release of the IPv6 Planning Guide. We also evaluated the effectiveness of NASA's IT security controls for devices configured to enable IPv6. See Appendix A for details of the audit's scope and methodology, our review of internal controls, and a list of prior coverage. See Appendix B for a glossary of selected terms.

[7] Available online at http://www.cio.gov/documents/IPv6_FAQs.pdf (accessed May 19, 2010).

[8] OMB defines "IPv6 enabled" as meaning that IPv6 is being used (see Appendix B).

TRANSITION PLANNING NEEDS IMPROVEMENT

NASA took preliminary steps in 2004–2010 for IPv6 transition and integration that were consistent with the OMB guidance. However, since that time NASA has not continued with active IPv6 planning and has not fully implemented OMB's planning requirements for transition to IPv6. Without adequate planning, NASA may encounter interoperability and security challenges when other parts of the Federal Government and the worldwide IT community transition to IPv6. As a result, NASA could find itself unprepared to securely communicate using IPv6.

NASA Has Taken Preliminary Steps for Transition and Integration

NASA has taken preliminary steps to meet OMB requirements for IPv6 transition and recommendations for integration that included the following actions:

Assigning a Lead. According to officials in the NASA Office of the Chief Information Officer (OCIO), in 2005 the NASA Deputy CIO was designated as the official to lead and coordinate planning for IPv6 transition. The Deputy CIO was actively involved with the IPv6 working group sponsored by the Architecture and Infrastructure Committee of the Federal Chief Information Officers Council. However, since he left the Agency in November 2006, no other official has been assigned to lead NASA's IPv6 transition effort.

Developing Inventories and an Impact Analysis. According to OMB, all Federal agencies, including NASA, were required to meet the November 15, 2005, deadline for completing an "inventory of existing routers, switches, and hardware firewalls" and the June 30, 2006, deadline for completing an "inventory of existing IP compliant devices and technologies not captured in first inventory." OMB also required agencies to complete an "impact analysis of fiscal and operational impacts and risks" related to IPv6 transition by June 30, 2006. We were unable to assess NASA's inventories or impact analysis because the Agency could not provide us with copies of these documents.[9] However, we were able to verify that NASA OCIO had issued two data calls to the NASA Centers requesting the inventory information required by OMB, and we confirmed that the inventory information requested was consistent with OMB requirements. We also confirmed that six Centers[10] provided the requested information

[9] NASA OCIO did not retain copies of the submissions and was unable to obtain copies from OMB.

[10] Ames Research Center, Dryden Flight Research Center, Glenn Research Center, Kennedy Space Center, Marshall Space Flight Center, and Stennis Space Center.

and that two Centers[11] prepared impact analyses. However, without reviewing NASA's submissions, we could not assess their quality or completeness.

Amending the Federal Register. In August 2006, NASA, the General Services Administration, and the Department of Defense published a proposed rule in the Federal Register to amend the Federal Acquisition Regulation "to ensure that all new IT acquisitions using Internet Protocol are IPv6 compliant." This proposed rule was finalized on December 10, 2009. NASA OCIO officials stated that all NASA Centers were notified of the final rule and that IT contracts created after that date should be in compliance.

Demonstrating Capability. NASA developed an IPv6 Demonstration Plan[12] and, in June 2008, successfully demonstrated IPv6 capability on the NASA Integrated Services Network (NISN) corporate backbone through the core Standard IP (SIP) routers. NASA determined the IPv6 accessibility of 12 core routers by using a utility to send a data packet to 12 IPv6 addresses and successfully receiving a reply. See Appendix C for the specific guidance we used to determine NASA's compliance with this requirement.

We also reviewed the certification and accreditation documentation and a vulnerability scan for the NISN corporate backbone. We found that security controls were generally effective for the 12 core routers that are IPv6-enabled.

Acquiring IPv6 Experience. We found that NISN engineers tested IPv6 functionality on the NASA Prototyping Network, a network laboratory environment used to test new technologies, protocols, and pre-operational equipment before deployment to the production network. For example, one test performed in 2004 on the NASA Prototyping Network showed that IPv6 would work with IPv4 using the dual-stack transition mechanism,[13] in which the network was configured to support IPv4 and IPv6 concurrently. Tests were conducted using network utilities common to IPv4 and IPv6. NISN engineers also used the NASA Prototyping Network to test security of the IPv6 control plane – the services, settings, and data streams that support the dynamic operation and traffic handling of routers – with the network running IPv6 (IPv6 enabled).[14]

These preliminary steps, while providing some assurance that NASA can adapt to the IPv6 transition, are not sufficient to ensure that NASA will be able to continue to effectively communicate over the Internet with the public, other Government agencies, and its worldwide partners when they transition to IPv6. The 2004 test noted that further

[11] Kennedy Space Center and Marshall Space Flight Center.

[12] "National Aeronautics and Space Administration (NASA) Agencywide IPv6 - Demonstration Plan," June 6, 2008.

[13] See Appendix B's entries for dual-stack and transition mechanism.

[14] The control plane supports the dynamic state of the router: the routing tables, access logs, traffic statistics, and cryptographic associations. If an attacker can inject control plane information into your router, then the attacker can exercise some control over packet forwarding, expose traffic to interception, and prevent effective communication among networks and hosts.

testing was needed for interoperability (as discussed on page 10), which has not yet been conducted. In addition, although the NISN corporate backbone was tested, NASA has not assessed whether testing is needed on other systems, such as mission systems.

IPv6 Transition Efforts Have Stalled

While NASA has taken a number of preliminary steps for transitioning to IPv6, its efforts have stalled partly because the individual assigned to lead the Agency's transition effort left NASA in November 2006 and another official has yet to be assigned. In addition, NASA has no sense of urgency on this issue because, as previously discussed, the Agency has ample IPv4 addresses available to meet its current and future requirements and therefore does not anticipate that it will be using IPv6 addresses in the foreseeable future. We believe NASA needs to reinvigorate its IPv6 planning efforts because, regardless of NASA's ample supply of IPv4 addresses, other users are beginning to use IPv6 addresses, and the transition to IPv6 is more complex than previous advances in Internet technology and requires detailed planning. At the time of the adoption of IPv4, there were less than 500 hosts connected to the Internet, a relatively small community of technical specialists was involved, and the Internet was operating in a non-commercial environment. By 2008, over 500 million hosts were connected to the Internet and 1.32 billion users had Internet access. These numbers and the associated technical complexities will only continue to increase as Internet users transition to IPv6.

NASA Needs to Improve Its Transition Planning

As of March 2010, NASA did not have an updated or complete IPv6 transition plan as required by OMB. As a result, the Agency does not have adequate assurance that it has considered all elements necessary to achieve a successful transition to IPv6. Among the challenges identified by the Architecture and Infrastructure Committee that agencies should consider is the need to maintain interoperability and security during transition, as well as manage the IPv6 standards and product evolution.

Updated Transition Plan

During our audit, NASA officials provided an IPv6 transition plan that had been in draft since April 2007 and that did not reflect transition elements required by OMB policy. OMB called for agencies to complete their IPv6 transition plans using guidance issued by the Architecture and Infrastructure Committee of the Federal Chief Information Officers Council in February 2006. This guidance outlined 17 elements agencies should consider to ensure all transition elements had been examined (see Appendix D). Although the guidance did not require that agency plans include all of the elements, 11 of the 17 are

required.[15] However, NASA's draft IPv6 transition plan does not include any of the 11 elements, although some of the elements were addressed by NASA's successful demonstration of IPv6 capability on the NISN corporate backbone and by NISN IPv6 testing in 2004, 2005, and 2010. The following paragraphs describe five unaddressed elements that we believe NASA needs to consider to promote an orderly and secure transition to IPv6.

Transition Priorities and Activities. NASA's draft IPv6 transition plan does not identify transition priorities or activities[16] for networks other than the NISN corporate backbone. Rather, the draft plan states only that the Agency's mission networks (e.g., the Integrated Operations Network and the Network Service Assurance Plan network) would be included in the Agency's long-term IPv6 transition strategy.

The 2009 IPv6 Planning Guide identifies priorities to help agencies in their transition:

> External facing eCommerce servers, mail gateways, instant messaging servers, Web servers, and voice over IP gateways hosting portals for remote clients, teleworkers, partner agencies, and group collaboration all have to serve content across the Internet backbone to external hosts. *Because of IPv4 address depletion and its effect on core routing, applications that rely on the Internet core for transport to external hosts should upgrade first to IPv6-capable versions by 2010.*

The IPv6 Planning Guide states that the second wave of upgrades should include host interfaces, such as Web servers and e-mail clients, that will connect to external servers. The final upgrade includes "internal facing systems in an Enterprise LAN [local area network], as these systems can continue to rely on IPv4 NAT [Network Address Translation][17] addresses for some time." Without transition priorities and activities, the Agency cannot determine the impact of the transition or the order in which networks will get funding for upgrade.

Interoperability and Security. NASA's draft IPv6 transition plan does not include a plan for maintenance of interoperability and security during the transition from IPv4 to IPv6. IPv6 transition challenges include maintaining dual IPv4 and IPv6 environments for an extended period, interfacing with partners in various stages of the transition, and managing information security in an environment more vulnerable to threats. The key to a successful IPv6 transition is interoperability with IPv4 hosts and routers already in existence. For IPv6 hosts and routers to interoperate with IPv4 hosts and routers, the IPv6 equipment must have a transition mechanism such as dual-stack or tunneling.[18] One test performed in 2004 on the NASA Prototyping Network concluded that further

[15] The Architecture and Infrastructure Committee's 2009 IPv6 Planning Guide required 11 elements to be included.

[16] Both elements – transition activities and transition priorities – are included in the guidance listed in Appendix D.

[17] See Appendix B for details about network address translation.

[18] A mechanism that allows an IPv6 packet to travel through an IPv4 network (see Appendix B).

testing was needed for the tunneling mechanism: "Until IPv6 has more widespread application support, it will be difficult to deploy IPv6 without some method of tunneling with IPv4."

In addition to interoperability issues, IPv6 introduces new security threats. The National Institute of Standards and Technology (NIST) USGv6 Profile[19] concluded that the "current state of IPv6 security and network protection technologies and operational knowledge lags behind that of IPv4 and the existing Internet." The IPv6 Planning Guide recommends steps for agencies to consider with regard to security, including development of a comprehensive IPv6 security plan and associated IPv6 policies within the IPv6 addressing rollout plan, upgrading network protection devices/tools for IPv6 support, and expanding core and perimeter boundary monitoring to incorporate IPv6 and IPv6-in-IPv4 tunnels. NASA has not completed any of these steps.

IPv6 Standards and Products. A fourth element not addressed in NASA's draft IPv6 transition plan is the use of IPv6 standards and products. While the base set of IPv6 protocols are stable and mature, many of the Internet standards supporting IPv6 features and IPv6 products in development are still evolving. With evolving IPv6 standards, challenges exist with acquiring IPv6-compliant products that will ensure interoperability and security. The NIST USGv6 Profile recommends a technology acquisition profile for common IPv6 devices in U.S. Government IT systems. However, NASA has not decided how to ensure compliance with the NIST USGv6 Profile.

Governance. The fifth element not addressed in NASA's draft IPv6 transition plan is transition governance, including Agency policy and roles and responsibilities. The NIST USGv6 Profile states:

> Beyond being much larger (128bit vs. 32bit), the IPv6 addressing architecture makes for the clear definition of multiple types of addresses (e.g., link-local, global, multicast, anycast) and multiple scopes of addresses (e.g., global, local, link).
>
> Any adoption and deployment of IPv6 requires the development of an addressing plan. There are many significant issues associated with strategies for IPv6 address allocation and assignment.

In addition, the IPv6 Planning Guide recommends a list of specific procedures for IP address management and allocation that includes (a) assessing existing IP address management and allocation governance and procedures and (b) developing and promulgating new/revised IPv6 address management and allocation governance including requirements, guidance, policy, procedures, and reporting. As of May 2010, NASA officials said they were working on but had not finalized an IP addressing plan. As NASA's international partners and others around the world transition to IPv6, NASA

[19] NIST Special Publication 500-267, "A Profile for IPv6 in the U.S. Government – Version 1.0," July 2008.

must have adequate guidance in place to ensure that its network managers can continue to securely meet NASA's needs.

No Lead for Continued Planning

As of March 2010, NASA's IPv6 transition plan had not been updated or completed, primarily because NASA had not reassigned these responsibilities in the nearly 4 years since the last official with responsibility for IPv6 planning left the Agency. NASA officials said they have not assigned a new IPv6 lead because the Agency has more than 3.3 million unused IPv4 addresses and therefore no current need for IPv6.[20]

In our judgment, NASA should make planning for IPv6 transition more of a priority because even if NASA continues to use IPv4 addresses, other Internet users will begin using IPv6 addresses in the near future and NASA must be prepared to ensure the security and interoperability of its systems in this new environment.

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

To ensure that NASA systems are interoperable and secure as Federal Government agencies and other organizations transition to IPv6, we recommended that the NASA CIO assign an IPv6 lead to complete an updated IPv6 transition plan that considers transition elements identified by the Architecture and Infrastructure Committee of the Federal Chief Information Officers Council in the "IPv6 Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government."

Management's Response. The CIO concurred with our recommendation and stated that she will appoint an IPv6 lead by September 30, 2010, to review the OMB requirements and develop a compliant IPv6 transition plan. The CIO stated that this transition plan will be completed by March 31, 2011.

Evaluation of Management's Response. We consider the CIO's 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.

In addition to responding to our recommendation, the CIO suggested a number of minor revisions to the draft report. Specifically, she suggested that we add the word "corporate" to our references to the NISN Backbone, noted an apparent discrepancy in the number of elements discussed under the heading "NASA Needs to Improve Its Transition Planning," questioned whether the report should reference the Space Network and the Ground Network, and clarified an official's title (see Appendix F for the full text of management's comments).

[20] As discussed on page 9, NASA has ample IPv4 addresses to meet its needs.

We used the term "NISN Backbone" in the draft because that was the term used in the certification and accreditation documentation provided to us by NASA. However, we made the change suggested by the CIO for clarification purposes. In addition, although there are only four subheadings in the Transition Planning section, we discuss five elements; two elements, transition priorities and transition activities, are combined in one heading. In response to the CIO's comments, we added a footnote to clarify this point. Finally, we included the Space and Ground Networks in our report because they were referenced in NASA's draft IPv6 transition plan. Based on the clarification from the CIO, we deleted the references to those networks in the final report. We also corrected the official's title, to the Associate CIO for Architecture and Infrastructure.

APPENDIX A

Scope and Methodology

We performed this audit from September 2009 through July 2010 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. We performed our audit at Kennedy Space Center, Marshall Space Flight Center, and NASA Headquarters.

To assess implementation of key planning requirements for IPv6 transition, we reviewed transition and integration requirements and guidelines in the following documents:

- OMB Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005;
- OMB Memorandum, "Release of the Planning Guide/Roadmap toward IPv6 Adoption within the US Government," May 20, 2009;
- Architecture and Infrastructure Committee, Federal Chief Information Officers Council, "IPv6 Transition Guidance," February 2006;
- Architecture and Infrastructure Committee, Federal Chief Information Officers Council, "Demonstration Plan to Support Agency IPv6 Compliance," January 28, 2008; and
- Architecture and Infrastructure Committee, Federal Chief Information Officers Council, "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government," May 2009.

We interviewed personnel from the NASA OCIO, the Marshall Space Flight Center OCIO, the Kennedy Space Center OCIO, and NISN. Officials interviewed included the NASA OCIO Enterprise Architect, the Associate CIO for Architecture and Infrastructure, Marshall's Deputy CIO, Kennedy's Network Engineer, the NISN Service Owner for Corporate Routed Data Service, and the NISN Network Engineer.

NASA OCIO officials could not provide the inventory or impact analysis submitted to OMB in November 2005 and June 2006. NASA OCIO officials stated that the documents had been lost due to changes in personnel, and the officials were unable to obtain copies from OMB. OMB did issue a statement that all agencies had met the

June 2008 deadline. Lacking those documents, we were unable to verify whether NASA's submissions to OMB were complete and accurate.

To identify actions taken to complete inventories and the impact analysis as required by OMB M-05-22, we obtained the following NASA OCIO action registry items with requirements for the Center OCIOs:

- Action Registry EA-12, "Actions for Transition Planning for Agency Internet Version 6 (IPv6)," required Centers to complete the first inventory due to OMB by November 2005. Action Registry EA-12 provided the Centers with a copy of the "IPv6 Transition Checklist" (Attachment A of OMB M-05-22) to complete the first inventory.

- Action Registry EA-25, "Action: IPv6 implementation activities related to enterprise architecture submissions to OMB that are due February 15, 2006," required Centers to complete the "IPv6 Transition Checklist" for all IP devices not captured in the first inventory. Action Registry EA-25 also requested that the Centers provide input for completion of Attachment B, "Impact Analysis," of OMB M-05-22.

- Action Registry EA-29, "Action: IPv6 Transition Planning activities to be completed by June 30, 2006," required Centers to complete the inventories of IP-aware applications and peripherals with dependencies on the network backbone and complete an impact analysis.

To obtain inventory lists submitted to the NASA OCIO, we contacted 10 NASA Center OCIOs: (1) Ames Research Center, (2) Dryden Flight Research Center, (3) Glenn Research Center, (4) Goddard Space Flight Center, (5) the Jet Propulsion Laboratory, (6) Johnson Space Center, (7) Kennedy Space Center, (8) Langley Research Center, (9) Marshall Space Flight Center, and (10) Stennis Space Center. We obtained and reviewed the completed OMB "IPv6 Transition Checklist," which includes inventory reported to the NASA OCIO, from 6 Centers: Ames, Dryden, Glenn, Kennedy, Marshall, and Stennis. These inventories, if unchanged by the NASA OCIO, would have provided the inventory information required for the OMB submissions. Two Centers, Johnson and Goddard, were unable to find a record of their submission; we did not receive a response from the Jet Propulsion Laboratory or Langley.

We also reviewed the following submissions to the NASA OCIO from the OCIOs at Kennedy and Marshall:

- Impact Analysis, "IP Version 6 Transition Initial Draft" (Kennedy).
- Impact Analysis, "Mission Support Network" (Marshall).
- Impact Analysis, "National Space Science Technology Center" (Marshall).
- Impact Analysis, "Huntsville Operations Support Center" (Marshall).

- Impact Analysis, "CIO – LAN [Local Area Network] Technical Refresh" (Marshall).

To assess the status of NASA efforts and plans to move forward with IPv6 integration since OMB announced the release of the IPv6 Planning Guide on May 20, 2009, we interviewed the NASA OCIO Enterprise Architect, the Associate CIO for Architecture and Infrastructure, Marshall's Deputy CIO, Kennedy's Network Engineer, the NISN Service Owner for Corporate Routed Data Service, and the NISN Network Engineer. To determine whether NASA implemented the final rule in the Federal Register to amend the Federal Acquisition Regulation "to ensure that all new IT acquisitions using Internet Protocol are IPv6 compliant," we interviewed the Kennedy Procurement Director. We did not review enterprise architecture or capital planning and investment control activities.

To evaluate the effectiveness of controls and processes for devices configured to enable IPv6, we reviewed the certification and accreditation documentation for the NISN corporate backbone. In November 2009, the NISN Network Engineer identified 12 core routers that had been configured to enable IPv6. These 12 core routers were part of the NISN corporate backbone, which included 381 routers, switches, and servers. SecureInfo Corporation, an independent third-party contractor, certified the NISN corporate backbone in August 2009. We accepted SecureInfo's determination that an adequate level of information system security existed to protect the information processed by the NISN corporate backbone. SecureInfo's certification included a review of controls from NIST Special Publication 800-53, Revision 2, "Recommended Security Controls for Federal Information Systems," and a vulnerability scan using McAfee Foundstone.

Use of Computer-Processed Data. We did not assess the reliability or validity of the data produced by McAfee Foundstone, because it is a widely used tool approved by NASA for vulnerability scanning. In addition, the data's reliability and validity would not impact our conclusions or recommendation.

Review of Internal Controls

We examined controls for ensuring appropriate IPv6 planning as required by OMB. We discussed the control weakness we identified in the Results section of this report. Our recommendation, if implemented, will improve the identified weakness.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) has issued two reports of particular relevance to the subject of this report. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov.

"Internet Protocol Version 6: Federal Government in Early Stages of Transition and Key Challenges Remain" (GAO-06-675, June 30, 2006)

"Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks" (GAO-05-471, May 20, 2005)

GLOSSARY

American Registry for Internet Numbers. A Regional Internet Registry, the American Registry for Internet Numbers is a non-profit membership organization established for the administration and disruption of IP addresses in the United States, Canada, many Caribbean, and North Atlantic islands.
(Source: https://www.arin.net/knowledge/arin_glance.pdf, accessed March 30, 2010)

Backbone. OMB M-05-22 identified "network backbone" as another name for an agency's infrastructure. OMB's IPv6 Frequently Asked Questions (http://www.cio.gov/documents/IPv6_FAQs.pdf) document states that the backbone includes the wide area network (WAN) core up to the local area network (LAN) point of demarcation, describing the LAN demarcation point as the device (e.g., router or switch) that services workstations. The Federal Chief Information Officers Council further defined the backbone, in the Architecture and Infrastructure Committee's "Demonstration Plan to Support Agency IPv6 Compliance," January 28, 2008, as "the operational core backbone network or the set of network transport devices (routers, switches) which provide the highest level of traffic aggregation in the network, and thus at the highest level of hierarchy in the network."

Domain Name System. DNS helps users to find their way around the Internet. Every computer on the Internet has a unique IP address. Because IP addresses are a string of numbers (e.g., 207.151.159.3), they are hard to remember. DNS makes using the Internet easier by allowing a domain name to be used instead (e.g., www.internic.net).
(Source: http://www.icann.org/en/general/glossary.htm#D, accessed May 18, 2010.)

Dual-Stack. Dual-stack is a transition mechanism in which the Internet host or router is capable of communicating using IPv4 and/or IPv6. The term "dual-stack routing" refers to a network that is dual IP, that is to say all routers must be able to route both IPv4 and IPv6. (Sources: The Architecture and Infrastructure Committee of the Federal Chief Information Officers Council "IPv6 Transition Guidance," online at http://www.cio.gov/Documents/IPv6_Transition_Guidance.doc, accessed May 26, 2010; and the NIST USGv6 Profile, online at http://www.antd.nist.gov/usgv6/usgv6-v1.pdf, accessed May 26, 2010.)

Internet Assigned Numbers Authority. Responsible for the global coordination of Internet protocol resources, the Internet Assigned Numbers Authority was originally responsible for the oversight of IP address allocation, the coordination of the assignment of protocol parameters provided for in Internet technical standards, and the management of the DNS, including the delegation of top-level domains and oversight of the root name server system. Under the Internet Corporation for Assigned Names and Numbers, it continues to distribute addresses to the Regional Internet Registries, coordinate with the

Internet Engineering Task Force and others to assign protocol parameters, and oversee the operation of the DNS. (Source: http://www.icann.org/en/general/glossary.htm#I, accessed May 18, 2010.)

Internet Corporation for Assigned Names and Numbers. A not-for-profit public-benefit corporation formed in 1998 with participants from all over the world and dedicated to keeping the Internet secure, stable, and interoperable. (Source: http://www.icann.org/en/about/, accessed May 19, 2010.)

Internet Engineering Task Force. This international community of network designers, operators, vendors, and researchers is concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. (Source: http://www.ietf.org/, accessed May 18, 2010.)

Internet Protocol. The communications protocol underlying the Internet. IP allows networks of computers to communicate with each other over a variety of physical links. Computers on the Internet use IP addresses to route traffic and establish connections among themselves; people generally use the human-friendly names made possible by the Domain Name System. (Source: http://www.icann.org/en/general/glossary.htm#I, accessed May 19, 2010.)

Internet Standard. An Internet Standard is a specification for using the Internet that has been adopted through the Internet Standards process, an activity that is organized and managed on behalf of the Internet community by the Internet Architecture Board and the Internet Engineering Steering Group. In outline, the process of creating an Internet Standard is straightforward: a specification undergoes a period of development and several iterations of review by the Internet community and revision based on experience, is adopted as a Standard by the appropriate body, and is published. (Source: Network Working Group, RFC2026, BCP9, "The Internet Standards Process – Revision 3," online at http://www.rfc-editor.org/rfc/bcp/bcp9.txt, accessed March 30, 2010.)

Internet Stream Protocol, Version 2 (ST2). ST2 is an experimental specification and is not an Internet Standard. The "experimental" designation typically denotes a specification that is part of some research or development effort. Both ST2 and IP apply the same addressing schemes to identify different hosts. ST2 differs from IP packets in the first four bits, which contain the internetwork protocol version number. Because number 5 is reserved for ST2, the IP version developed to replace IPv4 was assigned number 6. (Sources: Network Working Group, RFC1819, "Internet Stream Protocol Version 2 (ST2) Protocol Specification – Version ST2+," online at http://www.rfc-editor.org/rfc/rfc1819.txt, and RFC2026 or Best Current Practice 9, "The Internet Standards Process – Revision 3," online at http://www.rfc-editor.org/rfc/rfc2026.txt, accessed March 30, 2010.)

IP Address. A numerical address by which a location in the Internet is identified. (Source: http://www.icann.org/en/general/glossary.htm#I, accessed May 19, 2010.)

IP Aware. As used by OMB, an "IP-aware" device is one that is capable of recognizing the Internet protocol needed to communicate over the Internet.

IPv6 Capable. OMB provides two meanings for the term "IPv6 capable." The first refers to an agency's network backbone being capable of successfully passing IPv6 data traffic and supporting IPv6 addresses. The second refers to the technical specifications of a device, such as a computer. OMB notes that the terms "IPv6 compliant" and "using IPv6" in M-05-22 are synonymous with "IPv6 capable." (Source: OMB's IPv6 Frequently Asked Questions, online at http://www.cio.gov/documents/IPv6_FAQs.pdf, accessed May 19, 2010.)

IPv6 Compliant. See "IPv6 Capable."

IPv6 Enabled. The term "IPv6 enabled" is used to describe a network backbone that is not only capable of supporting IPv6 (IPv6 capable) but is actually "turned on" – implying that IPv6 traffic is actually successfully passing through the network. (Source: OMB's IPv6 Frequently Asked Questions, online at http://www.cio.gov/documents/IPv6_FAQs.pdf, accessed May 19, 2010.)

Network Address Translation (NAT). Network address translation is a method by which IP addresses are mapped, providing transparent routing to end hosts. An address realm is a network domain in which the network addresses are uniquely assigned to entities such that datagrams (packets) can be routed to them. The term "transparent routing" is used here for the routing functionality that a NAT device provides, which is different from the routing functionality provided by a traditional router device, which routes packets within a single address realm. Transparent routing refers to routing a packet between disparate address realms by modifying address contents in the IP header to be valid in the address realm into which the packet is routed. The need for network address translation arises when a network's internal IP addresses cannot be used outside the network because they are invalid for use outside or the internal addressing must be kept private from the external network. (Sources: Network Working Group, RFC2663, "IP Network Address Translator (NAT) Terminology and Considerations," online at http://www.rfc-editor.org/rfc/rfc2663.txt and http://en.wikipedia.org/wiki/Datagram, accessed May 28, 2010.)

Network Backbone. See "Backbone."

Technology Refresh. The periodic replacement of equipment to ensure continuing reliability of equipment or improved speed and capacity.
(Source: http://www.cryer.co.uk/glossary/t/technology_refresh.htm, accessed May 21, 2010.)

Transition Mechanism. Transition mechanisms ensure IPv4 and IPv6 interoperability. These mechanisms are categorized in the following three broad classes: dual-stack, tunnels (including configured and automatic tunnels), and translation mechanisms. (Source: The Architecture and Infrastructure Committee of the Federal Chief Information Officers Council "IPv6 Transition Guidance," online at http://www.cio.gov/Documents/IPv6_Transition_Guidance.doc, accessed May 26, 2010.)

Tunneling. Tunneling is a transition mechanism that encapsulates one version of IP in another so the packets can be sent over a backbone that does not support the encapsulated IP version. For example, when two isolated IPv6 networks need to communicate over an IPv4 network, dual-stack routers at the network edges can be used to set up a tunnel that encapsulates the IPv6 packets within IPv4, allowing the IPv6 systems to communicate without having to upgrade the IPv4 network infrastructure that exists between the networks. (Source: The Architecture and Infrastructure Committee of the Federal Chief Information Officers Council "IPv6 Transition Guidance," online at http://www.cio.gov/Documents/IPv6_Transition_Guidance.doc, accessed May 26, 2010.)

GUIDANCE FOR TESTING IPV6 CAPABILITIES

One of the requirements in OMB M-05-22 was for agency infrastructures (network backbones) to be IPv6 capable and to demonstrate that capability by June 30, 2008. For our evaluation of NASA's compliance with this requirement, we reviewed the "National Aeronautics and Space Administration (NASA) Agencywide IPv6 - Demonstration Plan," June 6, 2008; NASA's testing documentation; and the following guidance.

Guidance from OMB

The wording in M-05-22 led to some confusion, which OMB addressed in "Federal Government Transition Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6), Frequently Asked Questions," February 15, 2006. M-05-22 (see Appendix E) had stated the requirement as "must be using IPv6," which the IPv6 Frequently Asked Questions document clarified as meaning that agencies needed to demonstrate IPv6 capability on their network backbones by June 30, 2008 (see the "IPv6 Capable" glossary entry in Appendix B).

OMB's IPv6 Frequently Asked Questions document states that the backbone includes the wide area network (WAN) core up to the local area network (LAN) point of demarcation, describing the LAN demarcation point as the device (e.g., router or switch) that services workstations. The document also stated the specific actions required to meet the requirement:

> Agencies must be able to demonstrate they are capable of performing at least the following functions, without compromising IPv4 capability or network security:
>
> - Transmit IPv6 traffic from the Internet and external peers, through the core (WAN), to the LAN.
> - Transmit IPv6 traffic from the LAN, through the core (WAN), out to the Internet and external peers.
> - Transmit IPv6 traffic from the LAN, through the core (WAN), to another LAN (or another node on the same LAN).
>
> The requirements for June 30, 2008 are for the network backbone (core) only. Applications, peripherals, and other IT assets which are not leveraged in the execution of the functions mentioned above are not required for the June 30, 2008 deadline.

Agencies should verify this new capability through testing activities. Agencies are required to maintain security during and after adoption of IPv6 technology into the network core.

Guidance from the Federal Chief Information Officers Council

In January 2008, the requirements stated in OMB's IPv6 Frequently Asked Questions document were restated in the "Demonstration Plan to Support Agency IPv6 Compliance" issued by the Architecture and Infrastructure Committee, Federal Chief Information Officers Council. The document's purpose was to provide guidance and describe procedures to demonstrate IPv6 compliance, which it stated as showing "that IPv6 traffic has been successfully transported (i.e., received, processed, forwarded) through all IPv6 devices in an Agency's operational core backbone network."

Specifically, the Demonstration Plan stated that agencies must successfully demonstrate the following functions in order to be compliant with OMB's requirement:

- Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core), to the LAN.[21]
- Transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers.
- Transmit IPv6 traffic from the LAN, through the network backbone (core), to another LAN (or another node on the same LAN).

[21] The Demonstration Plan defined the term "LAN" for demonstration purposes as representing "IPv6-configured PCs/Laptops (with associated cabling and switching as needed), directly connected to IPv6 devices (routers, switches) in an Agency's operational core backbone network."

REQUIREMENTS AND GUIDANCE FOR A TRANSITION PLAN

For our evaluation of NASA's plans and efforts toward IPv6 transition and integration, we reviewed the following requirements and guidance to determine compliance for an appropriate transition plan.

OMB Requirements for a Transition Plan

OMB Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005, requires agencies to address each of the actions in Attachment C in the agency's IPv6 transition plan using the transition guidance issued by the Federal Chief Information Officers Council Architecture and Infrastructure Committee.

Following is the attachment from M-05-22:

> Attachment C: Transition Activities (Notional Summary of CIO Council Guidance)
>
> The CIO Council will develop additional transition guidance as necessary covering the following actions. To the extent agencies can address these actions now, they should do so. Beginning February 2006, agencies' transition activity will be evaluated using OMB's Enterprise Architecture Assessment Framework:
>
> - Conduct a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements.
> - Develop a sequencing plan for IPv6 implementation, integrated with your agency Enterprise Architecture.
> - Develop IPv6-related policies and enforcement mechanisms.
> - Develop training material for stakeholders.
> - Develop and implement a test plan for IPv6 compatibility/interoperability.
> - Deploy IPv6 using a phased approach.
> - Maintain and monitor networks.
> - Update IPv6 requirements and target architecture on an ongoing basis.

Guidance for Elements in the Transition Plan

IPv6 Transition Guidance. The Architecture and Infrastructure Committee of the Federal Chief Information Officers Council issued "IPv6 Transition Guidance" in February 2006, providing additional guidance to implement requirements of OMB M-05-22. The "IPv6 Transition Guidance" provides detailed "best practices" and recommendations to any Federal Government agency introducing IPv6 into its network environment. The Guidance includes a list of elements that could be used as the basis for an IPv6 transition plan. Although agencies were not required to include all of the elements in their transition plans, OMB recommended that each agency cross-check its plan against this list to ensure that all transition elements had been considered.

1. Identification of strategic business objectives.
2. Identification of transition priorities.
3. Identification of transition activities.
4. Transition milestones.
5. Transition criteria for legacy, upgraded, and new capabilities.
6. Means for adjudicating claims that an asset should not transition in prescribed timeframes.
7. Technical strategy and selection of transition mechanisms to support IPv4/IPv6 interoperability.
8. Management and assignment of resources for transition.
9. Maintenance of interoperability and security during transition.
10. Use of IPv6 standards and products.
11. Support for IPv4 infrastructure during and after 2008 IPv6 network backbone deployment.
12. Application migration (if required to support backbone transition).
13. Costs not covered by technology refresh.
14. Transition governance:
    a. Policy
    b. Roles and responsibilities
    c. Management structure
    d. Performance measurement
    e. Reporting
15. Acquisition and procurement.
16. Training.
17. Testing.

IPv6 Planning Guide. In May 2009, the Architecture and Infrastructure Committee of the Federal Chief Information Officers Council issued the "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government," which lists elements that must be included in the transition strategy plan.

1. Identification of transition priorities.
2. Identification of transition activities.
3. Transition milestones.
4. Transition criteria for legacy, upgraded, and new capabilities.
5. Dependencies.
6. Risks and mitigation strategies.
7. Maintenance of interoperability and security during transition.
8. Use of the NIST USGv6 Profile to express IPv6 capability requirements for specific products.
9. Transition governance:
    - Policy
    - Roles and responsibilities
    - Management structure
    - Performance measurement
    - Reporting
    - Management actions
10. Training.
11. Testing.

OMB M-05-22

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-05-22

August 2, 2005

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator
Office of E-Government and Information Technology

SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

As I stated in my testimony of June 29, 2005, before the House Committee on Government Reform, we have set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. This memorandum and its attachments provide guidance to the agencies to ensure an orderly and secure transition from Internet Protocol Version 4 (IPv4) to Version 6 (IPv6). Since the Internet Protocol is core to an agency's IT infrastructure, beginning in February, 2006 OMB will use the Enterprise Architecture Assessment Framework to evaluate agency IPv6 transition planning and progress, IP device inventory completeness, and impact analysis thoroughness.

Recent reports from the Government Accountability Office (GAO) and Department of Commerce's National Telecommunications and Information Administration (NTIA) discuss the benefits, complexity, costs, and risks organizations may encounter during the transition to IPv6. Additionally, the Department of Homeland Security's US-CERT has recently issued an advisory of security issues concerning IPv6. You should review these reports and the advisory to familiarize yourselves with the transition issues and ensure that risks are appropriately mitigated during your transition so the benefits are fully realized.[1]

What must agencies do and by when?

Following the guidance in the attachments to this memorandum, agencies must take the following actions by:

November 15, 2005

- Assign an official to lead and coordinate agency planning,
- Complete an inventory of existing routers, switches, and hardware firewalls (see Attachment A for details);

[1] References may be found at http://www.gao.gov/new.items/d05471.pdf, and http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/. The IPv6 vulnerability advisory from US-CERT was distributed via the Federal CIO Council and Small Agency Council list on April 5, 2005 and may be obtained from the secure US-CERT Portal.

- Begin an inventory of all other existing IP compliant devices and technologies not captured in the first inventory (see Attachment A for details); and
- Begin impact analysis to determine fiscal and operational impacts and risks of migrating to IPv6 (see Attachment B for details).

February 2006

- Using the guidance issued by Chief Information Officers Council Architecture and Infrastructure Committee (see below), address each of the elements in Attachment C in your agency's IPv6 transition plan and provide the completed IPv6 transition plan as part of the agency's Enterprise Architecture (EA) submission to OMB. Additional guidance on your agency's EA submission will be forthcoming.
- Provide a progress report on the inventory and impact analysis, as part of the agency's Enterprise Architecture (EA) submission to OMB. Additional guidance on your agency's EA submission will be forthcoming.

June 30, 2006

- Complete inventory of existing IP compliant devices and technologies not captured in first inventory, and
- Complete impact analysis of fiscal and operational impacts and risks.

June 30, 2008

- All agency infrastructures (network backbones) must be using IPv6[2] and agency networks must interface with this infrastructure. Agencies will include progress reports on meeting this target date as part of their EA transition strategy.

Selecting Products and Capabilities

To avoid unnecessary costs in the future, you should, to the maximum extent practicable, ensure that all new IT procurements are IPv6 compliant. Any exceptions to the use of IPv6 require the agency's CIO to give advance, written approval. An IPv6 compliant product or system must be able to receive, process, and transmit or forward (as appropriate) IPv6 packets and should interoperate with other systems and protocols in both IPv4 and IPv6 modes of operation. Specifically, any new IP product or system developed, acquired, or produced must:

- Interoperate with both IPv6 and IPv4 systems and products,
- If not initially compliant, provide a migration path and commitment to upgrade to IPv6 for all application and product features by June 2008, and
- Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

[2] Meaning the network backbone is either operating a dual stack network core or it is operating in a pure IPv6 mode, i.e., IPv6-compliant and configured to carry operational IPv6 traffic.

The National Institute for Standards and Technology (NIST) will develop, as necessary, a standard to address IPv6 compliance for the Federal government. Additionally, as necessary, the General Services Administration and the Federal Acquisition Regulation Council will develop a suitable FAR amendment for use by all agencies.

Additional Guidance

The Chief Information Officers Council Architecture and Infrastructure Committee will develop additional IPv6 transition guidance for the agencies. The Committee anticipates completing this guidance by November 15, 2005, and will address each of the elements identified in Attachment C.

If you have questions regarding Attachment C, please contact Richard Burk at 202-395-0379. For questions on Attachments A and B, please contact Lewis Oleinick at 202-395-7188 or oleinick@omb.eop.gov.

Attachments

MANAGEMENT COMMENTS

Final Report Reference

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

AUG 3 0 2010

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

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Response to Draft Audit Report, "Status of NASA's Transition to Internet Protocol Version 6 (IPv6)" (Assignment No. 09-017-00)

The Office of the Chief Information Officer (OCIO) appreciates the opportunity to respond to the draft Office of Inspector General (OIG) audit report, "Status of NASA's Transition to Internet Protocol Version 6 (IPv6)". In this response the OCIO addresses how well it will implement the single recommendation made in the draft audit as well as offering several comments on the draft report.

Recommendation: To ensure that NASA systems are interoperable and secure as Federal Government agencies and other organizations transition to IPv6, we recommend that the NASA CIO assign an IPv6 lead to complete an updated IPv6 transition plan that considers transition elements identified by the Architecture and Infrastructure Committee of the Federal Chief Information Officers Council in the "IPv6 Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government."

Management Response: The OCIO concurs with this recommendation. The OCIO will appoint an IPv6 lead and the direction to this individual will be to review the OMB requirements for IPv6 and to develop the planning and transition artifacts necessary to move the Agency forward in its IPv6 implementation. This will include developing an IPv6 transition plan as required by OMB, ensuring that the elements mentioned in the draft OIG report (on pages 10 and 11) are addressed.

Management Corrective Action Date: The OCIO will appoint an IPv6 lead by September 30, 2010. The updated IPv6 transition plan will be complete by March 31, 2011.

General Comments:

1. We recommend adding 'corporate' between 'NISN' and 'Backbone' to clearly identify which of the NISN physical backbone networks is being referenced. This change should be made in the following places:

changed

Final Report Reference

a) Page 8, in the 1st paragraph on 'Demonstrating Capability', line 3
b) Page 8, in the 2nd paragraph on 'Demonstrating Capability', line 2
c) Page 9, at the top of the page in the last sentences of the 'Acquiring IPv6 Experience', line 2
d) Page 10, at the top of the page in the last sentences of the 'Updated Transition Plan', line 3
e) Page 10, in the 1st paragraph on 'Transition Priorities and Activities', line 2
Page 15, in the 2nd paragraph, lines 6 and 8

page 17

2. In the last sentences of the 'Updated Transition Plan' section (on the top of page 10), it states that there are "five unaddressed elements that we believe NASA needs to consider". Only four elements are identified in the following paragraphs. Either the reference in the paragraph needs to change, or the fifth missing element needs to be identified.

footnote added in next paragraph for clarity

3. There is a reference in the 'Transition Priorities and Activities' section to the Space Network and the Ground Network. These networks are not fiber networks but are tracking networks for which the NISN Mission Backbone is the fiber connection. We are unclear as to why they are referenced herein (or, if the reference remains, why the Deep Space Network, the other NASA tracking network, was excluded).

changed

4. The 'IPv6 Standards and Products' element (discussed on page 11) is the third element discussed, not the fourth (as stated on line 1).

5. The 'Governance' element (discussed on page 11) is the fourth element discussed, not the fifth (as stated on line 1).

page 15
page 17
changed

6. On page 13, in the 3rd paragraph, the correct title is Associate CIO for Architecture and Infrastructure (vice 'Deputy'). This correction is also needed on page 15, 1st paragraph.

As requested, we reviewed the report and we did not find any information that should not be publicly released.

The OCIO is grateful to the OIG for their thorough review of the current status in NASA of IPv6 implementation. We welcome suggestions to reinvigorate our transition to IPv6.

Questions regarding this response should be directed to Ms. Betsy Edwards betsy.edwards@nasa.gov; (202) 358-4639.

Sincerely,

Linda Y. Cureton

cc:
HQ/Ms. Edwards
ARC/ Ms. De Leon
ARC/ Mr. Williams
MSFC/Mr. Dougle
MSFC/Mr. Pettus
MSFC/Mr. White

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief of Staff
Chief Information Officer
Ames Research Center Chief Information Officer
Dryden Flight Research Center Chief Information Officer
Glenn Research Center Chief Information Officer
Goddard Space Flight Center Chief Information Officer
Jet Propulsion Laboratory Chief Information Officer
Johnson Space Center Chief Information Officer,
Director of Information Technology and Communication Services, Kennedy Space Center
Langley Research Center Chief Information Officer
Marshall Space Flight Center Chief Information Officer
Stennis Space Center 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, 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

Congressional Committees and Subcommittees, Chairman and Ranking Member (continued)

House Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies
House Committee on Oversight and Government Reform
Subcommittee on Government Management, Organization, and Procurement
House Committee on Science and Technology
Subcommittee on Investigations and Oversight
Subcommittee on Space and Aeronautics

Major Contributors to the Report:

Wen Song, Director, Information Technology Directorate
Mindy Vuong, Project Manager
Linda Hargrove, Team Lead
Deirdre Beal, Auditor
Scott Riggenbach, Auditor

SEPTEMBER 9, 2010

REPORT No. IG-10-022

OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit http://oig.nasa.gov/audits/reports/FY10/ 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.