Report No. DODIG-2015-044

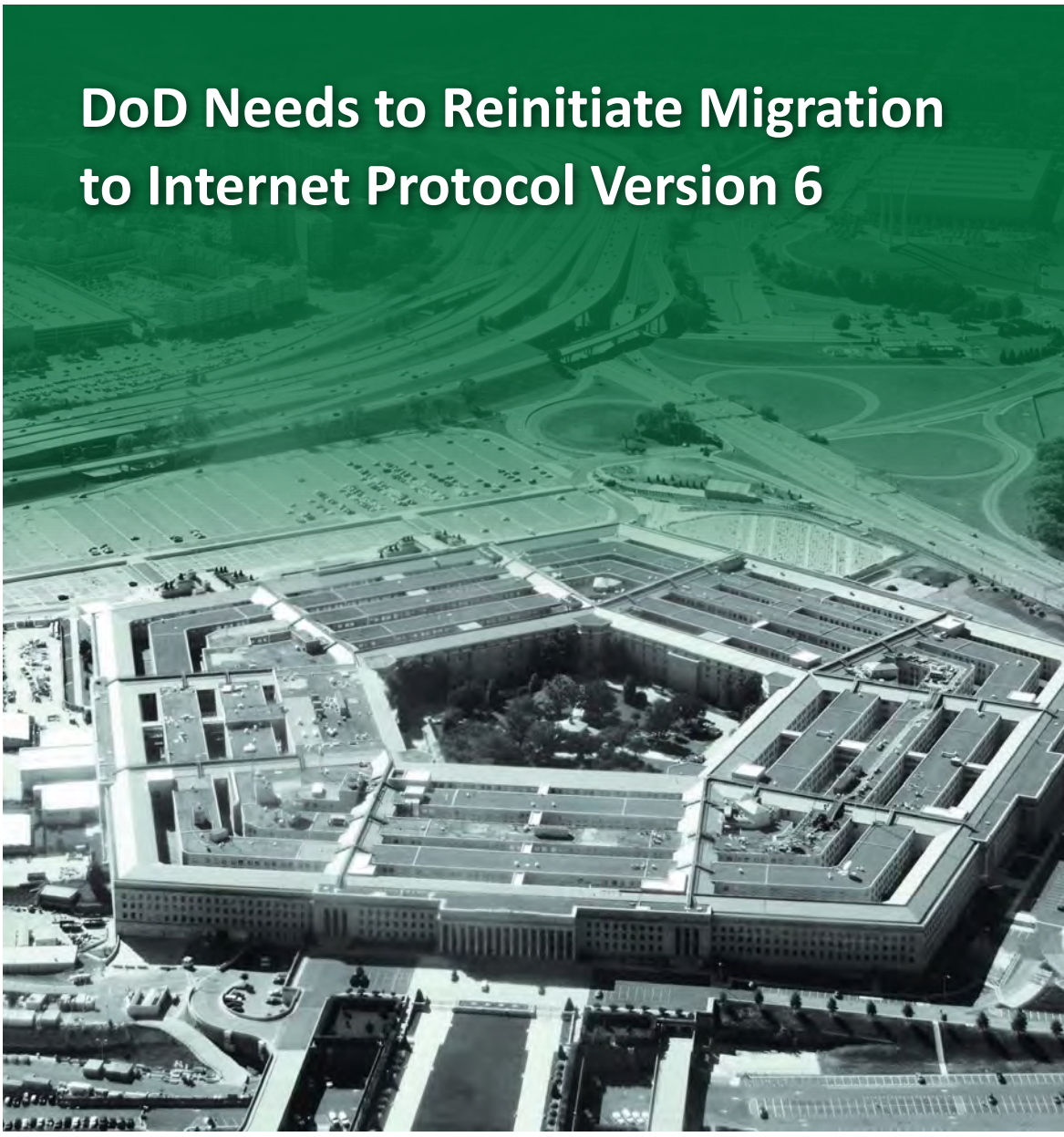
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 1, 2014

DoD Needs to Reinitiate Migration to Internet Protocol Version 6



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~FOR OFFICIAL USE ONLY~~

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 DEC 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
DoD Needs to Reinitiate Migration to Internet Protocol Version 6 (REDACTED)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Department of Defense Inspector General,4800 Mark Center Drive,Alexandria,VA,22350-1500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**52**	

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

DoD Needs to Reinitiate Migration to Internet Protocol Version 6

December 1, 2014

Objective

We determined whether DoD was effectively migrating to Internet Protocol Version 6 (IPv6).

Finding

Although DoD satisfied the requirement to demonstrate IPv6 on the network backbone by June 2008, DoD did not complete the necessary Federal and DoD requirements and deliverables to effectively migrate the DoD enterprise network to IPv6. This occurred because:

- DoD Chief Information Officer (CIO) and U.S. Cyber Command (USCYBERCOM) did not make IPv6 a priority;
- DoD CIO, USCYBERCOM, and Defense Information Systems Agency (DISA) lacked an effectively coordinated effort and did not use available resources to further DoD-wide transition toward IPv6; and
- DoD CIO did not have a current plan of action and milestones to advance DoD IPv6 migration.

As a result, DoD is not realizing the potential benefits of IPv6, including to battlefield operations. Furthermore, the delay in migration could increase DoD's costs and its vulnerabilities to adversaries.

Visit us at www.dodig.mil

Management Action Taken

On June 24, 2014, DoD IPv6 representatives met to discuss concerns and how best to authorize IPv6 on DoD networks. The group agreed to begin a limited deployment of IPv6 in October 2014, analyze results, and incrementally expand the deployment as conditions and results permit.

Recommendations

We recommend the DoD CIO:

- establish a DoD-wide IPv6 transition office and working groups to more effectively advance DoD's transition to IPv6;
- coordinate with the Commander, USCYBERCOM; Director, DISA; Commander, U.S. Army Information Systems and Engineering Command; Director, High Performance Computing Modernization Program; and other DoD test and evaluation components to establish a process to ensure test results and lessons learned are integrated into DoD IPv6 migration efforts;
- coordinate with the Commander, USCYBERCOM and the Director, DISA, to develop new DoD IPv6 transition milestones, roles and responsibilities, and enforcement mechanisms to ensure successful migration to IPv6; and
- monitor status of IPv6 milestones established above and elevate any delays to the Deputy Secretary of Defense.

Management Comments and Our Response

Comments from the Acting Principal Deputy DoD CIO fully addressed the recommendations and no additional comments are required. Additionally, we received unsolicited comments from the Director, C4 Systems and CIO Support (J6), USCYBERCOM. Please see the Recommendations Table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
DoD Chief Information Officer		1, 2, 3, 4

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

December 1, 2014

MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER

SUBJECT: DoD Needs to Reinitiate Migration to Internet Protocol Version 6 (IPv6) (DODIG-2015-044)

We are providing this report for your information and use. DoD has not met requirements to migrate the DoD enterprise network to IPv6. Consequently, DoD is not realizing the potential benefits of IPv6, including to battlefield operations, and could experience increased costs from further delays and increased vulnerability from adversaries.

We considered management comments on a draft of this report when preparing the final report. Comments from the Acting DoD Principal Deputy Chief Information Officer fully addressed all recommendations and conformed to the requirements of DoD Directive 7650.3; therefore, we do not require additional comments.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

Contents

Introduction

Objective

Our objective was to determine whether DoD was effectively migrating to Internet Protocol Version 6 (IPv6). See Appendix A for a discussion of our scope and methodology and prior audit coverage and the glossary for specialized terms used throughout the report.

Background

The Internet Protocol (IP) is a technical standard that enables computers and other devices to communicate with each other over networks, many of which interconnect to form the Internet. IP provides a standardized "envelope" that carries addressing, routing, and message-handling information, enabling the transmission of a message from its source to its destination over the interconnected networks that make up the Internet. Released in 1978, IP version 4 (IPv4) was the first stable version of the IP based on a 32-bit address format, which provides approximately 4.3 billion IP addresses. With the success of the Internet has come great demand for IP addresses, thereby exhausting the supply of available IPv4 addresses. On February 3, 2011, the Internet Assigned Numbers Authority issued the remaining IPv4 address blocks, thereby exhausting the supply of IPv4 addresses.

In response to the IPv4 address shortage, the Internet Engineering Task Force[1] developed IPv6, which has a vastly expanded address space. IPv6 addresses are composed of 128 bits, which equates to 340 trillion trillion trillion IP addresses. Although the shortage of IPv4 addresses has not been the primary driver for IPv6 migration in DoD (which has about 18 percent of the world's available IPv4 addresses), the greatly expanded address space provides an opportunity to redesign the DoD address space to better accommodate future increased use of networked sensors and mobile devices. Additionally, DoD Component networks enabled by IPv6 will support greater information sharing, resulting in improved military effectiveness. Regions around the world that have limited IPv4 address space, such as Asia and Europe, have undertaken efforts to develop, test, and implement IPv6.

[1] The Internet Engineering Task Force is the international community responsible for producing the Internet's technical standards.

Preferred IPv6 Transition Mechanism

The preferred mechanism for transitioning to IPv6 is to operate a dual stack network in which hosts and routers implement both IPv4 and IPv6. DoD has chosen dual stack as its IPv4 to IPv6 transition strategy. Figure 1 below depicts how dual stack networks can support both IPv4 and IPv6 services and applications during the transition period.

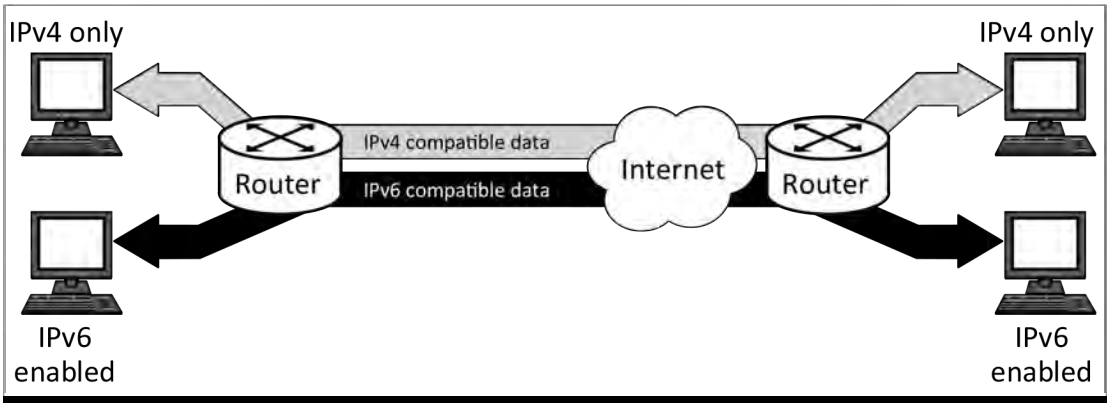


Figure. Dual Stack Network
Source: Government Accountability Office

Federal and DoD IPv6 Migration Guidance

On June 9, 2003, the DoD Chief Information Officer (CIO) issued the memorandum, "Internet Protocol Version 6 (IPv6)," stating that DoD's implementation of IPv6 is necessary because IPv4 has limitations that make it unable to meet long-term commercial and DoD requirements. The memorandum initiated DoD's transition to IPv6, with the goal to complete IPv6 transition by FY 2008. On August 2, 2005, the Office of Management and Budget (OMB) issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," (OMB M-05-22) to guide the Federal Government in its transition to IPv6. OMB M-05-22 outlined a transition strategy for Federal agencies to follow and established the goal for all network backbones to support IPv6 by June 30, 2008. The Federal Chief Information Officers Council Strategy and Planning Committee's "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government, Version 2.0," July 2012, states Federal agencies achieved the objectives of the 2005 OMB memorandum but noted that continued adoption of IPv6 within Federal enterprises required additional guidance. Furthermore, due to the complexities of full-enterprise transitions, OMB released a later memorandum, "Transition to IPv6," September 28, 2010, which includes specific completion requirements for FY 2012 and FY 2014.

DoD Key Offices Responsible for IPv6 Migration

DoD's key offices for IPv6 migration include the DoD CIO, the Defense Information Systems Agency (DISA), and U.S. Cyber Command (USCYBERCOM).[2] According to the "Department of Defense Internet Protocol Version 6 Transition Plan, Version 2.0," June 2006, the DoD CIO has overall responsibility for ensuring a coherent, timely transition to IPv6 across the Department that ensures interoperability and security and for issuing policy as needed. DISA is responsible for planning and implementing IPv6 on the Defense Information Systems Network Non-classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network. Additionally, DISA is responsible for acquiring, allocating, and managing IPv6 address space for DoD; conducting interoperability tests and certification for IPv6 products and capabilities; and ensuring, in conjunction with the National Security Agency (NSA), that IPv6 information assurance problems are identified and included in transition efforts. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified DoD information networks. USCYBERCOM is also responsible for conducting full spectrum military cyberspace operations to enable actions in all domains, and USCYBERCOM approval is necessary to enable IPv6 on the NIPRNet.

Review of Internal Controls

DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses relating to DoD's migration to IPv6. Specifically, DoD CIO and USCYBERCOM did not make IPv6 a priority and DoD's key offices for IPv6 migration lacked effective communication and did not properly plan to ensure the required resources were available to implement IPv6. Moreover, the DoD CIO did not update "The Department of Defense Internet Protocol Version 6 Transition Plan, Version 2.0," June 2006 (DoD IPv6 Transition Plan) to include revised requirements and additional roles and responsibilities for IPv6 migration. We will provide a copy of this report to the senior official responsible for internal controls in DoD CIO, DISA, and USCYBERCOM.

[2] USCYBERCOM was formed in 2010 by consolidating two of U.S. Strategic Command's subordinate organizations: Joint Functional Component Command–Network Warfare and Joint Task Force–Global Network Operations.

Finding

DoD Is Not Effectively Migrating to IPv6

Although DoD satisfied the OMB M-05-22 requirement to demonstrate IPv6 on the network backbone by June 2008, DoD did not complete the Federal and DoD requirements and deliverables to effectively migrate the DoD enterprise network to IPv6. This occurred because:

- DoD CIO and USCYBERCOM did not make IPv6 a priority;
- DoD CIO, DISA and USCYBERCOM, lacked an effectively coordinated effort and did not use available resources to further DoD-wide transition toward IPv6 operations; and
- DoD CIO did not have a current plan of action and milestones to advance DoD IPv6 migration efforts.

As a result, DoD is not realizing the potential benefits of IPv6, including to battlefield operations.[3] Furthermore, the delay in migration could increase DoD's costs and its vulnerability to adversaries.

[3] Battlefield operations include the movement, supply, attack, defense, and maneuvers needed to win any battle or campaign. See Appendix B for an illustration.

DoD Temporarily Demonstrated IPv6 on Network Backbone

DoD satisfied the OMB M-05-22 requirement to demonstrate IPv6 on the network backbone but disabled IPv6 functionality following the demonstration. As required by OMB M-05-22, the DoD CIO designated an IPv6 Transition Manager to lead and coordinate planning efforts to transition DoD's network backbone infrastructure by 2008. DISA, which manages the NIPRNet, assessed and determined the backbone configuration changes which were required to make the infrastructure IPv6 capable.

~~(FOUO)~~ In FY 2008, DoD satisfied the OMB M-05-22 requirement by temporarily demonstrating IPv6 capability on the NIPRNet through a series of tests. [redacted] Although the successful demonstration of IPv6 on NIPRNet was an important milestone, DoD CIO documented that further

~~(FOUO)~~ security implementation guidance and certified information assurance devices must be available before enabling IPv6 on the NIPRNet. According to the DoD IPv6 transition manager, DoD disabled IPv6 functionality following the demonstration, due to a lack of trained personnel and potential security risks.

DoD Did Not Complete Federal and DoD IPv6 Migration Requirements and Deliverables

Although DoD temporarily demonstrated the OMB M-05-22 requirements in 2008, DoD has not met later OMB requirements to support enterprise networks to operationally use native[4] IPv6. In addition, DoD Components have not completed the Federal and DoD requirements and deliverables to effectively migrate to IPv6.

OMB IPv6 Migration Requirements Not Met

DoD did not meet OMB's FY 2012 and FY 2014 IPv6 requirements. On September 28, 2010, OMB issued a memorandum for all Executive Branch Department and agency CIOs titled, "Transition to IPv6," which emphasized the Federal Government's commitment to the operational deployment and use of IPv6. The memorandum listed deadlines that each Federal agency was required to meet by the end of FY 2012 and FY 2014 to facilitate timely and effective IPv6 adoption. By the end of FY 2012, agencies were required to upgrade their public/external facing servers and services, such as Web, e-mail, and domain name systems, to operationally use native IPv6. By the end of FY 2014, agencies were required to upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6. However, DoD did not meet either FY requirement.

DoD did not meet OMB's FY 2012 and FY 2014 IPv6 requirements.

As of December 2013, according to the Director, Architecture and Interoperability, Office of the DoD CIO, the new estimated date for meeting the FY 2012 requirement was June 2014 for e-mail and domain name systems and September 2015 for the Web. Likewise, the Director stated that DoD would have the infrastructure available to provide internal IPv6 access to public Internet servers through IPv6-enabled and -protected Defense Enterprise Computing Centers in FY 2015. However, as of April 28, 2014, representatives from DoD CIO, DISA, and USCYBERCOM stated that a DoD IPv6 pilot must be created before DoD can begin to implement IPv6 on the network. The USCYBERCOM director of Command, Control, Communications, and Cyber Systems and CIO Support stated the pilot was

[4] Native IPv6 means transition to IPv6 without the use of translators, tunnels (IPv4 carrying IPv6). End users can communicate entirely via IPv6.

necessary to enable secure implementation of IPv6. As of July 10, 2014, according to DoD CIO officials, the estimated completion dates for OMB's requirements were no longer valid and revised dates were dependent on the IPv6 pilot results.

DoD-Wide IPv6 Migration Efforts Are Lacking

DoD-wide IPv6 migration efforts are lacking, although some DoD Components have taken steps to comply with Federal and DoD IPv6 requirements. For example, officials from the Navy's Program Executive Officer for Command, Control, Communications and Intelligence stated that Navy acquisition program offices key to enabling IPv6 have procured IPv6 capable devices and conducted lab network testing since 2006. The Space and Naval Warfare Systems Command, according to its Program Executive Office Tactical Networks Technical Director, requires operational testing on the DoD DISA-operated network to continue IPv6 migration efforts. However, DISA does not have an estimated time when the DoD network will be made available for IPv6 operational testing.

Since 2005, Federal and DoD policies mandate the completion of several key requirements and deliverables to facilitate an effective IPv6 migration.

- OMB-M-05-22, states agencies must complete an inventory of existing routers, switches, and hardware firewalls, and begin an inventory of all other existing IP-compliant devices and technologies by November 2005.
- "DoD IPv6 Transition Plan, Version 2.0," June 2006, requires each DoD Component to ensure an IPv6 Transition Plan is developed that includes network transition strategies, transition activities, and timelines.
- "DoD IPv6 Transition Plan, Version 2.0" also states DoD Components must establish an IPv6 Transition Office to manage IPv6 transition within the DoD Component.
- DoD CIO memorandum, "DoD Internet Protocol Version 6 (IPv6) Implementation," February 6, 2008, requires DoD Components to include IPv6 transition resource requirements in Program Objective Memorandum submissions for FY 2010 and beyond to effectively prioritize IPv6 resources and efforts across DoD.
- "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government, Version 2.0" states that developing and maintaining an Agency Addressing Plan encompassing IPv4 and IPv6 plans will help speed up the deployment of IPv6.

However, some DoD Components have not completed these IPv6 requirements or developed the key IPv6 deliverables to prepare for migration and are therefore

not ready to migrate. The table below provides the status of the specific DoD Components that we reviewed—Army, Navy, Air Force, Washington Headquarters Services/Mark Center, and the Defense Logistics Agency—in completing the requirements and critical IPv6 initiatives.

Table. DoD Component Status in Completing IPv6 Requirements and Developing Key IPv6 Deliverables

Requirements & Deliverables	Army	Navy	Air Force	Washington Headquarters Services/ Mark Center	Defense Logistics Agency
Complete Inventory of IP-Compliant Devices	No; inventory was complete February 2013 but no support provided for complete inventory.	No; officials stated Navy maintains inventory of IP-compliant devices but provided no documentation.	No	Yes	Yes
IPv6 Transition Plan	No, officials provided a draft 2004 plan, but as of August 2014, that plan was not approved.	Yes	No	No; officials stated they were waiting for a transition plan to be completed by their service provider.	No*
IPv6 Transition Office	No; officials established IPv6 working group and transition was up to individual commands.	No; its transition office closed FY 2012.	No; its transition office closed in 2012.	No	No; officials working to establish an IPv6 transition team.
Program Objective Memorandum for IPv6 Transition Resources	No; officials plan to develop a budget estimate for first quarter FY 2015.	No	No	No; officials stated they submitted a POM request, but it was not approved.	No
IPv6 Addressing Plan	No; officials provided a draft 2012 plan, but as of August 2014, that plan was not approved.	Yes, but it requires updating.	Yes, but it requires updating.	No; officials stated they are waiting for an addressing plan to be completed by their service provider.	Yes

* Officials provided a 2012 IPv6 Implementation Guide, however an IPv6 Transition Plan has not been completed.

IPv6 Migration Was a Low Priority

DoD's key offices responsible for IPv6 migration did not make IPv6 a high priority. Specifically, the DoD CIO did not maintain a DoD IPv6 transition office or working group to advance DoD IPv6 migration, and the USCYBERCOM division chief of Cyber Operations Planning stated USCYBERCOM was focused on defense of the IPv4 network and that there was no operational imperative for DoD to move to IPv6.

DoD CIO Did Not Maintain a Transition Office or Working Group to Advance IPv6 Migration

The DoD CIO, responsible for ensuring a coherent and timely IPv6 migration, did not maintain an IPv6 transition office or working group to advance DoD's IPv6 implementation. In March 2004, DISA, at the request of the DoD CIO, established the DoD IPv6 Transition Office (DITO) to ensure a comprehensive, timely transition with responsibility for developing common engineering solutions and guidance. In addition, the DITO was responsible for coordinating transition planning and implementation efforts across the DoD to reduce transition costs and avoid duplicative efforts. However, upon completion of development, engineering, and technical guidance required for the IPv6 transition, the DoD CIO released DISA from the DITO mission in July 2011, rather than directing the DITO to continue coordinating IPv6 implementation efforts throughout DoD.

According to the technical advisor to the Air Force CIO, DITO helped to focus the Military Services on the goal of IPv6 implementation, and once the DITO was disestablished, the Services lost focus on IPv6 efforts. Therefore, maintaining the DITO would have helped to address emergent technical issues and assist DoD Components in meeting IPv6 implementation objectives. During a meeting with DoD's key offices and Service personnel responsible for IPv6 in April 2014, other DoD Components also agreed that reestablishment of working groups would be beneficial to DoD's IPv6 migration. To help facilitate the implementation of IPv6 in DoD, the DoD CIO should establish the DoD-wide IPv6 transition office and working groups.

...once the DITO was disestablished, the Services lost focus on IPv6 efforts.

USCYBERCOM Focused on IPv4

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted] The division chief also stated IPv6 was not a priority and that USCYBERCOM believed DoD did not have an operational imperative to move to IPv6. However, select combatant commands have shown a need for IPv6. [redacted] In response to USPACOM's request, DISA provided a plan to enable pilot connections by March 1, 2014. However, according to the USPACOM CIO, DISA missed the March 2014 deadline for enabling IPv6.

The USCYBERCOM director of Command, Control, Communications, and Cyber and CIO Support stated funding constraints contributed to USCYBERCOM's lack of priority for IPv6. The division chief stated that because USCYBERCOM was not fully aware of the potential risks in transitioning to IPv6 or in protecting the IPv6 network, it prioritized funds to protect the current IPv4 network. The OMB IPv6 chief architect said that based on his meetings with DoD IPv6 representatives, he believes IPv6 was not given exposure or priority by senior DoD leaders. Additionally, the chief engineer of the Defense Research and Engineering Network (DREN)—who has achieved IPv6 operations on the DREN (which is separate from the NIPRNet)—stated that DoD is focusing only on short-term benefits IPv6 can bring to the Department. The chief engineer (also the network security manager for Space and Naval Warfare Systems Command and a Federal IPv6 Task Force member) added that DoD needs to take steps toward transitioning to IPv6 operations but must start now to gain the experience necessary for successful transition.

[5] The Joint Information Environment is a secure environment, comprising shared information technology infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize information technology efficiencies.

IPv6 Migration Efforts Not Effectively Coordinated

~~(FOUO)~~ The DoD CIO, DISA, and USCYBERCOM, have not effectively coordinated their IPv6 migration efforts. [redacted] In addition, DoD CIO and USCYBERCOM did not coordinate their use of testing resources.

~~(FOUO)~~ The DoD CIO, DISA, and USCYBERCOM, have not effectively coordinated their IPv6 migration efforts.

Ineffective Coordination Impeded IPv6 Migration

~~(FOUO)~~ DoD CIO, DISA, and USCYBERCOM did not conduct effective coordination to move forward with DoD's IPv6 implementation. In April 2011, the DoD IPv6 transition manager issued the "DoD Implementation Plan for OMB FYs 2012 and 2014 IPv6 Requirements," which identified security problems as a primary planning concern and critical dependency for the DoD IPv6 implementation. To assess the security risks associated with OMB's FY 2012 IPv6 requirement, the DoD CIO directed the NSA to conduct a DoD enterprise-wide risk analysis. In July 2011, the NSA Information Assurance Directorate concluded that the FY 2012 IPv6 requirements do not present a significant additional security risk. In addition NSA concluded that extensive documentation exists for securely implementing IPv6. [redacted]

~~(FOUO)~~ According to the technical director for the NSA Information Assurance Directorate, the main concern at that time (FY 2011) was that defensive systems and sensors had not yet evolved to include IPv6 functionality. However, as of March 2014, those tools are IPv6-capable. The DoD IPv6 transition manager stated the DoD CIO has been requesting a communications tasking order since November 2012, but USCYBERCOM has not changed its position or elaborated on its IPv6 security concerns, other than to suggest the need for further pilot testing. As of February 2014, DISA had no meetings scheduled with USCYBERCOM to discuss

[6] A communications tasking order is a method to communicate to components, specific instructions for what they need to accomplish a certain mission.

~~(FOUO)~~ ways to solve problems. In fact, the DISA IPv6 lead stated that the two groups have met only once to discuss IPv6 since he took over DISA IPv6 efforts in December 2013. [redacted] Conversely, the Director, C4 Systems and CIO Support (J6) stated that DISA and USCYBERCOM met once and talked on the phone twice during this period. However, the DISA IPv6 lead was unaware of the meeting and phone conversations.

DoD CIO and USCYBERCOM Did Not Ensure Effective Use of DoD Resources in IPv6 Migration

Although the DoD CIO, DISA, and USCYBERCOM met in February 2014 to discuss strategy and the status of DoD's IPv6 migration, they did not coordinate to ensure effective use of available resources, such as DREN lessons learned or test results from the Army Technology Integration Center (TIC). For example, USCYBERCOM officials stated that one of the biggest risks of IPv6 transition was a lack of knowledge about IPv6 and the need for pilot testing before implementation. However, in 2003, the DoD CIO designated the High Performance Computing Modernization Program's (HPCMP)[7] DREN[8] as the first DoD IPv6 pilot network to ensure their best practices could help facilitate the DoD-wide IPv6 implementation. The entire DREN wide-area network routinely supported end-to-end IPv6 traffic, several sites supported IPv6 and IPv4 (dual stack), and selected applications were IPv6 enabled by July 2005. In 2009, the DREN completed their transition from an IPv4 network which supports IPv6 to an IPv6 network with legacy IPv4 support. According to a 2009 HPCMP point paper, the DREN accomplished the IPv6 transition without additional personnel and with less than $100,000 in additional funding. The point paper also noted that performance and security were as good as and in some ways better than pre-IPv6 pilot levels. According to the HPCMP Associate Director for Networking, the DREN backbone and several sites are now fully dual stack and all management of network infrastructure is accomplished using IPv6.

In addition to the DREN, the DISA Joint Interoperability Test Command (JITC) tests and certifies information technology products for IPv6 capabilities, and the Army TIC tests security and monitoring devices, including penetration testing for IPv6. Specifically, the JITC tests DoD vendors' equipment for IPv6 functionality and to ensure IPv6 performs at least as well as IPv4 (functional parity). According to a JITC electronic engineer, by 2009, JITC had more than 100 vendors participating

[7] HPCMP is an Office of the Secretary of Defense program managed, since 2011, by the U.S. Army Corps of Engineers.

[8] DREN is an element of the DoD HPCMP, and was formed from elements of the Army, Air Force, and Navy supercomputing networks to be the DoD's premier research, development, test, and evaluation network connecting DoD high-performing computing centers with users.

in IPv6 functionality testing. Furthermore, according to Army TIC personnel, the TIC tests vendor claims about security and tested firewalls, intrusion-detection systems, intrusion-prevention systems, and network controls, including a comparison of IPv4 and IPv6. Once testing is completed, TIC analyzes the data, determines whether or not the equipment passed and reports the results to the Army Certification Authority to issue a certificate. The certificate certifies that the device tested meets IPv6 Capable Simple Server interoperability requirements. The Army TIC also set up an IPv6 lab, which ran performance tests to compare a dual stack environment with a native IPv6 environment. As of July 7, 2014, there were 88 special interoperability test certification memorandums issued for IPv6 capability. USCYBERCOM expressed concerns over enabling IPv6 but has not used any of the test results nor communicated with the DREN, JITC, or Army TIC. Likewise, DISA had not used the lessons learned from the DREN. The DoD CIO should coordinate with Components to establish a process to ensure these testing resources and lessons learned are used to effectively advance DoD's IPv6 migration.

Plans for Migrating to IPv6 Not Updated

DoD CIO has not updated the June 2006 DoD IPv6 Transition Plan, which stated that DoD CIO is responsible for approving and updating the DoD IPv6 Transition Plan and updates. The June 2006 DoD IPv6 Transition Plan contained the overall strategy for IPv6 transition, identified roles and responsibilities of DoD Components, and outlined IPv6 milestones. However, the DoD CIO did not update the plan to include the roles and responsibilities of USCYBERCOM, which was established in 2009. The DoD IPv6 Transition Plan also contained a governance structure for addressing critical aspects of the transition; this structure consisted of the working groups and the DITO, which no longer exist. Furthermore, DoD has not met the milestones established in the plan, the last of which was for Components to be authorized to operate IPv6 enterprise-wide by FY 2008.

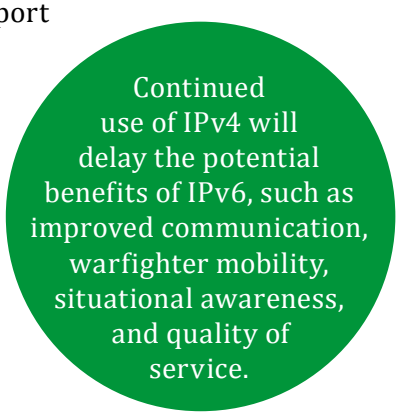
In addition, DoD's IPv6 implementation plan, issued in April 2011, contained the methodology and actions to coordinate and guide the DoD's efforts for compliance with the OMB FY 2012 IPv6 requirements and laid groundwork for compliance with FY 2014 requirements. However, DoD did not accomplish the FY 2012 and FY 2014 requirements to operationally enable native IPv6. Although the requirements were not met by the planned dates, DoD has not issued an updated implementation plan. The DoD CIO, in coordination with DISA, and USCYBERCOM should develop new milestones, roles and responsibilities, and enforcement mechanisms to provide DoD with a detailed approach to further IPv6 migration.

IPv6 Benefits Not Realized

DoD is not realizing IPv6 potential benefits to DoD operations, such as the ability to improve situational awareness for warfighters and commanders during battle maneuvers. See Appendix B for an illustration of the improved battlefield operations. Additionally, DoD could experience increased costs of IPv6, due to the delay in migration and increased risk from adversaries attempting to exploit DoD networks.

Delayed Benefits of IPv6 in Battlefield Operations

Continued use of IPv4 will delay the potential benefits of IPv6, such as improved communication, warfighter mobility, situational awareness, and quality of service. IPv4 is unable to meet the future requirements of battlefield operations. Cyber and IPv6 subject matter experts agree that IPv4 cannot support future networking and combat system demands. For example, according to the DoD IPv6 transition manager, it took 2 months to create an operational network in Iraq using IPv4, whereas using IPv6 would have allowed this network to be created in hours. Secure ad hoc networking and mobility provided by IPv6 auto-configuration capabilities, as well as improved end-to-end security and simplified network management capabilities, enable individuals and entire units to disconnect from military base networks, travel into theater, and quickly establish communications. Additionally, IPv6 capabilities will allow warfighters and commanders to improve situational awareness during deployment and battle operations allowing units to securely move from one wireless network to another.



Further Delay Could Raise IPv6 Migration Costs and Increase Risk from Adversaries

The longer DoD waits to migrate to IPv6, the more expensive the migration will become. In October 2007, the DoD IPv6 transition manager prepared a white paper to document benefits of IPv6 migration. He stated that the longer DoD delays IPv6 implementation, the more embedded IPv4 will become in critical mission systems. The result will be increased transition difficulty, complexity, and cost. He also stated in June 2014 that this information is still accurate. Furthermore, adversaries are gaining experience using IPv6, and DoD's delayed migration is

leaving network security personnel without the expertise to identify malicious activity in the new IPv6 environment. According to the DoD IPv6 transition manager and Federal CIO Council personnel, China is forging ahead with native IPv6 implementations.

Management Actions Taken During the Audit

On April 28, 2014, a meeting was held between DoD CIO, DISA, USCYBERCOM, NSA, DREN, Army, Navy, Air Force, and Marine Corps personnel to discuss DoD's IPv6 migration. The DoD CIO led the meeting and requested input from the other DoD Components on the migration. Specifically, the participants discussed the actions necessary to enable DoD's IPv6 migration and to develop a plan to solve IPv6 implementation problems. As a result, the DoD CIO assumed responsibility for gathering input from the Components and for beginning the planning for a DoD IPv6 pilot implementation.

On June 24, 2014, representatives from DoD CIO, DISA, USCYBERCOM, NSA, DREN, Army, Navy, and Marine Corps met to discuss IPv6 cybersecurity concerns and how best to authorize IPv6 on DoD networks. The group agreed to begin a limited deployment of IPv6 in October 2014, analyze cybersecurity results, and incrementally expand the deployment as conditions and results permit. The group set January 31, 2015, as the deadline for analyzing the results and recommending a way forward to the DoD CIO. We commend the DoD CIO and the other participants for taking steps to reinitiate IPv6 transition efforts across the Department. However, the DoD CIO should also establish the DoD IPv6 transition office and its associated working groups to further ensure coordination of Component IPv6 implementation efforts. In addition, the DoD CIO, who has overall responsibility for ensuring a timely IPv6 transition across the Department, should closely monitor and enforce the achievement of established IPv6 implementation milestones and hold Components accountable for any delays.

Management Comments on the Finding and Our Response

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, provided comments on sections of the finding, which are summarized below. For the full text of the Acting Principal Deputy's comments, see the Management Comments section of the report. Although not required to comment, the Director, C4 Systems and CIO Support (J6), USCYBERCOM also provided comments. See Appendix C for USCYBERCOM comments and our responses and for the full text of the Director's comments, see the Management Comments section of the report.

Management Comments on Not Making IPv6 a Priority

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, disagreed that DoD CIO and USCYBERCOM did not make IPv6 a priority, stating IPv6 is a DoD priority but conducting an expensive transition from IPv4 to an IPv6 environment is neither cost effective nor warranted. He also stated there is no DoD Component operational imperative or business case to implement IPv6.

Our Response

~~(FOUO)~~ We disagree that IPv6 implementation is not warranted. As stated in this report, OMB issued a memorandum for all Executive Branch Department and agency CIOs titled, "Transition to IPv6," September 28, 2010, which listed deadlines that each Federal agency was required to meet by the end of FY 2012 and FY 2014 to facilitate timely and effective IPv6 adoption. DoD did not meet OMB's FY 2012 and FY 2014 IPv6 requirements. [redacted]

Management Comments on Lack of Effective Coordination and Use of Available Resources to Further IPv6 Migration

The Acting Principal Deputy DoD CIO disagreed that the DoD CIO, DISA, and USCYBERCOM lacked an effectively coordinated effort and did not use available resources to further DoD-wide transition toward IPv6 operations. He said the Department effectively coordinated with all Components to ensure networks were capable of using IPv6. He stated the DoD CIO is collaborating with DISA and USCYBERCOM to develop an updated plan of action and milestones, which include development of a limited IPv6 deployment plan in the first quarter of FY 2015. With respect to the use of available resources, the Acting Principal Deputy DoD CIO stated that the Department leveraged and will continue to leverage available test and evaluation resources as the DoD IPv6 implementation evolves.

Our Response

We commend the Department for coordinating with all Components to ensure networks are capable of using IPv6. However, the criterion we used to determine whether DoD was effectively migrating to IPv6 was OMB memorandum, "Transition to IPv6," September 28, 2010. The OMB memorandum listed deadlines that each Federal agency was required to meet by the end of FY 2012 and FY 2014 to facilitate timely and effective IPv6 adoption.

Additionally, we disagree with the Acting Principal Deputy DoD CIO's comments that DoD CIO, DISA, and USCYBERCOM have used available resources to further DoD-wide IPv6 implementation. As we state in this report, USCYBERCOM officials stated one of the biggest risks of IPv6 transition was a lack of knowledge about IPv6 and the need for pilot testing before implementation. However, the IPv6 transition experience gained by the DREN as far back as 2003 was not fully considered.

Management Comments on Lack of Plan of Action and Milestones for IPv6 Migration

The Acting Principal Deputy DoD CIO partially agreed that the DoD CIO did not have a current plan of action or milestones to advance DoD IPv6 migration efforts. He stated that DoD developed a transition plan in 2006 and a follow-on plan of action and milestones in 2011 advancing IPv6 implementation efforts. He stated the 2011 plan of action and milestones are still relevant but that the timelines and scope have changed as a result of evolving technology and cyber threats. DoD CIO is revisiting development of a limited IPv6 deployment plan with DISA and USCYBERCOM by the 2nd quarter of FY 2015 and development of an updated plan of action and milestones.

Our Response

Although we requested that the DoD IPv6 transition manager provide a copy of the most current plan of action and milestones for IPv6 implementation, we were not provided with the 2011 plan. Therefore, we could not determine whether the plan of action and milestones were still relevant. However, in the Acting Principal Deputy DoD CIO's comments to Recommendation 3, he stated that the DoD CIO will draft and coordinate a memorandum with transition milestones, roles, responsibilities, and enforcement mechanisms for each DoD office involved in the IPv6 implementation. That action will address the need for an updated plan.

Additional Management Comments

The Acting Principal Deputy DoD CIO included in his comments, a copy of a Department of the Navy Deputy CIO memorandum, which was provided to the OIG on May 9, 2014. The Acting Principal Deputy DoD CIO stated that information provided in the Department of Navy memorandum was not taken into account in the final draft report. The Acting Principal Deputy DoD CIO also stated that the Navy recommended, during the review of the discussion draft report, that the OIG aggregate interview responses from individual commands to the Military Service level.

Our Response

The DoD OIG fully considered the Department of the Navy Deputy CIO memorandum's statement that the Navy has maintained an inventory of IP-compliant devices and technologies since 2009. However, we did not receive any supporting documentation to verify that the Navy completed an inventory of existing IP-compliant devices and technologies as required by OMB Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005. Additionally, the OIG requested clarification from the Navy IPv6 point of contact regarding aggregation of responses from individual commands to the Military Service level but did not receive a response.

Recommendations, Management Comments, and Our Response

We recommend DoD Chief Information Officer:

Recommendation 1

Establish a DoD-wide Internet Protocol Version 6 transition office and working groups to advance DoD's transition to Internet Protocol Version 6. At a minimum, working groups should include representation from Defense Information Systems Agency, U.S. Cyber Command, Defense Research and Engineering Network, and Service Chief Information Officers.

DoD Chief Information Officer Comments

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, disagreed, stating there is no need for a DoD IPv6 transition office with dedicated resources. He said the DoD has adopted a more agile and resource-efficient approach by establishing a steering group to coordinate Department IPv6 implementation actions, address cybersecurity problems, and define the way forward to obtain authorization of IPv6 on DoD networks. The steering group is led by the DoD CIO and consists of representatives from DISA, USCYBERCOM, DREN, and Military Department CIOs. Additionally, DISA has established an Integrated Project Team to address the technical aspects required to implement IPv6 actions.

Our Response

Although the Acting Principal Deputy DoD CIO disagreed with the recommendation, the establishment of a steering group fully addressed the intent of the recommendation, and no further comments are required.

Recommendation 2

In coordination with the Commander, U.S. Cyber Command; the Director, Defense Information Systems Agency; the Commander, U.S. Army Information Systems and Engineering Command/Army Technology Integration Center; the Director, High Performance Computing Modernization Program/Defense Research and Engineering Network; and other DoD test and evaluation components, establish a process to integrate component testing results and lessons learned into DoD Internet Protocol Version 6 migration efforts.

DoD Chief Information Officer Comments

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, agreed, stating the DoD CIO will continue to work with the various test centers to assess IPv6 threats and develop appropriate countermeasures. Additionally, he stated the DISA Integrated Project Team will integrate component testing results and lessons learned to guide IPv6 implementation efforts and inform the pace, scope, and timing of the IPv6 deployment.

Our Response

Comments from the Acting Principal Deputy DoD CIO fully addressed the recommendation, and no further comments are required.

Recommendation 3

In coordination with the Commander, U.S. Cyber Command, and the Director, Defense Information Systems Agency, develop new DoD Internet Protocol Version 6 transition milestones, roles and responsibilities of each DoD office involved with the migration, and enforcement mechanisms to ensure successful migration to Internet Protocol Version 6; and update the DoD Internet Protocol Version 6 Transition Plan to reflect these changes.

DoD Chief Information Officer Comments

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, agreed, stating the DoD CIO will draft and coordinate a memorandum with transition milestones, roles, responsibilities, and enforcement mechanisms for each DoD office involved in the IPv6 implementation with input from DISA, USCYBERCOM, NSA, Military Department CIOs, HPCMP/DREN, and other DoD test and evaluation components, as appropriate. The DoD CIO will issue the updated plan of action and milestones in the third quarter of FY 2015.

Our Response

Comments from the Acting Principal Deputy DoD CIO fully addressed the recommendation, and no further comments are required.

Recommendation 4

Develop procedures to monitor the status of Internet Protocol Version 6 milestones as identified in Recommendation 3 and elevate milestone deficiencies to the Deputy Secretary of Defense for information and potential corrective action if delays exceed 90 days.

DoD Chief Information Officer Comments

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, partially agreed, stating the DoD CIO will monitor the status of all IPv6 milestones contained in the plan of action and milestones and elevate deficiencies exceeding 90 days on a case-by-case basis.

Our Response

The actions identified by the Acting Principal Deputy DoD CIO in response to Recommendation 3 and the decision to elevate deficiencies exceeding 90 days on a case-by-case basis meets the intent of the recommendation. Therefore, no further comments are required.

Appendix A

Scope and Methodology

We conducted this performance audit from December 2013 through September 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To determine whether DoD was effectively migrating to IPv6, we interviewed officials from the following offices responsible for DoD's overall IPv6 migration: DoD CIO, DISA, and USCYBERCOM. Additionally, we interviewed officials responsible for IPv6 migration at the following organizations:

- U.S. Pacific Command,
- Military Departments (Army, Navy, and Air Force),
- Defense Logistics Agency,
- Washington Headquarters Services,
- High Performance Computing Modernization Program, and
- Space and Naval Warfare Systems Command.

We obtained and analyzed DoD IPv6 planning documents, to include:

- DoD IPv6 Master Test Plan, Version 1.0, September 2005, and Version 2.0, September 2006;
- DoD IPv6 Transition Plan, Version 1, March 2005, and Version 2.0, June 2006;
- DoD IPv6 Integrated Implementation Schedule, Version 1.0, October 4, 2007;
- NIPRNet IPv6 Compliance Demonstration, Version 1.0, June 2008;
- FY 2009 DoD IPv6 Test and Evaluation Report, February 2010 (compiled from field tests, exercises, demonstrations, experiments, simulations, and analyses conducted from 2005 through 2010);
- Director of National Intelligence/DoD IPv6 Information Assurance Guidance for Milestone Objective 3, Version 1.0, June 2010; and
- DoD Implementation Plan for OMB FYs 2012 and 2014 IPv6 Requirements, April 2011.

We developed requests for information to determine the status and progress made to enable IPv6 on DoD's backbone networks and DoD Component networks. We compared IPv6 status-reporting documentation against numerous Federal and DoD IPv6 policies and guidance, including:

- Federal Chief Information Officers Council, "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government, Version 2.0," July 2012;
- OMB Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005;
- OMB Memorandum, "Transition to IPv6," September 28, 2010;
- DoD CIO Memorandum, "Internet Protocol Version 6 (IPv6)," June 9, 2003;
- DoD CIO Memorandum, "DoD Internet Protocol Version 6 (IPv6) Implementation," February 6, 2008; and
- Assistant Secretary of Defense for Networks and Information Integration Memorandum, "Guidance and Policy for Implementation of OMB IPv6 FYs 2012 and 2014 Requirements," March 7, 2011.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Prior Coverage

During the last 5 years, the Army Audit Agency issued a report discussing the Army's migration to IPv6. Unrestricted Army reports can be accessed from .mil and gao.gov domains at https://www.aaa.army.mil/.

Army

Army Audit Agency Report No. A-2011-0149-IET, "Internet Protocol Version 6," July 11, 2011

Appendix B

Improved Battlefield Operations

According to the DoD IPv6 transition manager, DoD Component networks, enabled by IPv6, will increase our military's effectiveness by supporting greater information sharing to enhance decision making and situational awareness. The figure below depicts six benefits that IPv6 implementation can bring to battlefield operations.

Figure B. IPv6 Enabled Battlefield
Source: Air Force Network Integration Center

Appendix C

Unsolicited Management Comments on the Finding and Our Response

Although not required to comment, the Director, C4 Systems and CIO Support (J6), USCYBERCOM provided the following comments on the finding. The Director stated USCYBERCOM concurred with all recommendations in the report.

Item 1. (Overall Draft Report)

Management Comment

The Director said that the DoD CIO, DISA, and USCYBERCOM should be listed in that order in the final report.

Our Response

We agreed with the Director's comment and made the change.

Item 2. (Page 3, Internal Controls)

Excerpt: "Specifically, DoD CIO and USCYBERCOM did not make IPv6 a priority and DoD's key offices for IPv6 migration lacked effective communication and did not properly plan to ensure the required resources were available to implement IPv6."

Management Comment

The Director requested that we revise the sentence to state: "Specifically, because of funding constraints and competing operational requirements, DoD CIO and USCYBERCOM…"

Our Response

The body of the draft report on page 10, in the first and second paragraphs, states, "USCYBERCOM focused on the defense of the IPv4 network due to an increased threat environment" and "funding constraints contributed to USCYBERCOM's lack of priority for IPv6." Therefore, we made no changes to the report.

Item 3. (Page 4, Finding)

Excerpt: "DoD CIO and USCYBERCOM did not make IPv6 a priority"

Management Comment

The Director asked that we revise the first bullet to state: "DoD CIO and USCYBERCOM did not make IPv6 a priority because of competing operational requirements and budget constraints."

Our Response

The body of the draft report on page 10, in the first and second paragraphs, states, "USCYBERCOM focused on the defense of the IPv4 network due to an increased threat environment" and "funding constraints contributed to USCYBERCOM's lack of priority for IPv6." Therefore, we made no changes to the report.

Item 4. (Page 4, Finding)

Excerpt: "As a result, DoD is not realizing the potential benefits of IPv6, including to battlefield operations. Furthermore, the delay in migration could increase DoD's costs and its vulnerability to adversaries."

Management Comment

The Director recommended we revise the excerpt to state: "As a result, DoD is not realizing the potential benefits of IPv6."

Our Response

Our description of the likely effect on battlefield operations and the increased costs and vulnerabilities is fully supported by DoD and Federal Government reports. Therefore, we made no changes to the report.

Item 5. (Page 4, Finding)

Excerpt: "DoD CIO did not have a current plan of action and milestones to advance DoD IPv6 migration efforts."

Management Comment

The Director recommended that we revise the order of the bullets in the finding paragraph.

Our Response

We consider the current order of the bullets to be consistent with the points made in the report finding. Therefore, we made no changes to the report.

Item 6. (Page 6, IPv6 Migration Requirements Not Met)

Excerpt: "However, as of April 28, 2014, representatives from DoD CIO, DISA, and USCYBERCOM stated that a DoD IPv6 pilot must be created before DoD can begin to implement IPv6 on the network."

Management Comment

The Director requested that we revise the sentence to state: "...DoD IPv6 pilot must be created to enable secure implementation before DoD can begin to implement IPv6 on the network."

Our Response

The sentence on page 6 of the draft report states, "...the pilot was necessary to enable secure implementation of IPv6." Therefore, we made no changes to the report.

Item 7. (Page 9, IPv6 Migration was a Low Priority)

Excerpt: "...and the USCYBERCOM division chief of Cyber Operations Planning stated USCYBERCOM was focused on defense of the IPv4 network and that there was no operational imperative for DoD to move to IPv6."

Management Comment

The Director requested that we revise the sentence to state: "...USCYBERCOM was focused on defense of the IPv4 network because of a significantly increased threat environment..."

Our Response

The sentence was a quote made by the division chief in a February 2014 meeting. Therefore, we made no changes to the report.

Item 8. (Page 10, USCYBERCOM Focused on IPv4)

Excerpt: "The division chief also stated IPv6 was not a priority and that USCYBERCOM believed DoD did not have an operational imperative to move to IPv6."

Management Comment

The Director requested that we revise the sentence to state: "The division chief also stated that because of a significant increase in IPv4 threat activity and likely risk associated with transitioning to IPv6 and protecting the IPv6 network, it focused effort on protecting the current IPv4 network."

Our Response

The sentence was a quote made by the division chief in a February 2014 meeting. Therefore, we made no changes to the report.

Item 9-11. (Page 11, IPv6 Migration Efforts Not Effectively Coordinated)

~~(FOUO)~~ Excerpt: [redacted] In addition, DoD CIO and USCYBERCOM did not coordinate their use of testing resources."

Management Comment

The Director requested that we delete the excerpt. Additionally, the Director stated that DISA has responsibility to perform testing as identified on page 3 of the draft report, "DoD Key Offices Responsible for IPv6 Migration."

Our Response

~~(FOUO)~~ [redacted] Additionally, the "Department of Defense Internet Protocol Version 6 Transition Plan, Version 2.0," June 30, 2006, assigned DISA responsibility for ensuring, in conjunction with the NSA, that IPv6 information assurance problems are identified and included in transition efforts. However, as we note in this report, DoD CIO did not update the plan to include the roles and responsibilities of USCYBERCOM, established in 2009. According to the USCYBERCOM mission statement, USCYBERCOM will coordinate and synchronize activities to direct the operations and defense of specified DoD networks. [redacted] Therefore, we made no changes to the report.

Item 12. (Page 12, Ineffective Coordination Impeded IPv6 Migration)

Excerpt: "In fact, the DISA IPv6 lead stated that the two groups have met only once to discuss IPv6 since he took over DISA IPv6 efforts in December 2013."

Management Comment

The Director disputed the factual accuracy of the sentence, stating USCYBERCOM personnel met with DISA personnel once at DISA HQ and twice over the phone in January/February 2014, concerning IPv6 implementation and participated in the IPv6 working group until it ceased in October/November 2013.

Our Response

We added a sentence stating the Director, C4 Systems and CIO Support (J6) stated that DISA and USCYBERCOM met once and talked on the phone twice during this period. However, the DISA IPv6 lead was unaware of the meeting and phone conversations.

Item 13. (Page 15, Further Delay Could Raise IPv6 Migration Costs and Increase Risk from Adversaries)

Excerpt: "The result will be increased transition difficulty, complexity, and cost."

Management Comment

The Director recommended that we delete the excerpt. He stated that transition difficulty and complexity will not change over time but may be reduced as technology capabilities advance. Furthermore, the Director stated that cost would increase consistent with inflation but would not increase relative to the net present value.

Our Response

According to a 2007 white paper prepared by the DoD IPv6 transition manager, the longer IPv6 implementation is delayed, the more embedded IPv4 will become in critical systems, resulting in increased transition difficulty, complexity, and cost. The DoD IPv6 transition manager stated in June 2014 that this information remains accurate. Therefore, we made no changes to the report.

Item 14. (Overall Draft Report)

Management Comment

~~(FOUO)~~ [redacted]

Our Response

The "DoD Key Offices Responsible for IPv6 Migration" section on page 3 of the draft report provides the responsibility of DoD CIO, DISA, and USCYBERCOM as they pertain to IPv6. It also describes the duties of the DoD CIO and DISA as stated in the June 2006 DoD IPv6 Transition Plan. However, as we state in this report, the DoD CIO did not update the plan to include the roles and responsibilities of USCYBERCOM, established in 2009. According to the USCYBERCOM mission statement, USCYBERCOM will plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of DoD networks. Additionally, as we state in this report, USCYBERCOM approval is necessary to enable IPv6 on the NIPRNet. Therefore, we made no changes to the report.

Item 15. (Page i, Results in Brief)

Excerpt: "Although DoD satisfied the requirement to demonstrate IPv6 on the network backbone by June 2008, DoD did not complete the necessary Federal and DoD requirements and deliverables to effectively migrate the DoD enterprise network to IPv6. This occurred because:

- DoD Chief Information Officer (CIO) and U.S. Cyber Command (USCYBERCOM) did not make IPv6 a priority;
- DoD CIO, USCYBERCOM, and Defense Information Systems Agency (DISA) lacked an effectively coordinated effort and did not use available resources to further DoD-wide transition toward IPv6; and
- DoD CIO did not have a current plan of action and milestones to advance DoD IPv6 migration."

Management Comment

The Director stated the bulleted paragraphs are "a bit harsh" and omit the real security concern.

Our Response

~~(FOUO)~~ The bulleted statements are supported by information obtained during the audit. [redacted] Therefore, we made no changes to the report.

Item 16. (Page i, Results in Brief)

Excerpt: "DoD CIO, DISA, and USCYBERCOM lacked an effectively coordinated effort and did not use available resources to further DoD-wide transition toward IPv6."

Management Comment

The Director recommended that we add NSA to the coordination.

Our Response

As discussed in the DoD IPv6 cybersecurity meeting held by the DoD CIO in June 2014, NSA agreed to coordinate on future discussions and actions regarding enabling IPv6 on DoD networks. Further, based on the DoD CIO comments to the draft report, DoD CIO will draft and coordinate a memorandum with transition milestones, roles, responsibilities, and enforcement mechanisms for each DoD office involved in the IPv6 implementation with input from DISA, USCYBERCOM, and NSA. Because NSA has already agreed to coordinate on IPv6 implementation and will be providing input to the DoD CIO memorandum, we did not revise the recommendation to specifically include NSA in the coordination.

Item 17. (Page 1, Background)

Excerpt: "With the success of the Internet has come great demand for IP addresses, thereby exhausting the supply of available IPv4 addresses. On February 3, 2011, the Internet Assigned Numbers Authority issued the remaining IPv4 address blocks, thereby exhausting the supply of IPv4 addresses."

Management Comment

The Director stated that the excerpt is oversimplified.

Our Response

We made no changes to the report.

Items 18 and 19. (Page 1, Background)

Excerpt: "Additionally, DoD Component networks enabled by IPv6 will support greater information sharing, resulting in improved military effectiveness."

Management Comment

The Director recommended rewording the sentence to state that IPv6 can offer improved network operations agility, as opposed to greater information sharing. Additionally, he recommended that we add the following sentence: "More importantly, mobile operators all over the world, including major U.S. operators, are deploying IPv6."

Our Response

The excerpt was taken from a 2007 white paper prepared by the DoD IPv6 transition manager. As of June 2014, the DoD IPv6 transition manager confirmed that this information remains accurate. Therefore, we made no changes to the report.

Item 20. (Page 4, Finding)

Excerpt: "DoD CIO and USCYBERCOM did not make IPv6 a priority;"

Management Comment

The Director requested that we add a 4th fourth bullet stating, "DoD had very serious concerns about DoD technical and personnel readiness to conduct network defense operations in a dual-stack environment."

Our Response

During the audit, we did not receive supporting documentation from USCYBERCOM or NSA regarding technical and personnel readiness for IPv6 operations. Therefore, we made no changes to the report.

Item 21. (Page 5, IPv6 Migration Requirements Not Met)

Excerpt: "However, DoD did not meet the FY 2012 and FY 2014 OMB requirement and is not on schedule to meet the FY 2014 requirement."

Management Comment

The Director recommended revising "is not on schedule" to "DoD will not meet FY 2014 OMB requirements."

Our Response

We revised the report to state DoD did not meet the FY 2014 OMB requirements.

Item 22. (Page 10, USCYBERCOM Focused on IPv4)

Excerpt: "The division chief stated that because USCYBERCOM was not fully aware of the potential risks in transitioning to IPv6 or in protecting the IPv6 network, it prioritized funds to protect the current IPv4 network."

Management Comment

The Director stated his memory of the meeting is that USCYBERCOM was not able to quantify the potential risks posed by enabling IPv6, or how to manage those risks in defensive operations.

Our Response

As we state in this report, the USCYBERCOM division chief of Cyber Operations Planning stated that USCYBERCOM was not fully aware of the potential risks in transitioning to IPv6 or in protecting the IPv6 network, USCYBERCOM prioritized funds to protect the current IPv4 network. Therefore, we made no changes to the report.

Item 23. (Page 12, Ineffective Coordination Impeded IPv6 Migration)

~~(FOUO)~~ Excerpt: "According to the technical director for the NSA Information Assurance Directorate, the main concern was that defensive systems and sensors had not yet evolved to include IPv6 functionality."

Management Comment

The Director recommended that we add "at that time (gate FY11)," after "main concern."

Our Response

The sentence has been reworded to state: "According to the technical director for the NSA Information Assurance Directorate, the main concern at that time (FY 2011) was that defensive systems and sensors had not yet evolved to include IPv6 functionality."

Item 24. (Page 14, Plans for Migrating to IPv6 Not Updated)

Excerpt: "However, DoD did not accomplish the FY 2012 requirements and is not on track to meet FY 2014 requirements to operationally enable native IPv6."

Management Comment

The Director recommended revising "is not on track" to "will not meet."

Our Response

We revised the report to state DoD did not meet the FY 2014 OMB requirements.

Item 25. (Page 14, Delayed Benefits of IPv6 in Battlefield Operations)

Excerpt: "Continued use of IPv4 will delay the potential benefits of IPv6, such as improved communication, warfighter mobility, situational awareness, and quality of service."

Management Comment

The Director stated the report excerpt is factual but omits the defensive operations burden imposed by network address translation, which IPv6 could reduce or eliminate.

Our Response

During the audit, we were not provided supporting documentation for the defensive operations burden imposed by network address translation, which IPv6 could reduce or eliminate. Therefore, we made no changes to the report.

Item 26. (Page 16, Recommendation 3)

Excerpt: "In coordination with the Commander, U.S. Cyber Command, and the Director, Defense Information Systems Agency, develop new DoD Internet Protocol Version 6 transition milestones, roles, and responsibilities for each DoD office involved with the migration, as well as enforcement mechanisms to ensure successful migration to Internet Protocol Version 6; and update the DoD Internet Protocol Version 6 Transition Plan to reflect these changes."

Management Comment

The Director recommended that we add NSA to the recommendation.

Our Response

As discussed in the DoD IPv6 cybersecurity meeting held by the DoD CIO in June 2014, NSA agreed to coordinate on future discussions and actions regarding enabling IPv6 on DoD networks. Further, based on the DoD CIO comments to the draft report, DoD CIO will draft and coordinate a memorandum with transition milestones, roles, responsibilities, and enforcement mechanisms for each DoD office involved in the IPv6 implementation with input from DISA, USCYBERCOM, and NSA. Because NSA has already agreed to coordinate on IPv6 implementation and will be providing input to the DoD CIO memorandum, we did not revise the recommendation to specifically include NSA in the coordination.

Item 27. (Overall Draft Report)

Management Comment

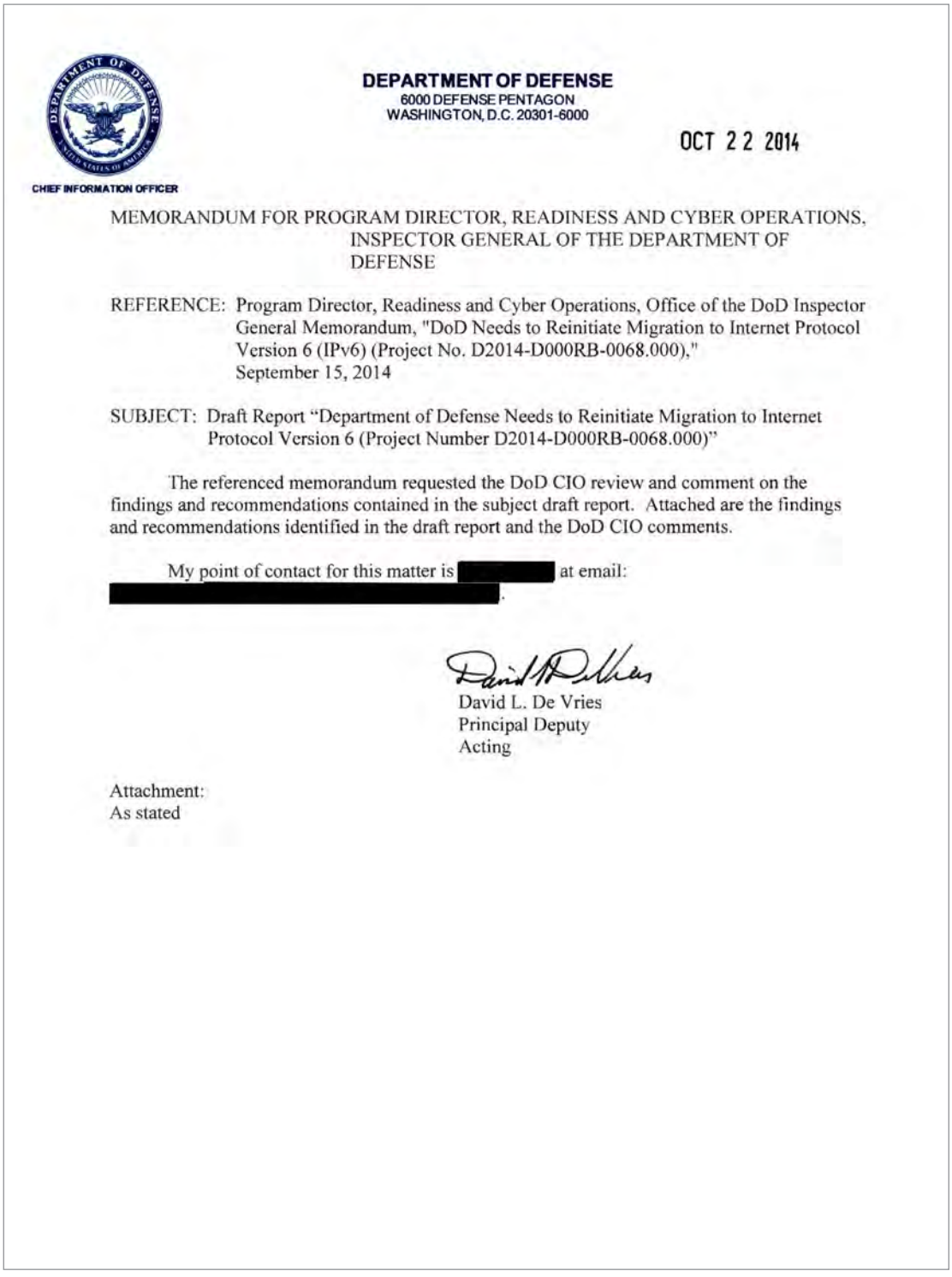
~~(FOUO)~~ [redacted]

Our Response

During the audit, we did not receive supporting documentation from USCYBERCOM or NSA regarding technical and personnel readiness for IPv6 operations. Therefore, we made no changes to the report.

Management Comments

DoD Chief Information Officer Comments



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

OCT 22 2014

MEMORANDUM FOR PROGRAM DIRECTOR, READINESS AND CYBER OPERATIONS, INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

REFERENCE: Program Director, Readiness and Cyber Operations, Office of the DoD Inspector General Memorandum, "DoD Needs to Reinitiate Migration to Internet Protocol Version 6 (IPv6) (Project No. D2014-D000RB-0068.000)," September 15, 2014

SUBJECT: Draft Report "Department of Defense Needs to Reinitiate Migration to Internet Protocol Version 6 (Project Number D2014-D000RB-0068.000)"

The referenced memorandum requested the DoD CIO review and comment on the findings and recommendations contained in the subject draft report. Attached are the findings and recommendations identified in the draft report and the DoD CIO comments.

My point of contact for this matter is [redacted] at email: [redacted].

David L. De Vries
Principal Deputy
Acting

Attachment:
As stated

DoD Chief Information Officer Comments (cont'd)

DOD IG DRAFT REPORT DATED SEPTEMBER 15, 2014
(PROJECT NO. D2014-D000RB-0068.000)

"DOD NEEDS TO REINITIATE MIGRATION TO INTERNET PROTOCOL VERSION 6"

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER COMMENTS TO THE DOD IG FINDINGS AND RECOMMENDATIONS

GENERAL: DoD Is Not Effectively Migrating to IPv6. *Although DoD satisfied the OMB M-05-22 requirement to demonstrate IPv6 on the network backbone by June 2008, DoD did not complete the Federal and DoD requirements and deliverables to effectively migrate the DoD enterprise network to IPv6. This occurred because:*

SUB FINDING 1: *DoD CIO and U.S. Cyber Command (USCC) did not make IPv6 a priority.*

DoD CIO RESPONSE:
Disagree. IPv6 is a DoD priority, but conducting an expensive transition from IPv4 to an IPv6 environment is not cost effective nor warranted. Based on technology changes and lessons learned in recent years, DoD has implemented IPv6 enclaves which support necessary IPv6-based operations while maintaining the extensive IPv4 environment of today. Additionally, DoD has sufficient IPv4 address space to support future operations. There is no DoD Component operational imperative or business case to implement IPv6. Further, the security of DoD networks is the highest priority of the Department. The Department is taking concrete steps (described below) to address the USCC cybersecurity concerns and continue IPv6 implementation as warranted.

SUB FINDING 2: *DoD CIO, USCC, and the Defense Information Systems Agency (DISA) 1) lacked an effectively coordinated effort and 2) did not use available resources to further DoD-wide transition toward IPv6 operations.*

DoD CIO RESPONSE:
Disagree DoD CIO, USCC, and DISA lacked an effectively coordinated effort. The Department effectively coordinated with all Components to ensure DoD networks are capable of utilizing IPv6 (e.g., the Sensitive but Unclassified IP Router Network is IPv6 capable via dual stack and IP devices are certified for IPv6 capability prior to connection to DoD networks). Based on technology changes in recent years and a rise in the sophistication of the cyber threat, additional research and development is required to resolve the cybersecurity concerns raised by USCC in November 2012. To effectively coordinate a resolution to the cybersecurity concerns, DoD CIO is collaborating with USCC and DISA to develop an updated plan of action and milestones (POA&M) which includes development of a limited IPv6 deployment plan in first quarter of fiscal year 2015.

Disagree DoD CIO, USCC, and DISA did not use all available resources to further DoD-wide transition toward IPv6 operations. To test and evaluate many aspects of IPv6 implementation,

DoD Chief Information Officer Comments (cont'd)

the Department leveraged the Air Force Research Lab, the Air Force Information Warfare Center, the National Security Agency (NSA), the Joint Interoperability Test Command test facilities, the Army Technology Information Center, the Navy Space and Warfare Systems Command laboratories, and the Defense Research and Engineering Network. As the DoD evolves the IPv6 implementation, DoD CIO, USCC, and DISA will continue to leverage available test and evaluation resources from USCC, NSA, Military Department CIOs, High Performance Computing Modernization Program/Defense Research and Engineering Network, and other DoD test and evaluation facilities.

SUB FINDING 3: *DoD CIO did not have a current plan of action and milestones to advance DoD IPv6 migration efforts.*

DoD CIO RESPONSE: Partially agree. DoD developed a transition plan in 2006 and a follow-on POA&M in 2011 advancing IPv6 implementation efforts based on knowledge at that time. Although 2011 POA&M actions are still relevant, timelines and scope have changed due to changing technology and changing cyber threat. DoD CIO is revisiting development of a limited IPv6 deployment plan with USCC and DISA by second quarter of fiscal year 2015 and development of an updated POA&M based on that plan.

RECOMMENDATION 1: *Establish a DoD-wide Internet Protocol version 6 transition office and working groups to advance DoD's transition to Internet Protocol version 6. At a minimum, working groups should include representation from DISA, USCC, Defense Research and Engineering Network, and Service Chief Information Officers.*

DoD CIO RESPONSE: Disagree. There is no need for a DoD IPv6 transition office with dedicated resources from DISA, USCC, Defense Research and Engineering Network, and Service Chief Information Officers. The DoD has adopted a more agile and resource-efficient approach by establishing a steering group to coordinate Department IPv6 implementation actions, address USCC cybersecurity issues, and define the way forward to obtain USCC authorization of IPv6 on DoD networks. The group is led by the DoD CIO and consists of representatives from DISA, USCC, Defense Research and Engineering Network, and Military Department Chief Information Officers. Additionally, DISA has established an Integrated Project Team (IPT) consisting of representatives from DoD CIO, USCC, and NSA to address the technical aspects required to implement IPv6 actions.

RECOMMENDATION 2: *In coordination with the Commander, U.S. Cyber Command; the Director, Defense Information Systems Agency; the Commander, U.S. Army Information Systems and Engineering Command/Army Technology Integration Center; the Director, High Performance Computing Modernization Program/Defense Research and Engineering Network; and other DoD test and evaluation components, establish a process to integrate component testing results and lessons learned into DoD Internet Protocol version 6 migration efforts.*

DoD CIO RESPONSE: Agree. The DoD CIO will continue to work with the various research and development centers and test centers to assess IPv6 threats and to develop

DoD Chief Information Officer Comments (cont'd)

appropriate counter measures to these threats. Additionally, the DISA IPv6 IPT will integrate component testing results and lessons learned to guide IPv6 implementation efforts and inform the pace, scope, and timing of the IPv6 deployment. IPv6 test and evaluation results and analysis of the initial limited deployment should be available in third quarter of fiscal year 2015.

RECOMMENDATION 3: *In coordination with the Commander, U.S. Cyber Command, and the Director, Defense Information Systems Agency, develop new DoD Internet Protocol version 6 transition milestones, roles and responsibilities of each DoD office involved with the migration, and enforcement mechanisms to ensure successful migration to Internet Protocol version 6; and update the DoD Internet Protocol version 6 Transition Plan to reflect these changes.*

DoD CIO RESPONSE: Agree. The DoD CIO will draft and coordinate a memorandum with transition milestones, roles, responsibilities, and enforcement mechanisms for each DoD office involved with the IPv6 implementation. The DoD CIO will involve USCC, DISA, NSA, Military Department CIOs, High Performance Computing Modernization Program/Defense Research and Engineering Network, and other DoD test and evaluation components, as appropriate, in drafting this memorandum. The updated POA&M will be issued in third quarter of fiscal year 2015.

RECOMMENDATION 4: *Develop procedures to monitor the status of Internet Protocol version 6 milestones as identified in Recommendation 3 and elevate milestone deficiencies to the Deputy Secretary of Defense for information and potential corrective action if delays exceed 90 days.*

DoD CIO RESPONSE: Partially agree. The DoD CIO will monitor status of all IPv6 milestones contained in the POA&M, as appropriate. DoD CIO will elevate deficiencies exceeding 90 days on a case-by-case basis.

ADDITIONAL DoD CIO COMMENTS:

The DoD CIO comments on the internal control weaknesses discussed in the report are included in the DoD CIO's comments to the findings.

Enclosed is the Navy, Deputy CIO information provided to the Office of Inspector General in response to a request for information. It appears this information was not taken into account in the final draft report. Specifically, the Navy does maintain an inventory of IP compliant devices in the Department of Navy Application and Database Management System, which is not reflected in this report. Also, the Navy provided a recommendation during review of the unofficial draft report to aggregate interview responses from individuals to the Military Service level. This recommendation was not accepted by the Office of the Inspector General of the Department of Defense in developing the draft official report. Please consider the Navy, Deputy CIO input when developing the final official report.

DoD Chief Information Officer Comments (cont'd)

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

2000
Ser N2N6BC/4U120157
9 May 14

From: Department of Navy, Deputy Chief Information Officer (Navy) (DDCIO(N))
To: Team Lead, Inspector General Department of Defense

Subj: REQUEST FOR INFORMATION PROJECT NO. D2014-D000RB-0068.000

Ref: (a) DOD IG RFI #02 of 5 May 14
(b) DON CIO 021936Z JAN 09

1. The Department of Navy Deputy Chief Information Officer (Navy) (DDCIO(N)) has reviewed reference (a) and provides the following response:

a. *Did the Navy complete an inventory of existing IP compliant devices and technologies, to include existing routers, switches, and hardware firewalls, in accordance with Office of Management and Budget (OMB) M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005? If yes, please provide a copy of this inventory. If no, please provide an explanation as to why.* It is Navy policy, per reference (b), to maintain an inventory of IP compliant devices and technologies within the Department of Navy Application and Database Management System (DADMS). DADMS is authoritative, dynamically updated, and does not include the ability to cull historic time bound device inventories. There are currently 72000 devices and servers registered in DADMS. Conducting a DADMS pull of these devices and technologies operating across 5000 Navy locations is time and cost prohibitive.

b. *Did the Navy include IPv6 transition resource requirements in their POM submissions for FY 2010 - FY 2014 per the DoD CIO memorandum, "DoD Internet Protocol Version 6 (IPv6) Implementation," February 6, 2008? If yes, please provide the POMs and identify the IPv6 resources needed. If no, please provide an explanation as to why.* The Chief of Naval Operations did not include FY10 POM submissions for IPv6 transition. During the FY10 POM development process, the CNO selected higher priority resourcing and capabilities to meet the Navy's Title 5 United States Code responsibilities.

DoD Chief Information Officer Comments (cont'd)

Subj: REQUEST FOR INFORMATION PROJECT NO. D2014-D000RB-0068.000

2. My point of contact is [redacted], Governance and Enterprise Architecture Branch Head, at commercial: [redacted] or e-mail: [redacted].

JANICE C. HAITH, SES
By direction

2

U.S. Cyber Command Comments

DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6477
FORT GEORGE G. MEADE, MARYLAND 20755

23 Oct 14

Reply to:
USCYBERCOM/J6
9800 Savage Road, Ste 6477
Fort Meade, MD 20755

MEMORANDUM FOR DOD IG READINESS AND CYBER OPERATIONS
ATTN: [redacted]

Subject: Draft Report, "DoD Needs to Reinitiate Migration to Internet Protocol Version 6," dtd 15 Sep 14, Project No. D2014-D000RB-0068.000

Reference: [redacted] email, same subj, dtd 15 Sep 14

1. Key personnel within USCYBERCOM and NSA have reviewed the draft report, with comments attached. Overall USCYBERCOM concurs with the recommendations contained within report; however, there are several areas of concern that we have offered comment and ask to be considered.

2. If you have any questions, please contact the undersigned at [redacted]

[redacted]

Attachments:
Enclosure A – IPv6 CRM

Copy:
[redacted]

U.S. Cyber Command Comments (cont'd)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) IG Draft Report,"DoD Needs to Reinvigorate Migration to IPV 6"
(U) Comment Matrix
10/10/2014

*For comment matrix instructions, see "Instructions" tab at bottom left.
Please remember to portion mark classified comments.

Page #	Para or Line #	POC Info: (Organization, Name, Title, Phone)	Comment Type Critical (C) Substantive (S) Administrative (A)	Comments (Use classification portion markings)	Rationale (Use classification portion markings)	Adjudication (Accepted or Rejected) (Use classification portion markings) (For Policy Officer Use Only)
All		[redacted]J65 C4IT/CIO Support, USCYBERCOM	A	(U) When listing the three organization, list "DoD CIO, DISA, and USCYBERCOM" in that order	Continuity throughout document	
3	2nd para, line 5	[redacted] J6 Director, USCYBERCOM	S	(U) Change to read "... migration to IPv6. Specifically, because of funding contraints and competing operational requirements, DoD CIO and USCYBERCOM		
4	1st para	[redacted] J6 Director, USCYBERCOM	S	(U) 1st bullet, change to: " DoD CIO and USCYBERCOM did not make IPv6 a priority because of competing operational requirements and budget constraints." Move to bottom of bullet list		
4	1st para	[redacted] J6 Director, USCYBERCOM	S	(U) Delete "...including to battlefield operations. Furthermore, the delay in migration could increase DoD's costs and its vulnerability to adversaries." After 3rd bullet		
4	1st para	[redacted]J65 C4IT/CIO Support, USCYBERCOM	A	(U) Move 3rd bullet to the 1st bullet position		
6	1st para, line 8	[redacted] J6 Director, USCYBERCOM	S	(U) Change to read, "... DoD IPv6 pilot must be created to enable secure implementation before DoD can begin to ..."		
9	1st para, line 4	[redacted] J6 Director, USCYBERCOM	S	(U) Change to read "... USCYBERCOM was focused on defense of the IPv4 network because of a significantly increased threat environment and that there..."		
10	1st para, line 6	[redacted] J6 Director, USCYBERCOM	S	(U) Change to read " The division chief also stated that because of a significant increase in IPv4 threat activity and likely risk associated to transitioning to IPv6 and protecting the IPv6 network, it focused effort on protecting the current IPv4 network." starting at the end of the line		
11	2nd para	[redacted] J6 Director, USCYBERCOM	S	(U) Delete "Since 2012, USCYBERCOM has continued to deny request from DISA and DoD CIO for a communications tasking order."		
11	2nd para, lines 3	[redacted] J6 Director, USCYBERCOM	S	(U) Delete ", which would include instructions form USCYBERCOM on what DISA needs to do to implement IPv6. In addition, DoD CIO and USCYBERCOM did not coordinate their use of test resources."		
11	2nd para	[redacted] J6 Director, USCYBERCOM	S	(U) Delete "In addition, DoD CIO and USCYBERCOM did not coordinate their use of testing resources"	(U) DISA has the responsibility to perform testing (ref. p.3, 1st para).	
12	1st para	[redacted] J6 Director, USCYBERCOM	S	(U) "In fact, the DISA IPv6 lead stated that the two groups have met only once to discuss IPv6 since he took over DISA IPv6 efforts in December 2013."	(U) This is incorrect. [redacted] have met with DISA personnel once at DISA HQ and twice over the phon in January/February 2014 concerning IPv6 implementation. USCYBERCOM has participated in the IPv6 working group until it ceased in October/November 2013.	
15	2nd para, line 5	[redacted]J65 C4IT/CIO Support, USCYBERCOM	S	(U) Delete sentence, "The result will be increased..."	Transition difficulty and complexity will not change over time, but may be reduced as technology capabilites advance. Cost would be a factor of inflation, but not increase relative to the net present value.	
OVERALL		[redacted]J65 C4IT/CIO Support, USCYBERCOM	S	[redacted]		Classified By: [redacted] Derived From: NSA/CSSM 1-52 Dated: 20070108 Declassify On: 20390401

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Final Report Reference

Revised

Revised, Page 11

U.S. Cyber Command Comments (cont'd)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U) IG Draft Report,"DoD Needs to Reinvigorate Migration to IPV 6"
(U) Comment Matrix
9/26/2014

*For comment matrix instructions, see "Instructions" tab at bottom left.
Please remember to portion mark classified comments.*

Page #	Para or Line #	POC Info: (Organization, Name, Title, Phone)	Comment Type Critical (C) Substantive (S) Administrative (A)	Comments (Use classification portion markings)	Rationale (Use classification portion markings)	Adjudication (Accepted or Rejected) (Use classification portion markings) (For Policy Officer Use Only)
i	Finding, bulleted paragraphs	[redacted] IA Technical Director, NSA	S	Bulleting paragraphs are a bit harsh and omit real security concern		
i	Recommendation, 3rd bulleted paragraphs	[redacted] IA Technical Director, NSA	S	(U) Add NSA to the coordination.	(U) Due to NSD-24 authorities, NSA should be included in the coordination on IPv6 milestones, roles, and responsibilities	
1	2nd paragraph	[redacted] IA Technical Director, NSA	S	(U) Last 2 sentences are over simplified.		
1	3rd para	[redacted] IA Technical Director, NSA	S	Last sentence, "will support greater information sharing ..." should be reworded.	(U) Not sure this is justified; what evidence? Better to say that IPV6 can offer improved network operations agility.	
1	3rd para	[redacted] IA Technical Director, NSA	A	(U) Add a sentence, "More importantly, mobile operators all over the world, including major U.S. operators, are deploying IPv6."		
4	bulleted paras	[redacted] IA Technical Director, NSA	S	(U) Add a 4th bullet, "-- It is also true that DoD (DISA, NSA, USCC, CIO) had very serious concerns about DoD technical and personnel readiness to conduct network defense operations in a dual-stack environment."		
5	Para 3, last sentence	[redacted] IA Technical Director, NSA	S	(U) Reword "is not on schedule" to "DoD will not meet FY 2014 OMB requirements."		
10	second para, second sentence	[redacted] IA Technical Director, NSA	S	(U) My memory of this meeting is that the J6 said that USCC was not able to quantify the potential risks posed by enabling IPv6, or how to manage those risks in defensive operations.		
12	first sentence	[redacted] IA Technical Director, NSA	S	(U) Add, "at that time (gate,FY11)," after "concern."		
14	second para, second sentence	[redacted] IA Technical Director, NSA	S	(U) Change "is not on track" to "will not meet".		
14-15	Delayed Benefits para	[redacted] IA Technical Director, NSA	S	(U) This long paragraph is true, but omit the defensive operations burden imposed by NAT which IPv6 could reduce or eliminate.		
16	Recommendation 3., first sentence	[redacted] IA Technical Director, NSA	S	(U) Insert "and NSA" after Defense Information Systems Agency.	(U) Due to NSD-24 authorities, NSA should be included in the coordination on IPv6 milestones, roles, and responsibilities.	
OVERALL		[redacted] DIAD Special Projects Office - VS	S	[redacted]		

Classified By [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20390401

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Final Report Reference

Revised

Revised, Page 10
Revised, Page 12

Glossary

Battlefield Operation: The process of carrying on combat, including movement, supply, attack, defense, and maneuvers needed to gain the objectives of any battle or campaign.

Dual Stack: Method of IPv4 to IPv6 transition in which each host is both IPv4 and IPv6 aware. Dual stack hosts run both IPv4 and IPv6 protocols and allocate addresses for both protocols.

Internet Protocol (IP): The standardized "envelope" that carries addressing, routing, and message-handling information, thereby enabling a message to be transmitted from its source to its final destination over the various interconnected networks that comprise the Internet.

IPv4: The protocol currently in use on the Internet. IPv4 was the first stable version of the IP based on a 32 bit address format, which equates to approximately 4.3 billion IP addresses.

IPv6: The next-generation network layer protocol of the Internet designed to handle the growth of the Internet and to cope with the demanding requirements of services, mobility, and end-to-end security. The key characteristics of IPv6 are designed to greatly expand available IP address space.

Joint Information Environment (JIE): A secure joint information environment comprised of shared IT infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies.

Native IPv6: The transition to IPv6 without the use of translators, tunnels (IPv4 carrying IPv6). End users can communicate entirely via IPv6.

Network Backbone: For the purposes of IPv6 migration, a network backbone is the set of network transport devices (routers, switches) that provide the highest level of traffic aggregation in the network.

Acronyms and Abbreviations

CIO	Chief Information Officer
DISA	Defense Information Systems Agency
DITO	DoD IPv6 Transition Office
DREN	Defense Research and Engineering Network
HPCMP	High Performance Computing Modernization Program
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
JITC	Joint Interoperability Test Command
NIPRNet	Non-classified Internet Protocol Router Network
NSA	National Security Agency
OMB	Office of Management and Budget
TIC	Technology Integration Center
USCYBERCOM	U.S. Cyber Command
USPACOM	U.S. Pacific Command

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report@listserve.com

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098