Audit of NARA's Transition to Internet Protocol Version 6
OIG Report No. 09-05
March 11, 2009

EXECUTIVE SUMMARY

The Internet protocol (IP) provides the addressing mechanism that defines how and where information such as text, voice, and video move across interconnected networks. Internet protocol version 4 (IPv4), which is widely used today, may not be able to accommodate the increasing number of global users and devices that are connecting to the Internet. As a result, IP version 6 (IPv6) was developed to increase the amount of available IP address space. Use of both IPv4 and IPv6 is expected to overlap for some time and the hardware and software infrastructure needed to support both IPv4 and IPv6 presents a challenge to the Federal Government.

To guide Federal Government agencies in their transition to IPv6, in August 2005, the Office of Management and Budget (OMB) issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6", which outlined a transition strategy for agencies to follow and established the goal for all Federal agency network backbones to support IPv6 by June 30, 2008.

For this audit, we assessed NARA's efforts to transition to IPv6. Specifically, our objective was to determine whether NARA was in compliance with the OMB mandate, and if not, to identify what major obstacles or challenges exist and whether a plan for compliance has been developed.

NARA did not comply with the OMB mandate because NARA has not verified whether the network backbone is capable of supporting IPv6. Specifically, IPv6 testing on the production environment did not test NARA's ability to transport IPv6 traffic through all devices in the core network and did not test whether NARA could successfully receive and transmit IPv6 traffic outside NARA's network. As a result, NARA does not have assurance that the planned implementation strategy will work.

We also found that additional work is needed in order for NARA to address future obstacles and challenges. For example, NH officials involved in planning for the transition to IPv6 did not identify or address risks and challenges associated with the transition. If not addressed, these risks and challenges may result in increased costs and security risks associated with the transition to IPv6. In addition, new IT equipment orders did not contain a requirement for products to be IPv6 compliant or interoperate with both IPv4 and IPv6 systems. As a result, NARA may have to spend additional funds to acquire IPv6 compliant equipment.

This report contains five audit recommendations which upon implementation would both bring NARA into compliance with OMB requirements and provide the foundational structure for transition to IPv6. However, full concurrence was not forthcoming from the CIO specific to four of the recommendations.

The first two recommendations put forth were grounded in OMB criteria which NARA failed to address. We revised the recommendations to afford the CIO opportunity to seek a waiver from defined OMB criteria. The CIO had no additional comments on the revised recommendations and it is unclear whether the CIO will seek a waiver from

OMB. As of the date of issuance of this report, NARA remains in non-compliance with OMB M-05-22.

Specific to the third recommendation, while the CIO indicates concurrence, she in fact does not concur with the breadth of the recommendation. She does not agree with the language in our recommendation defining participants and scope of IPv6 training to be extended to those involved in IPv6 planning and execution.

Finally, the CIO disagreed with the fifth recommendation that NARA Interim Guidance 801-2 and Directive 805 identify IPv6 management controls to ensure IPv6 compliance. She provides as her rational that this is unnecessary and unwarranted. We disagree with this position as planning for new projects, systems, and associated procurements involve both the capital planning and system development life cycle processes.

BACKGROUND

Internet Protocol (IP) is the "language" and set of rules computers use to talk to each other over the Internet. The existing protocol supporting the Internet today - Internet Protocol Version 4 (IPv4) - provides the world with only 4 billion IP addresses, inherently limiting the number of devices that can be given a unique, globally routable address on the Internet. The emergence of IPv6, providing the world with an exponentially larger number of available IP addresses, is essential to the continued growth of the Internet and development of new applications leveraging mobile Internet connectivity. Although the information technology (IT) community has come up with workarounds for this shortage in the IPv4 environment, IPv6 is the true long-term solution to this problem. Use of both IPv4 and IPv6 is expected to overlap for some time. The hardware and software infrastructure needed to support both IPv4 and IPv6 presents a challenge to the Federal Government.

In August of 2005, the Office of Management and Budget issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6," establishing the goal of enabling all Federal government agency network backbones to support the IPv6 by June 30, 2008.

The memorandum required that the agency's network backbone be ready to transmit both IPv4 and IPv6 traffic, and support IPv4 and IPv6 addresses, by June 30, 2008. Agencies were to demonstrate they could perform <u>at least</u> the following functions, without compromising IPv4 capability or network security:

- Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core), to the LAN.
- 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).

NARA's Chief Information Officer assigned the Chief Technology Officer to lead and coordinate planning for IPv6. NARA's overriding strategy for the transition was to align all IPv6 implementation activities with other network engineering projects and business application release schedules to eliminate the need for multiple and costly system testing and infrastructure recertification efforts. NARA planned to upgrade its IP-dependent devices to IPv6 compliant levels and install, configure, and operate both IPv6 and IPv4 infrastructure on the network to provide IPv6 interoperability with external clients that may require IPv6 addressing. This would address the OMB requirement of ensuring IPv6 compatibility and compliance. However, NARA would not *operationally enable* IPv6 until: (a) the overall network architecture upgrade specified in the Enterprise Architecture was complete, (b) the business applications move to IPv6 compliant environments as part of their product update and release strategies, and (c) IPv6 is mature, widely deployed across the Internet, and fully supported by the IT industry.

OJECTIVE, SCOPE, METHODOLOGY

The objective of this audit was to assess NARA's efforts to transition to IPv6. Specifically, we determined whether NARA was in compliance with the OMB mandate, and if not, to identify what major obstacles or challenges exist and whether a plan for compliance has been developed.

The audit was conducted at Archives II in College Park, MD, primarily with the Office of Information Services (NH). We also contacted the Acquisition Services Division (NAA).

In support of the audit objective, we evaluated NARA's actions and responses to OMB Memorandum 05-22 milestones for transitioning to IPv6. We reviewed additional guidelines and procedures issued by the Federal Chief Information Officers Council (CIOC) Architecture and Infrastructure's Committee and the National Institute of Standards and Technology's Special Publication 500-267 "A Profile for IPv6 in the U.S. Government – Version 1.0," July 2008 in support of OMB M-05-22.

To determine whether NARA was in compliance with the OMB mandate, we analyzed the planning activities completed, identified devices within the NARA infrastructure, obtained and reviewed test results, reviewed the controls in place over the acquisition and procurement process and reviewed the actions taken to address security risks associated with the transition to IPv6. We reviewed progress reports submitted to OMB to determine whether any challenges, risks, or other issues were identified by NARA.

To determine whether NARA adequately planned for the transition we reviewed the IPv6 Transition Strategy, Implementation Plan, and meeting notes from various planning meetings held between January 2006 and December 2007. We also interviewed the IPv6 Project Lead along with support contractors who wrote the planning documentation.

To determine whether NARA's infrastructure contained IPv6 compliant devices we obtained copies of equipment inventories submitted to OMB along with reports generated from an automated monitoring tool to detect devices currently attached to the network and the operating software loaded on the devices. We also reviewed NARANET infrastructure drawings current as of May 2008. We compared the devices in the network and the operating software to those devices used during IPv6 testing in the production environment. We reviewed the test plan and test results documented to determine whether NARA tested the scenarios required by OMB and the CIO Council in their Demonstration Plan.

To determine whether controls were in place to ensure new IT procurements were IPv6 compliant, we interviewed NH officials to determine the procurement process for new IT orders and reviewed existing Information Management Directives and NARA acquisition policy. We selected nine IT procurements occurring between September 2005 and September 2008 and reviewed the product plan (if available), solicitation documentation, and the resulting contract to determine whether the requirement for IPv6 compliant equipment was included.

To determine whether NARA has taken action to address security risks we evaluated the risks identified in the IPv6 Impact Analysis and reviewed whether NH officials and IT staff (including contractors) responsible for implementing IPv6 received training.

Our audit work was performed at Archives II in College Park, MD between March 2008 and January 2009. We conducted this performance audit 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.

FINDINGS AND RECOMMENDATIONS

Testing Was Not Adequate to Demonstrate IPv6 Compliance

IPv6 testing on the production environment did not demonstrate NARA's ability to successfully transport IPv6 traffic on the network backbone. This occurred because NH officials did not use the Chief Information Officer (CIO) Council's Demonstration plan in developing their test plan and NARA did not contact any external agencies to partner with to complete the testing. By June 30, 2008, agencies were to confirm to OMB that they could: transmit IPv6 traffic to and from the Internet and external peers and transmit IPv6 traffic from the Local Area Network[1] (LAN) to another LAN. As a result of performing only limited testing, NARA does not have assurance that the planned implementation of a dual-stack IPv6 and IPv4 architecture on NARANET will work.

By June 30, 2008, agencies were to confirm to OMB that they could:

- Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core) to the LAN;
- 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).

The CIO Council issued additional guidance and procedures to be used by agencies in demonstrating IPv6 compliance. This demonstration plan provided detailed procedures on how to conduct the testing, success criterion, and the documentation of the test results.

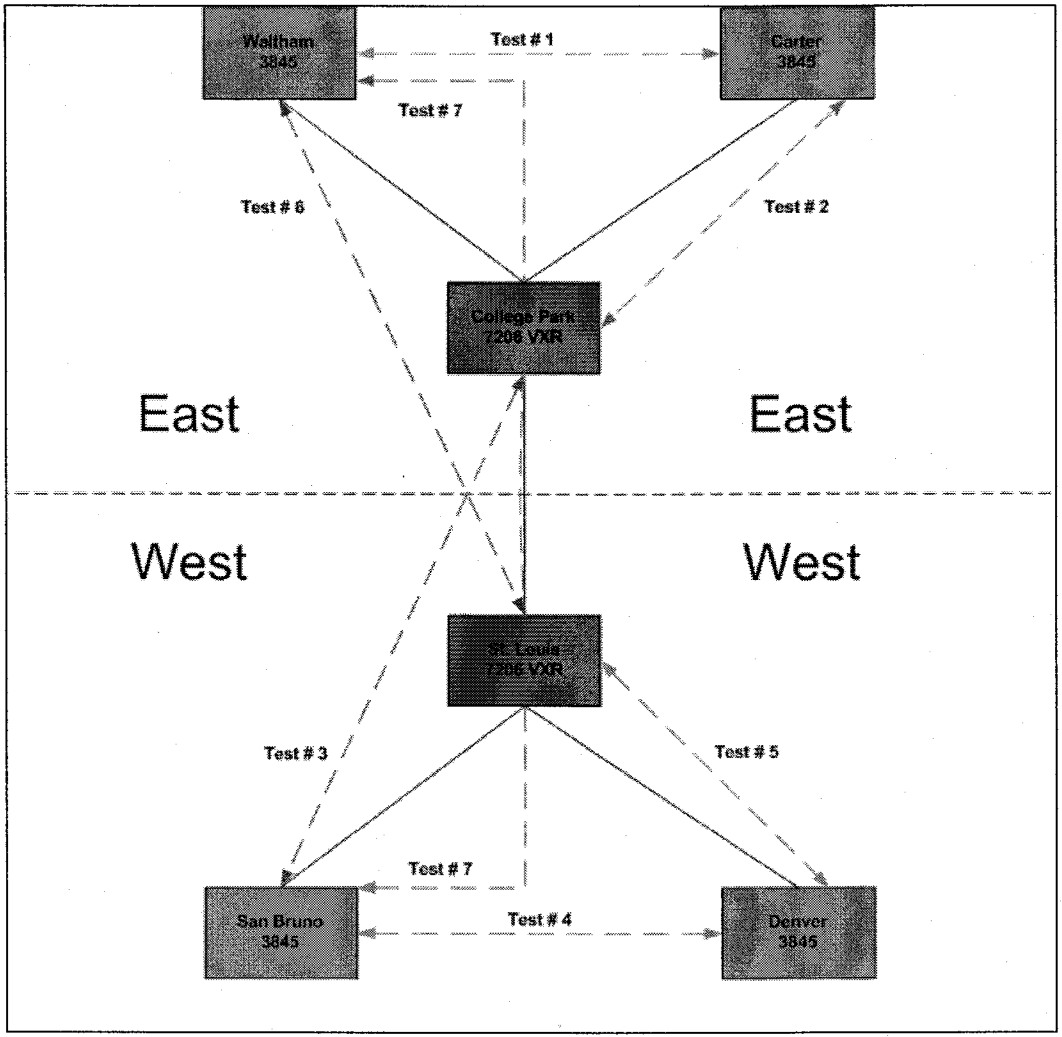
The OMB deadline of June 30, 2008 has passed however, NARA has not verified whether the network backbone is capable of supporting IPv6. Specifically, IPv6 testing on the production environment did not test NARA's ability to successfully transport IPv6 traffic through all devices in the core network and did not test whether NARA could successfully receive and transmit IPv6 traffic outside NARA's network.

Instead of using the test scripts identified in the CIO Council's Demonstration Plan, the Chief Technology Officer (CTO) along with support contractors developed seven scenarios to test for the June 2008 deadline. Test scenarios involved running a ping[2] command between six routers at the selected NARA sites. As shown in Figure 1 below, the scenarios included six different NARA sites using two types of Cisco routers.

[1] For the demonstrations, the term "LAN" represents IPv6-configured PCs or Laptops directly connected to IPv6 devices (routers, switches) in an Agency's operational core backbone network.

[2] Ping is a computer network tool used to test whether a particular host is reachable across an IP network.

Figure 1. IPv6 Production Verification Testing Overview



Source: NARA IPv6 Production Verification Results

NARA used two Cisco 7206 VXR routers, four Cisco 3845 routers and six Dell laptops using Windows XP to perform the testing. The tests did not include additional routers and switches identified in NARANET infrastructure drawings as part of NARA's core backbone network.

According to the CTO, NARA's core backbone network consists of -------------------------
----------------------------redacted pursuant to FOIA exemption "high" b(2)------------------
----

------. These devices should have been included in the IPv6 production verification testing.

After NARA conducted its test of the production network an NH official reported to OMB that testing addressed the scenarios identified by OMB and the tests were successful. However, the production testing did not include tests to verify NARA's ability to transmit and receive IPv6 traffic from an external network[3]. According to a summary of the test scenarios included in the verification results, NARA's Internet Service Provider could not provide a native IPv6 Internet environment to interface with the NARANET production infrastructure at the time of the test, therefore NARA emulated in previous tests[4] an external IPv6 network to pass native IPv6 traffic to and from NARANET. Guidance from the CIO Council addressed this limitation stating if an agency's ISP is not IPv6 enabled or does not offer IPv6 internet services, a static IPv6 over IPv4 tunnel can be used between the agency gateway and the corresponding internet border gateway.

According to OMB, agencies were required to ensure their network backbones were IPv6 capable. Agencies were to demonstrate this capability by completing the tests identified in the CIO Council test guidance. However, NH officials did not use the CIO Council's Demonstration Plan and instead, wrote their own test scenarios. In December 2007, the CTO made the decision that the production testing would be internal only because testing with an external partner would have to be done using a tunnel[5] which the CTO believed would not have any significance. No attempt was made to contact external agencies to discuss partnering for the tests.

The purpose of the testing was to demonstrate IPv6 compliance by showing that IPv6 traffic could be successfully transported (i.e., received, processed, forwarded) through all IPv6 devices in NARA's operational core network. In addition, the tests were to confirm that NARA could transmit IPv6 traffic to and from the Internet and external peers as well as transmit traffic from the LAN to another LAN. However, based on the limitations of the testing, NARA does not have assurance that the core network is capable of supporting IPv6 traffic. NARA should conduct IPv6 testing using the procedures outlined in the CIO Council's demonstration plan.

Management Comments on the Finding.

The Assistant Archivist for Information Services/CIO (hereafter referred to as the CIO) believed that NARA's actions substantively addressed the requirements to develop an IPv6 test plan as set forth by the OMB mandate and supplemental OMB guidance. She also believed that the tests conducted in the laboratory and on the production network conformed to OMB guidance and in her opinion; the testing unequivocally established that NARA's core backbone is capable of carrying IPv6 and IPv4 traffic simultaneously. According to the CIO, NARA's network core consists of ----redacted pursuant to FOIA exemption "high" b(2)-----, therefore, the testing actually went beyond the requirement because the 3845 routers installed at the field sites are not part of the core network but were tested.

[3] According to the CIO Council procedures, the term "Internet and external peers" refers to an external network (i.e. a network owned and operated by an organization different from that Agency) chosen for the demonstrations, and which may be from a partner Agency, an ISP, or other IPv6 organization.

[4] This previous testing was conducted in the system engineering lab environment in which a server was set up to simulate the Internet.

[5] Tunneling allows IPv6 packets to be sent between computers via IPv4 traffic.

The CIO clarified that their IPv6 tests were not "conformance" tests in the formal, engineering sense of that term and that any inference that OMB guidance provides true IPv6 conformance testing scenarios and procedures is mistaken. The CIO believes it is not valid to imply that their engineering methods are non-conforming or invalid based upon general statements of intent in a policy mandate or because they did not exactly mirror a set of ad-hoc, test scenarios. In addition, the CIO did not believe that a test partner was needed to verify that the network backbone could transport IPv6 traffic.

Audit Response

The test guidance issued by the CIO Council clearly established the scenarios agencies were to perform and the success criterion agencies should use to demonstrate that their core backbones were IPv6 capable. Testing was to be performed on all devices in NARA's operational core backbone network and was to include connectivity with an external network. NARA's testing did not meet either of these requirements therefore, we do not agree that the testing unequivocally established that NARA's core backbone is capable of carrying IPv6 traffic.

We revised this finding to clarify our position on the devices that should have been tested as part of the core network. We agree with NH officials that based on the definition of core network provided in the CIO Council's Demonstration Plan, the 3845 routers would not be considered part of the backbone network and removed that section from the report. However, we disagree that the core backbone consists of --redacted, "high" b(2)-- because those routers only aggregate traffic from NARA's field sites which does not include the majority of users at Archives I and Archives II.

<u>Recommendation 1</u>

The Assistant Archivist for Information Services/CIO should ensure testing required by OMB and outlined in the Federal CIO Council Architecture and Infrastructure Committee "Demonstration Plan to Support Agency IPv6 Compliance," version 1.0 on NARA's operational core network is performed and the test results as required by the CIO Council to demonstrate compliance are documented or obtain a written waiver from OMB.

Management Comments

The CIO disagreed with this recommendation stating that she believes additional testing as per the OMB Demonstration Plan is unnecessary and that resources would be better spent on the overall NARANET reengineering project.

Audit Response

We revised this recommendation to include the option for the CIO to either conduct the required testing or contact OMB to request a written waiver. The CIO had no additional comments on the revised recommendation and it is unclear whether the CIO will seek a waiver from OMB. NARA did not test all devices in its core network and did not test whether NARA could transmit IPv6 traffic to and from the Internet and external peers as required by OMB. Instead of contacting OMB regarding their concerns with the test scenarios or their intent to deviate from the scenarios in the CIO Council's Demonstration Plan, NARA reported to OMB that IPv6 verification testing was performed on the production network and testing "addressed the scenarios identified by OMB."

The requirement set by OMB was for Federal agencies to ensure their network backbones were IPv6 capable and there were tests agencies were required to complete in accordance with the CIO Council test guidance. If the CIO continues to believe that the required testing is unnecessary, she should contact OMB to request a written waiver.

Transition Risks Not Identified or Addressed

NH officials involved in planning for the transition to IPv6 did not identify or address risks and challenges associated with the transition. This occurred because NH officials have not updated the IPv6 Impact Analysis since June 2006 and based their planning activities on the belief that NARA will not operationally enable IPv6 in the near term. If not addressed, these risks and challenges may result in increased costs and security risks associated with the transition.

OMB Memorandum 05-22 required agencies to begin an impact analysis that included both cost and risk elements. According to the memorandum, the risk analysis should include areas such as dependencies and interoperability issues, business risks, and security risks. NARA's IPv6 Impact Analysis included a paragraph on each area associated with IPv6 implementation required by OMB M-05-22 but did not fully address the associated risks. For example, the Impact Analysis does not identify any dependencies or interoperability issues involved with IPv6 even though several NARA systems were identified as dependent on the version of IP that is used and did not support IPv6. According to the Impact Analysis, "this project is only dependent upon approval of the funding and staffing that is required to implement it. It is completely self-contained and will not interoperate with any other system or project."

The Impact Analysis did not identify any business impact or risk associated with the transition to IPv6. However, several critical NARA business applications, including the Case Management and Reporting System (CMRS) and the Archival Research Catalog (ARC), were found to be dependent upon the version of IP that is used. According to the CTO, NARA has lots of homegrown applications that run on IPv4 and it has yet to be determined what percentage of those applications can easily use IPv6. The CTO also stated ARC and CMRS would require substantial work to be able to support IPv6.

In another example, the Impact Analysis considered IPv6 to be no more or less secure than IPv4 and therefore, would not pose any new security risks to IT operations. Reports issued by the Government Accountability Office along with a Department of Homeland Security US-CERT advisory discuss multiple security issues concerning IPv6. According to GAO, IPv6 creates new opportunities for network abuse if IPv6 capable devices are not properly managed. Two IPv6 features—automatic configuration and tunneling—could present serious risks to federal agencies. Automatic configuration can facilitate network attacks because a rogue or unauthorized router may reconfigure neighboring devices by assigning them new addresses and routes. Tunneling can permit unauthorized traffic into the network undetected. The US-CERT alert warned federal agencies that unmanaged, or rogue, implementations of IPv6 present network management security risks. NARA's Impact Analysis did not address these security risks.

The IPv6 Impact Analysis identified training costs for 15 NH employees involved in the IPv6 transition however, training has not been provided. According to GAO, a challenge to the transition will be maintaining dual IPv4 and IPv6 environments for extended periods of time. Maintaining two network protocols is challenging in that it adds complexity to network maintenance and associated costs are higher. It also requires skilled personnel and may be difficult to maintain hardware and software interoperability across dual environments. NARA IPv6 planning documents did not address this challenge.

NH officials have not updated the IPv6 Impact Analysis since June 2006. At that time, NH officials based their planning activities on the belief that NARA will not operationally enable IPv6 in the near term. The impact analysis alludes to future risks once IPv6 is enabled however, the plan states that implementation was not being considered since it was not required to meet the OMB mandate.

In December 2008, the CIO Council issued draft guidance[6] for adopting IPv6 within the Federal government. According to the guidance, the next phase is the deployment of secure, end-to-end, IPv6-enabled network services which support federal agency core missions and applications. The guidance establishes a proposed timeline of January 2010 for Federal agencies to begin the transition phase. With the transition one year away, NARA should update the Impact Analysis to identify and address those risks and challenges associated with the transition and maintaining a dual-stack network. Knowing what risks there are and how to mitigate them appropriately will lessen problems in the future. If challenges and risks are not addressed, NARA will face potentially increased costs and security risks associated with the transition.

Management Comments on the Finding

The CIO stated that IPv6 has been identified as one of a number of interrelated network technologies in the Enterprise Architecture to be incorporated into the future design of NARANET. Specifically, NARA is migrating from a Frame Relay service to Multiprotocol Label Switching (MPLS) services under the Networx contract and OMB's Trusted Internet Connections requirement will force a complete reconfiguration of NARA's Internet Service Provider interface at the network edge. The CIO stated that the integration risks and complexities of transitioning to IPv6 require that it be pursued as one element of a comprehensive NARANET reengineering strategy and that to do otherwise would introduce unacceptable business risk, cost, and operational complexity to NARA.

The CIO stated that several statements in the draft report prematurely highlight the need to address "future" obstacles, risks, and challenges associated with implementing IPv6 in NARA's production environment. The CIO agreed that additional work efforts will be required in the future when NARA transitions to IPv6 deployment and operation, however, she did not believe that these "future" work efforts are applicable to satisfying the OMB mandate of verifying IPv6 capabilities in the network core.

[6] Architecture and Infrastructure Committee, Federal Chief Information Officers Council, "The Business Case and Roadmap for Completing IPv6 Adoption in US Government," Draft, version 0.1, December 22, 2008

Audit Response

We agree that transitioning to IPv6 should be part of the comprehensive NARANET reengineering strategy however, we do not agree with the CIO's approach to delay addressing risks with IPv6 until IPv6 is deployed and in operation at NARA. The purpose of creating an impact analysis was to determine fiscal and operational impacts and risks of migrating to IPv6. NARA officials focused on satisfying the OMB mandate to verify IPv6 capabilities in the network core by June 30, 2008 instead of creating a comprehensive plan to prepare for the eventual transition to IPv6. The risks and challenges associated with IPv6 need to be addressed now in order to plan how those risks will be mitigated when IPv6 is implemented.

Recommendation 2

The Assistant Archivist for Information Services/CIO should update the IPv6 Impact Analysis to address the security and business risks associated with implementing IPv6 or obtain a written waiver from OMB that waiting until IPv6 is implemented to address risks is an acceptable posture.

Management Comments

The CIO agreed with the recommendation but stated this should be handled as part of the NARANET redesign project. The CIO added that this should not be inferred as an issue of compliance with the past OMB M-05-22 mandate requiring a specific impact analysis at a past point in time. According to the CIO, risks associated with "implementing" IPv6 were not applicable to this project because there was no requirement or intent to "implement" IPv6 in production, just to verify certain IPv6 capabilities in the network core.

Audit Response

While the CIO indicated she agreed with this recommendation, her comments show that she does not agree with the intent of the recommendation. This recommendation addresses NARA's lack of planning for the transition to IPv6. The impact analysis was to aid agencies in planning for the transition by identifying fiscal and operational impacts and risks of migrating to IPv6. NARA has not identified those impacts and risks because NARA officials focused their planning efforts on meeting the OMB June 30, 2008 deadline to verify the capability of the network core, instead of planning for the eventual transition to IPv6. It is imperative that NARA identify potential issues and risks with the transition to IPv6 and ensure that risks are appropriately mitigated before IPv6 is implemented. We revised the recommendation so that if the CIO continues to believe that addressing IPv6 risks and challenges can be delayed until NARA implements IPv6 then she can request a written waiver from OMB that this is an acceptable posture.

Recommendation 3

The Assistant Archivist for Information Services/CIO should ensure employees responsible for planning, implementing, maintaining, and securing an IPv6 network for NARA receive appropriate IPv6 training.

Management Comments

The CIO agreed with this recommendation, but believed that this should be handled as part of the NARANET redesign project. The CIO also noted that this is not a matter of training but rather a skill required for network engineers going forward, similar to IPv4 currently.

Audit Response

While the CIO indicated she agreed with this recommendation, her comments show that she does not agree with the intent of the recommendation. We continue to disagree with the CIO's position that IPv6 training would only be needed for network engineers. According to the CIO Council, most IT personnel will require formalized training. In their Transition Guidance, the CIO Council identifies four main categories of education: awareness, architectural, operational, and specialized. In order to help ensure a successful transition to IPv6, the CIO should provide appropriate training to those employees responsible for planning, implementing, maintaining, and securing an IPv6 network.

Controls Not In Place to Ensure New IT Procurements were IPv6 Compliant

Orders for IT networking equipment did not include a requirement for IPv6 compliant equipment. This occurred because management controls identified in the IPv6 Transition Plan were not implemented. OMB Memorandum 05-22 states that in order to avoid unnecessary costs in the future, agencies should, to the maximum extent practicable, ensure that all new IT procurements are IPv6 compliant. As a result of not implementing necessary management controls, NARA may have to spend additional funds to acquire IPv6 compliant equipment.

According to OMB Memorandum 05-22, 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.

According to NARA's IPv6 Transition Plan, management controls were to be implemented in the Enterprise Architecture, Capital Planning and Investment Control (CPIC), Systems Development Life Cycle (SDLC) and procurement processes in order to verify and assure IPv6 compliance. The transition schedule shows these controls should have been implemented during the third quarter of FY 2006. NARA Interim Directive 801-2 "Review of IT Investments" was updated in July 2006 however, the recommended controls identified in the transition plan were not included in the revision. NARA Directive 805 "Systems Development Life Cycle" was last updated in January 2002 with two supplements to the directive issued in July 2005. Neither document addressed the controls identified in the transition plan.

NH contractor support personnel provided the Enterprise Architecture Conformance Review checklist they use to review product plans. The checklist includes a box to verify whether IPv6 compliance requirements were specified. While this checklist is useful, it has some limitations and cannot be relied on as the only review for IPv6 requirements. For example, this checklist is used only by the contractor support personnel and the contractors do not review every product proposal. Also, the checklist is only used in the review of full product plans therefore, projects requiring only a summary proposal or purchases of IT equipment outside the CPIC process would not be reviewed for IPv6 compliance.

We reviewed a sample of nine IT purchases occurring between September 2005 and September 2008. As shown in Table 1 "Review of IT Purchases," none of the orders reviewed contained a requirement that the equipment had to be IPv6 compatible. In addition, only three of the nine orders went through the CPIC process. Of the three that did go through the CPIC process, evidence was available to show that IPv6 compliance was considered during the acquisition process for only one of the orders.

Table 1. Review of IT Purchases

Order No.	Description	Order Amount	IPv6 Requirements Reviewed as part of CPIC Process?	IPv6 Compliance Included in Order?
1. NAMA-07-F-0136	Switches	$2,003,376	No	No
2. NAMA-08-F-0148	PBX Upgrade	$1,197,387	Yes	No
3. NAMA-06-F-0107	Switches	$507,721	N/A	No
4. NAMA-05-F-0108	Cisco 3845 routers	$340,028	N/A	No
5. NAMA-07-F-0146	Citrix Server and Access Gateway	$268,231	No	No
6. NAMA-08-M-0098	Cisco IOS, memory upgrades, and switch	$216,111	N/A	No
7. NAMA-07-F-0116	Redundant Switches for STL	$73,698	N/A	No
8. NAMA-06-F-0138	Essential Elements of the COOP Network and Firewall	$73,678	N/A	No
9. NAMA-07-F-0120	Switches, firewall, & routers	$69,597	N/A	No

In one example, NARA planned an upgrade of obsolescent NARANET switches in FY 2007. The contract was awarded for $2 million and did not mention a requirement for IPv6 compliant equipment in the Request for Quote or the order. The replacement of NARANET switches went through the CPIC process however, the need for IPv6 compliant equipment was not mentioned in the product proposal. NH support contractors were not asked to review this full product plan therefore, an Enterprise Architecture conformance review checklist was not completed for this project.

In another example, NARA bought equipment in September 2005 that had to be upgraded or replaced in order for the devices to be IPv6 compliant. NARA spent $340,000 for 40 Cisco 3845 routers with accessories. The devices were not IPv6 capable because the router operating system did not have the feature pack needed to support IPv6 traffic. In September 2008, NARA spent $216,000 to purchase upgrades for the router operating systems, flash memory cards, and memory upgrades.

A key milestone identified in NARA's Transition Plan was to adjust standard contracting language to assure that any new products and services procured by the agency would be IPv6 compliant or would have a commitment from the vendor to upgrade to IPv6 compliance. This management control was to be in place by June 30, 2006. An NH official stated that standard contract language was sent to the Acquisitions Services Division (NAA) to be included in the NARA Procurement Guide around June 2006 however, NAA did not update the guide due to resource issues. If this management control is not implemented, NARA may have to spend additional funds to acquire IPv6 compliant equipment.

Recommendation 4

The Assistant Archivist for Administration should direct the Director, Acquisitions Services Division to develop standard contract language for all IT orders to require IT products and services be IPv6 compliant.

Management Comments

The Director NAA concurred with this recommendation stating that he will add a statement to IT equipment purchases that all equipment and software delivered to NARA must be IPv6 compliant.

Recommendation 5

The Assistant Archivist for Information Services/CIO should update NARA Interim Guidance 801-2 and NARA Directive 805 to include those management controls identified in the NARA IPv6 Transition Plan to ensure all NARA IT projects, systems, and associated procurements are IPv6 compliant.

Management Comments

The CIO disagreed with this recommendation as written and asked that the OIG reconsider the approach. According to the CIO, NARA 812 and the Enterprise Architecture already contain this requirement. In addition, the CIO stated that it may not make sense to put specific technology requirements directly into the CPIC and SDLC policy documents because it would create a constant need to update and change policy every time a new technology requirement came along or an old technology requirement is retired. The CIO stated fixing management controls around acquisition and their approval and signoff procedures may be a better option.

Audit Response

We do not agree with the CIO that current controls within the Enterprise Architecture adequately address this requirement. In addition, management controls for ensuring IPv6 requirements cannot be limited to only the acquisition process. Planning for new projects and systems along with associated procurements involve both the CPIC and SDLC processes. The IPv6 Transition Plan identified specific management controls that should be implemented within the CPIC and SDLC processes. For example, the plan recommends that controls be established within the Decide phase of the CPIC process to specifically identify IPv6 compliance as part of the proposed solution and ensure that IPv6 costs are accurately reflected in the cost estimates. Including controls within NARA Interim Guidance 801-2 and NARA Directive 805 is necessary to ensure NARA's compliance with OMB policy.

Appendix A

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: FEB 27 2009

To: Office of the Inspector General (OIG)

From: Office of Information Services (NH)

Subject: Draft Report 09-05, Audit of NARA's Transition to Internet Protocol Version 6 (IPv6)

We have reviewed the draft OIG Report No. 09-05, January 16, 2009, titled *Audit of NARA's Transition to Internet Protocol Version 6.* We have also met with OIG staff on two occasions to discuss the draft. First, we want to thank your staff for meeting with us and providing a draft report that is well written and organized--it is clear that the auditor dedicated significant time in understanding the issues and presenting a coherent argument.

Nevertheless, based upon several of the findings and the recommendations set forth in this draft report, we believe we must respond thoroughly to several issues, which in our opinion, reflect misinterpretations regarding NARA's response to OMB Memo *M-05-22, Transition Planning for Internet Protocol Version 6.* In the table attached, we provide detailed responses to the draft audit report. The OIG made five recommendations; we concurred with two recommendations with comment; we disagreed with two recommendations, and one recommendation was to the Assistant Archivist for Administration. Our response to each recommendation is found on the attached matrix.

A summary of our major observations and comments on the draft follow:

1. Although we recognize that the OIG is simply restating OMB's language, we believe OMB M-05-22 does not outline a viable transition strategy or any other type of strategy for IPv6 implementation. This memorandum merely asserts a general policy mandate for planning IPv6 adoption. We believe it is inappropriate to consider this policy mandate and its associated guidance a valid, step-by-step, conformance testing and implementation approach for establishing IPv6 capability. In our opinion, transitioning to IPv6 cannot be undertaken or validated as an end unto itself. The integration risks and complexities of transitioning to IPv6 require that it be pursued as one element of a comprehensive NARANET reengineering strategy. To do otherwise would introduce unacceptable business risk, cost, and operational complexity to NARA.

2. We believe we substantively addressed the requirements to develop an IPv6 test plan as set forth by the M-05-22 mandate and supplemental OMB guidance. We also believe that the tests we conducted in our laboratory and on our production network conform to OMB guidance. In our opinion, we have tested beyond what is implied by the mandate and our tests have unequivocally established that NARA's core/backbone is capable of carrying IPV6 and IPv4 traffic simultaneously. In addition, we demonstrated our capability to communicate externally through emulation in our laboratory.

3. Our test reports have been written to show our capability regarding the essential intent of the OMB mandate, that being, to pass IPv6 packets through the network core. The reports are surely not "legal" documents required to show adherence to certain step-by-step procedures asserted by OMB or any other organization. We want to make it clear that our IPv6 tests, whether conducted in our laboratory or in the production network, are not "conformance" tests in the formal, engineering sense of that term, and that any inference that OMB guidance provides true IPv6 conformance testing scenarios and procedures is mistaken. Formal conformance testing requires rigorous test suites and test beds to verify specific engineering requirements against well-understood standards. Since NIST is just now in the process of establishing IPv6 compliance standards and test mechanisms for the Federal government, we feel it is not valid to imply that our engineering methods are non-conforming or invalid based upon general statements of intent in a policy mandate or because we did not exactly mirror a set of ad-hoc, test scenarios.

4. What OMB has produced over the last couple of years regarding IPv6 testing is neither a rigorous test suite nor a set of well-understood standards. What OMB has produced can only be considered guidance to assess the general viability of certain, specific IPv6 capabilities within certain parts of an agency's network. Additionally, the guidance has changed over time, presumably based on feedback from Federal agencies. Initially, IPv6 was supposed to have been implemented or "used" within the core of an agency's network by June 30, 2008. Subsequent OMB guidance changed the requirement from be "used" to being "ready to pass IPv6 traffic and support IPv6 addresses within the core" by June 30, 2008.

Neither has there been a consistent definition of "core/backbone." The current definition identifies major "aggregation nodes" as "core/backbone." NARA can identify such aggregation nodes within our current Frame Relay environment, but such identification would not be possible if an agency has an MPLS network. For an MPLS network, one may be able to approximately identify a "core/backbone" by saying "a set of nodes experiencing the heaviest traffic." The point is that "core/backbone" can only be defined within a certain context, and it is a general concept that is only minimally useful for the purpose of engineering network implementations. It is not possible for OMB or any other organization to have procedures, tests and standards defined for a multitude of unknown "core/backbone" definitions.

5. OMB continues to refine guidance related to IPv6 in response to feedback from Federal agencies, and in recognition of IT product and service market realities. We expect that this refinement will continue for the foreseeable future. Irrespective of these future considerations, Federal agencies can plan for the arrival of IPv6; and we are doing so.

We have identified IPv6 as one of a number of interrelated network technologies in the Enterprise Architecture (EA) to be incorporated into the future design of NARANET. In the short-term, we have taken the OMB IPv6 mandate seriously and have performed significant IPv6 verification testing--within the real world constraints of IPv6 adoption and availability in the IT product and service marketplace, and ever cognizant of the risks to NARA's business operations. We would add that expending resources to perform additional testing as prescribed by OMB and as recommended in the report would not be a fruitful activity since we would be testing on an infrastructure that will be replaced. Currently, (a) NARA is now migrating from Sprint's Frame Relay services to Qwest's MPLS services under Networx, and (b) the OMB Trusted Internet Connections (TIC) requirement will force a complete reconfiguration of NARA's Internet Service Provider (ISP) interface at the network edge, activities that would make additional testing as prescribed by the OMB Demonstration Plan of questionable value.

Finally, we believe that there are several statements in the draft report that prematurely highlight the need to address "future" obstacles, risks, and challenges associated with implementing IPv6 in NARA's production environment. Although it is true that additional work efforts will be required in the future when NARA transitions to IPv6 deployment and operation, we do not believe that these "future" work efforts are applicable to satisfying the M-05-22 mandate of verifying IPv6 capabilities in the network core.

We hope you consider these comments and those on the attached matrix as you develop your final draft of the audit report. As always, we are available to discuss any issues and meet with your and your staff. If you have specific questions about the text of the response, please call Haseen Uddin on 301-837-3072 or via email at haseen.uddin@nara.gov.

Martha Morphy

MARTHA MORPHY
Assistant Archivist for Information Services

Attachment: Detailed Comments on OIG IPv6 Audit Report No. 09-05

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
To guide Federal Government agencies in their transition to IPv6, in August 2005, the Office of Management Budget issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6", which outlined a transition strategy for agencies to follow and established the goal for all Federal agency network backbones to support IPv6 by June 30, 2008.	Page 1 / Paragraph 2	**We do not agree that M-05-22 outlines a transition strategy. /** Although we recognize that the OIG is simply restating OMB's language, in our opinion OMB M-05-22 does not outline a transition strategy or any other type of strategy. It merely asserts a general policy mandate for planning IPv6 adoption.
NARA did not comply with the OMB mandate because NARA has not verified whether the network backbone is capable of supporting IPv6. Specifically, IPv6 testing on the production environment did not test NARA's ability to transport IPv6 traffic through all devices in the core network and did not test whether NARA could successfully receive and transmit IPv6 traffic outside NARA's network. As a result, NARA does not have assurance that the planned implementation strategy will work.	Page 1 / Paragraph 4	**We disagree with this assertion. We believe that we verified that the NARANET backbone is capable of supporting IPv6. /** Our production testing conclusively verified and documented that IPv6 packets can be propagated on and routed through the core of NARANET. Our simulations in the lab proved that our network equipment configurations are capable of routing IPv6 packets to and from NARANET at the edge (outside) of the network. The lab simulations we performed were our best alternative for testing the ISP interface at the time of the test because our ISP could not provide a native IPv6 interface at that time. This mandate did not assert a requirement to "implement" IPv6 in production, so we believe that any "implementation strategy", outside of our strategy for verification testing of certain IPv6 capabilities, is not germane to this mandate or this discussion. Both the last section of M-05-22 and Appendix C state that additional guidance on IPv6 will be provided by the CIO Council Architecture and Infrastructure Committee. This subsequent guidance stated that IPv6 does not need to be operationally enabled by June 30, 2008; i.e., there was not an "implementation" requirement to make IPv6 operational, only a requirement to verify certain IPv6 capabilities in the network core.

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
We also found that additional work is needed in order for NARA to address future obstacles and challenges. For example, NH officials involved in planning for the transition to IPv6 did not identify or address risks and challenges associated with the transition. If not addressed, these risks and challenges may result in increased costs and security risks associated with the transition to IPv6. In addition, new IT equipment orders did not contain a requirement for products to be IPv6 compliant or interoperate with both IPv4 and IPv6 systems. As a result, NARA may have to spend additional funds to acquire IPv6 compliant equipment.	Page 1 / Paragraph 5	**We believe this paragraph inaccurately highlights the need to address the "future" obstacles, risks, and challenges associated with implementing IPv6 in NARA's production environment. Although it is true that additional work efforts will be required in the future when NARA transitions to IPv6 deployment and operation, we do not believe that these "future" work efforts are applicable to satisfying the M-05-22 mandate to verify IPv6 capabilities in the network core.** The summary paragraph of our strategy states: "Since NARA had no immediate operational need for IPv6, it was determined that the strategy going-forward would be to align all IPv6 engineering, acquisition, and implementation activities with other network engineering projects and business application release schedules. This approach would eliminate the need for multiple and costly system testing, rollout, and infrastructure recertification efforts." (Section 1.2 page 3, IPv6.Closeout.Report). The risks associated with the IPv6 verification testing activities required by the mandate are documented in section 10, page 41 of the IPv6.Implementation. Plan. Section 5, page 8 of the IPv6 Closeout Report summarizes additional risks and considerations that are key to the actual implementation of IPv6 at NARA. Although we agree that future risks associated with implementing, integrating, and operating IPv6 will need to be addressed (and they will be), we do not believe that they are germane to this mandate, or its specific deliverables and timeframes.

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
		Although we agree that NARA may need to spend additional funds to acquire IPv6 compliant equipment in future, this will be due to the timing of and requirements for actual IPv6 implementation, not necessarily because of past procurements. In the future, some products that NARA has acquired may need upgrades for production implementation of IPv6, some may not, and some may need to be replaced. However, IPv6 is but one factor in these considerations and many of the specific engineering requirements for production operation of IPv6 by way of developing a bill of materials (BOM) are unknown at this time. Additionally, NIST is just now establishing IPv6 standards, and USG compliant IPv6 devices are not expected to be available for acquisition until July 2010. Although we agree that we should try to acquire IPv6 capable products and services, we need to recognize that some product vendors and service providers may not provide products that are IPv6 capable at this time, and some segments of the market like ISPs, IP telephony vendors, security product vendors, and middleware vendors are not yet transitioned to IPv6. NARA needs to be careful not to prohibit the use of products and services needed to support today's business operations because those products do not yet support an implementation requirement that may be more than 5 years in the future. OMB M-05-22 actually states that: "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…"

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
IPv6 testing on the production environment did not demonstrate NARA's ability to successfully transport IPv6 traffic on the network backbone. This occurred because NH officials did not use the Chief Information Officer (CIO) Council's Demonstration plan in developing their test plan and NARA did not contact any external agencies to partner with to complete the testing.	Page 5 / Paragraph 1	**We disagree with this assertion. We believe that our tests and the corresponding results clearly demonstrate that NARA's backbone can and did propagate, transport, and route IPv6 traffic. /** IPv6 packets were clearly propagated, transported, and routed through the network backbone as is evident by the results of 7 different ping test scenarios. We believe our test results are valid even if they did not mirror the OMB Demonstration plan test scenarios verbatim. Also, verifying that the network backbone can transport IPv6 traffic does not require a test partner in our opinion.
The OMB deadline of June 30, 2008 has passed however; NARA has not verified whether the network backbone is capable of supporting IPv6. Specifically, IPv6 testing on the production environment did not test NARA's ability to successfully transport IPv6 traffic through all devices in the core network and did not test whether NARA could successfully receive and transmit IPv6 traffic outside NARA's network.	Page 5 / Paragraph 4	**We disagree with this assertion. We believe we have clearly demonstrated that IPv6 packets can traverse the backbone and we have documented test results that support our position. /** We believe that our tests and the corresponding results demonstrate that NARA can transport IPv6 traffic through the network core. IPv6 packets were clearly propagated on and transported through the network core as is evident by the results of 7 different ping test scenarios. We also believe that the simulation tests we performed in the lab demonstrate that NARA's infrastructure components will be able to receive and transmit IPv6 traffic to/from NARA's network core, when there is a source for such traffic. OMB asserts at least two different definitions for the network core/backbone as listed below. Based on OMB's second and most current definition, NARA's core would consist only of the Cisco 7206 routers in College Park and St. Louis. By this definition, our testing actually went beyond this requirement.

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
		(1) E·GOV Federal Government Transition Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6) Frequently Asked Questions, 2/15/06. "The "backbone" includes the wide area network (WAN) core up to the local area network (LAN) point of demarcation. The LAN demarcation point is the device (e.g., router, switch) which services the workstations)." (2) Demonstration Plan to Support Agency IPv6 Compliance, Version 1.0, January 28, 2008. "For the purposes of the IPv6 transition, the core network (a.k.a. backbone network) is the set of network transport devices (routers, switches) that provide the highest level of traffic aggregation in the network, and thus at the highest level of hierarchy in the network."
The CIO Council emphasized that the demonstration of IPv6 compliance must be performed on the Agency's operational core network. However, NARA had to modify equipment software in order to perform the testing. Specifically, the operating software installed on the Cisco 3845 routers was not IPv6 capable. NH officials agreed to upgrade only those four devices involved in the testing and then remove the update once the test was complete. Therefore, testing conducted was not an accurate reflection of NARA's operational core network.	Page 6 / Paragraph 2	**We disagree with this assertion. The upgrades were made for the purposes of the test - directly on the NARANET production network devices and the test were executed concurrent with normal NARANET operations on those devices. /** Based on Cisco's "Hierarchical Networking Model" definition and OMB's Demonstration plan definition, the 3845 routers installed at the field sites are part of the distribution layer of the network, not the "core" layer of the network. The 7206 routers that constitute the core layer of the network can support IPv6 operationally as-is from a HW/IOS perspective.

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
		Additionally, we went beyond this limited definition of "core" and actually included testing of selected field site 3845 routers in the network distribution layer across the entire country. However, the changes needed to be rolled-back from the 3845 routers because it is bad operations management practice to leave components installed that are not in use, and doing so would violate the "Least Privilege" NIST security control [AC-6.2]: "For moderate or high confidentiality information systems, NARA shall employ the concept of least privilege for specific duties and information systems (including specific ports, protocols and services) in accordance with risk assessments as necessary to adequately mitigate risk to NARA operations, NARA assets and individuals."
After NARA conducted its test of the production network an NH official reported to OMB that testing addressed the scenarios identified by OMB and the tests were successful. However, the production testing did not include tests to verify NARA's ability to transmit and receive IPv6 traffic from an external network. According to a summary of the test scenarios included in the verification results, NARA's Internet Service Provider could not provide a native IPv6 Internet environment to interface with the NARANET production infrastructure at the time of the test, therefore NARA emulated in previous tests an external IPv6 network to pass native IPv6 traffic to and from NARANET. Guidance from the CIO Council addressed this limitation stating if an agency's ISP is not IPv6 enabled or does not offer IPv6 internet services, a static IPv6 over IPv4 tunnel can be used between the agency gateway and the corresponding internet border gateway.	Page 6 / Paragraph 3 onto page 7	**We disagree that the CIO Council's guidance prescribing a tunneling approach addresses the limitation of an agency's ISP not being IPv6 enabled. In our opinion this is not valid from a network engineering perspective. /** When tunneling as suggested, IPv6 packets are not propagated or routed, IPv4 packets are. This is no different that what is performed on the IPv4 network today. The suggested tunneling configuration does not verify IPv6 traffic propagation or IPv6 routing.
According to OMB, agencies were required to ensure their network	Page 7 /	**The OMB Demonstration plan guidance was promulgated too late**

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
backbones were IPv6 capable. Agencies were to demonstrate this capability by completing the tests identified in the CIO Council test guidance. However, NH officials did not use the CIO Council's Demonstration Plan and instead, wrote their own test scenarios. In December 2007, the CTO made the decision that the production testing would be internal only because testing with an external partner would have to be done using a tunnel which the CTO believed would not have any significance. No attempt was made to contact external agencies to discuss partnering for the tests.	Paragraph 2	**to be used by NARA without seriously disrupting our IPv6 testing and EA submission schedules. Although our test scenarios did not mirror the scenarios set forth in the OMB Demonstration plan verbatim, we believe they were sufficiently robust to demonstrate IPv6 capability in the network core. /** The OMB Demonstration plan guidance did not come out until after NARA had completed lab testing and the majority of our production test development and preparation was complete. (NARA was actually late on our schedule - we had planned to complete the production tests just prior to the XMAS holiday break.) The OMB Demonstration plan guidance was received only 28 days before NARA's EA submission was due, and it is important to remember that the EA submission required IPv6 work products. It was decided that it was too late to change the testing strategy because it would have caused rework that could have jeopardized completion of the tests and could have impacted our EA scores. As stated above, we simulated the ISP interface because Verizon/UUNET did not provide a native IPv6 feed at the time of the test. In our opinion, setting up a test-bed with an external agency would have been no more representative of NARA's production environment than our simulations because an external agency test-bed is not an ISP nor would it necessarily simulate one. As stated above, tunneling IPv6 through IPv4 does not validate any aspect of IPv6 functionality in our opinion.
The purpose of the testing was to demonstrate the implementation and the interoperability of a dual-stack IPv6 and IPv4 architecture on the core of NARANET however, based on the limitations of the testing,	Page 7 / Paragraph 3	**We disagree with this assertion. We believe that our tests and the corresponding results clearly demonstrate that NARA's backbone can transport IPv6 and IPv4 traffic concurrently. Installing IOS**

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
NARA does not have assurance that their IPv6 strategy will work or that the core backbone is capable of supporting IPv6 traffic. In September 2008, NH officials purchased IOS upgrades for the 3845 routers so that routers will be IPv6 capable. Once the IOS upgrades are installed, NARA should conduct IPv6 testing using the procedures outlined in the CIO Council's demonstration plan.		**upgrades on the 3845s and retesting will just consume time and resources to repeat more instances of what we have already done./** The test scenario in the CIO Council's Demonstration plan that applies to the 3845s has already been performed. As noted above, depending on the definition of "core" that is used, the 3845s may not even be applicable. The testing to verify external interaction with the ISP that we simulated in the lab, and that this report considers invalid, would not involve the 3845s because external interaction tests occur on the edge of the network, not in the core. Practically speaking, when IPv6 gets operationally deployed it will likely be done incrementally on a router by router basis, so having some 3845 routers with IPv6 implemented and some without is actually a more realistic test. In our opinion, it is inaccurate to infer that performing testing as per the OMB Demonstration assures IPv6 capability or verifies the viability of IPv6. The OMB prescribed test scenarios only investigate specific, limited IP capabilities. The OMB test scenarios do not provide a comprehensive validation of overall IPv6 readiness because they do not address applications, integration, management, security, performance, capacity, interoperability, IT market penetration and support, commercial viability, or the product and service certification aspects of IPv6 migration. Additionally, NIST is just now establishing IPv6 standards, and USG compliant IPv6 devices are not expected to be available for acquisition until July 2010.
Recommendation 1	Page 7 /	**We disagree with this recommendation. We believe that additional testing as per the OMB Demonstration plan is**

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
The Assistant Archivist for Information Services should ensure testing required by OMB and outlined in the Federal CIO Council Architecture and Infrastructure Committee "Demonstration Plan to Support Agency IPv6 Compliance," version 1.0 on NARA's operational core network is performed and the test results as required by the CIO Council to demonstrate compliance are documented.	Paragraph 4	**unnecessary and that our resources would be better spent on the overall NARANET reengineering project of which IPv6 is but one part. /** In our exit review on IPv6, performed by GSA on behalf of OMB, no concerns were expressed regarding our approach to the IPv6 mandate. Additionally, NARA received a perfect 5 out of 5 for the IPv6 criteria score on the FY07 and FY08 EA submissions. OMB is aware of how we tested, and why we tested in the manner that we did. The facts are that: (1) NARA is now migrating from Sprint Frame Relay services to Qwest MPLS services under Networx, and (2) the TIC requirement will force a complete reconfiguration of NARA's ISP interface at the network edge would seem to make additional testing as prescribed by the OMB Demonstration plan on the current infrastructure even less useful. Additionally, OMB has release new draft guidance on IPv6 (*The Business Case and Roadmap for Completing IPv6 Adoption in US Government, version 0.1, December 22, 2008*). This new guidance has new requirements and new timelines, so the past IPv6 activities associated with M-05-22 have been overtaken by new events and new requirements. Some items of note: (1) *The new guidance aligns with the approach we have been pursuing and states that an IPv6 Transition Strategy Plan should be developed that integrates with other agency activities.* "The IPv6 Transition Strategy Plan should be folded into the Enterprise Transition Strategy Plan, should link to core mission segments as appropriate, and should define a specific timeline and set of

Report Statement	Page / Paragraph	Comment / Rationale
		milestones to deploy the IPv6-enabled network services defined in the IT Infrastructure Segment Architecture. As with any other technology integration effort, the planning effort should consider multiple timelines, including: • Budget cycles • Technology refresh cycles • IT Infrastructure quality improvements • Equipment and software certification cycles • IT project dependencies • Technology standards development and adoption When developing the transition strategy, focus on ensuring that network, computing, application, and service components are enabled in a sequence that will generate the maximum amount of meaningful end-to-end IPv6 activity. At times, an immediate incremental change has advantages over waiting for all IPv6 features to be available in the next version of a product. (2) *IPv6 tests should be done in a lab environment – much like we have done.* "Setting up a test lab is important for the safe controlled introduction of new technology into your network and prototyping with an emphasis on small scale validation of targeted performance outcomes (e.g. experimenting with secure IPv6-enabled teleworking). Testing in a lab enables the agency IT group to perform tests that

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
		could potentially be disruptive or introduce a security risk if deployed on the production network. The test environment should be set up as close as possible to resemble the production environment. At first, the test sites should not be connected to the production network or to each other." (3) *NIST is establishing an official IPv6 Test Program to truly verify IPv6 compliance of IT products.* "Following publication of the USG IPv6 Standards Profile, an infrastructure to demonstrate IPv6 product compliance needed to be set up. As a result, NIST is establishing a testing program based on ISO 17025 accredited test laboratories and standard reference tests, to assure compliance of Hosts, Routers and Network Protection Devices. NIST is developing a document *SP 500-273 Guidance on IPv6 Test Methods and Validation*, due for publication late 2008. This is pre-requisite to open public review of the test specifications, and Accreditation Bodies' establishing assessment programs, leading to the creation of Test Laboratories that adhere to the ISO 17025 "General Requirements for the Competence of Testing and Calibration Laboratories". The goal is to have USG compliant IPv6 devices available for acquisition by July 2010. Compliance is signaled by device vendors issuing a "Suppliers Declaration of Conformance", based on ISO 17050. Specific provisions of this SDOC require that host and router products be tested for conformance and interoperability, and network protection products undergo functional testing, in accredited laboratories. (4) Regarding ISPs, we offer the following relevant quote: *"The technical stuff for IPv6 is done. IPv6 is ready. This is a business issue in the internet service industry. The ISP community round the world needs to pay attention... They are persisting in the 'nobody is asking*

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
		for this' mentality. They are not valuing business continuity as they should. When they finally wake up, there is going to be a mad scramble for IPv6 and they won't implement it properly". Vinton Cerf, September 30, 2008.
NH officials involved in planning for the transition to IPv6 did not identify or address risks and challenges associated with the transition. This occurred because NH officials have not updated the IPv6 Impact Analysis since June 2006 and based their planning activities on the belief that NARA will not operationally enable IPv6 in the near term. If not addressed, these risks and challenges may result in increased costs and security risks associated with the transition. OMB Memorandum 05-22 required agencies to begin an impact analysis that included both cost and risk elements. According to the memorandum, the risk analysis should include areas such as dependencies and interoperability issues, business risks, and security risks. NARA's IPv6 Impact Analysis included a paragraph on each area associated with IPv6 implementation required by OMB M-05-22 but did not fully address the associated risks. For example, the Impact Analysis does not identify any dependencies or interoperability issues involved with IPv6 even though several NARA systems were identified as dependent on the version of IP that is used and did not support IPv6. According to the Impact Analysis, "this project is only dependent upon approval of the funding and staffing that is required to implement it. It is completely self-contained and will not interoperate with any other system or project." The Impact Analysis did not identify any business impact or risk associated with the transition to IPv6. However, several critical NARA	Page 8 / Paragraphs 1, 2, & 3	**We believe these paragraphs inaccurately highlight the need to address "future" risks and challenges associated with implementing IPv6 in NARA's production environment. Although it is true that additional work efforts will be required in the future when NARA transitions to IPv6 deployment and operation, we do not believe that these "future" work efforts are applicable to satisfying the M-05-22 mandate to verify IPv6 capabilities in the network core by June 30, 2008. Additionally, we believe that we developed and submitted an IPv6 impact analysis as per OMB's prescribed format and guidelines – and in fact, we submitted it to OMB for review on two separate occasions as part of our EA submissions. /** These paragraphs, ironically, make the very case we have been asserting. We purposely pursued a strategy of "capability verification" rather than "production implementation" to avoid risk to NARA. The reason we did not identify implementation, application, integration, and business risk is because we approached this effort as a capability verification project, not an implementation project. In other words, the management of these types of risks are applicable to future projects that will actually transition IPv6 to production operations. They are not applicable to a project that is only verifying IPv6 capabilities in the network core. Applications and integration were not even in scope for this initial

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
business applications, including the Case Management and Reporting System (CMRS) and the Archival Research Catalog (ARC), were found to be dependent upon the version of IP that is used. According to the CTO, NARA has lots of homegrown applications that run on IPv4 and it has yet to be determined what percentage of those applications can easily use IPv6. The CTO also stated ARC and CMRS would require substantial work to be able to support IPv6.		effort, although we did identify the applications that will have IPv6 dependencies when the production implementation of IPv6 is addressed. In our opinion, the OMB mandate did not require us to address application integration and rework by June 30, 2008.
In another example, the Impact Analysis considered IPv6 to be no more or less secure than IPv4 and therefore, would not pose any new security risks to IT operations. Reports issued by the Government Accountability Office along with a Department of Homeland Security US-CERT advisory discuss multiple security issues concerning IPv6. According to GAO, IPv6 creates new opportunities for network abuse if IPv6 capable devices are not properly managed. Two IPv6 features—automatic configuration and tunneling—could present serious risks to federal agencies. Automatic configuration can facilitate network attacks because a rogue or unauthorized router may reconfigure neighboring devices by assigning them new addresses and routes. Tunneling can permit unauthorized traffic into the network undetected. The US-CERT alert warned federal agencies that unmanaged, or rogue, implementations of IPv6 present network management security risks. NARA's Impact Analysis did not address these security risks.	Page 8 / Paragraph 4	**We disagree and stand by our stated assertions for the verification tests. IPv6 was purposely not made operational, so these risks would not be incurred using our verification test approach. /** This paragraph is just a general statement of potential risks; it does not specify risks applicable to this project that were not effectively identified and mitigated. We do not believe that our testing scenarios exposed the agency to any auto configuring, tunneling, or poor IP management risks. This paragraph actually supports our rationale for not making IPv6 operational at this time, re: security. This is one reason we pursued a capabilities verification approach, and rolled it back.
The IPv6 Impact Analysis identified training costs for 15 NH employees involved in the IPv6 transition however, training has not been provided. According to GAO, a challenge to the transition will be maintaining dual IPv4 and IPv6 environments for extended periods of time. Maintaining two network protocols is challenging in that it adds	Page 8 / Paragraph 5 onto page 9	**IPv6 is not running in production operations so there is nothing to train at this time. /** In our opinion, the training requirement will not manifest itself until IPv6 goes into production operations. The engineers involved in the

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
complexity to network maintenance and associated costs are higher. It also requires skilled personnel and may be difficult to maintain hardware and software interoperability across dual environments. NARA IPv6 planning documents did not address this challenge		test did not require training because IPv6 was part of their skill-set. This paragraph actually supports our rationale for not making IPv6 operational at this time, re: operations complexity. This is one reason we pursued a capabilities verification approach, and rolled it back.
Recommendation 2 The Assistant Archivist for Information Services should update the IPv6 Impact Analysis to address the security and business risks associated with implementing IPv6.	Page 9 / Paragraph 4	**We agree with the recommendation, but this should be handled as part of the NARANET redesign project as per our stated strategy and OMB's new guidelines.** This should not be inferred as an issue of compliance with the past M-05-22 mandate requiring a specific impact analysis at a past point in time, which we did, in fact, provide. Additionally, risks associated with "implementing" IPv6 were not applicable to this project because there was no requirement or intent to "implement" IPv6 in production, just to verify certain IPv6 capabilities in the network core. We also assert that going forward; we need an impact analysis for the overall NARANET redesign, not just for IPv6 unto itself.
Recommendation 3 The Assistant Archivist for Information Services should ensure employees responsible for planning, implementing, maintaining, and securing an IPv6 network for NARA receives appropriate IPv6 training.	Page 9 / Paragraph 5	**We agree with the recommendation, but this should be handled as part of the NARANET redesign project as per our stated strategy and OMB's new guidelines.** This should not be inferred as an issue of compliance with the past M-05-22 mandate. We would note that this is not really a matter of training but rather a skill required for network engineers going forward – much like IPv4 currently.
In another example, NARA bought equipment in September 2005 that had to be upgraded or replaced in order for the devices to be IPv6	Page 11 / Last	**This is not a full characterization of what happened. /**

Detailed Responses to OIG IPv6 Audit Report No. 09-05, January 16, 2009

Report Statement	Page / Paragraph	Comment / Rationale
compliant. NARA spent $340,000 for 40 Cisco 3845 routers with accessories. The devices were not IPv6 capable because the router operating system did not have the feature pack needed to support IPv6 traffic. In September 2008, NARA spent $216,000 to purchase upgrades for the router operating systems, flash memory cards, and memory upgrades.	Paragraph	These upgrades were not only purchased for IPv6, but also to support the long term administration and management of Cisco's IOS enterprise-wide and to support the transition to MPLS under Networx.
Recommendation 4 The Assistant Archivist for Administration should direct the Director, Acquisitions Services Division to: a.) Develop standard contract language for all IT orders to require IT products and services be IPv6 compliant; and b.) Update the NARA Procurement Guide to require all acquisitions of IT hardware, software, and services be IPv6 compliant.	Page 12 / Paragraph 2	**While NA will provide a response to these recommendations, we have the following comments as to their context: /** Although we agree that we should try to acquire IPv6 capable products and services, we need to recognize that some product vendors and service providers may not provide products that are fully IPv6 capable at this time, and some segments of the market like ISPs, IP telephony vendors, security product vendors, and middleware vendors have not yet transitioned to IPv6. As stated in the very last paragraph of the IPv6 Closeout Report: "It may not make sense to re-engineer and upgrade platforms having a five year life expectancy to support a technology that is not expected to attain wide-scale adoption for five to ten years." NARA needs to be careful not to prohibit the use of products and services needed to support today's business operations because they don't yet support an implementation requirement that may be more than 5 years in the future. OMB M-05-22 actually states that: "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…"