DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

DHS Must Address Internet Protocol Version 6 Challenges

OIG-08-61

May 2008

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 28, 2008

MEMORANDUM FOR: Elaine Duke
Deputy Under Secretary for Management

Richard L. Skinner

FROM: Richard L. Skinner
Inspector General

SUBJECT: *DHS Must Address Internet Protocol Version 6 Challenges,*
OIG-08-61

We evaluated the Department of Homeland Security's (DHS') transition to Internet Protocol Version 6 (IPv6). The Office of Management and Budget (OMB) requires federal agencies to demonstrate by June 2008, the capability to pass IPv6 traffic and support IPv6 addresses from the (1) Internet to their local area network; (2) their local area network to the Internet; and (3) their local area network to other local area networks. Our objective was to determine whether DHS is effectively managing its implementation of IPv6.

Although DHS has begun the early stages of implementing OMB's IPv6 transition requirements, it is unlikely that the department will be positioned to take timely advantage of the enhanced capabilities of IPv6 as IPv6-capable products and services become available. Specifically, we recommend that DHS (1) complete an inventory of IPv6 applications and devices; (2) finalize its IPv6 transition strategy; (3) provide guidance to its components and offices to plan for their IPv6 transition; and (4) better coordinate with the OneNet Steward.

The five recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. In response to our draft report, DHS concurred with our recommendations. DHS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix A.

Please advise our office within 90 days of the date of this memorandum of the progress in implementing the recommendations. Your response, or action plan, should discuss the relevant actions taken or planned, parties responsible, key milestones, and other supporting information that demonstrates your progress.

Consistent with our responsibility under the Inspector General Act, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the DHS. In addition, we will post a copy of the report on our website for public dissemination.

Should you have any questions, please call me, or your staff may contact Frank Deffer, Assistant Inspector General for IT Audits, at (202) 254-4100.

Background

Internet Protocol (IP) includes the language and rules that computers use to transmit information (such as email and other data, voice communications, and video) over the Intranet and Internet. Devices that directly connect to the Internet need a unique IP address to identify where information originates and its destination. The existing protocol supporting the Internet today–Internet Protocol Version 4 (IPv4)–supports 4.3 billion IP addresses, limiting the number of devices that can be given a unique IP address to connect to the Internet. This cap has constrained the growth of the Internet worldwide and has limited the number of computers and other devices that can be connected to one another over the Internet. In addition, there are many security considerations when introducing emerging technology into a network. The United States Computer Emergency Response Team (US-CERT) warned in April 2005 that the unmanaged implementation of IPv6 increases security risks to agencies' networks.

On August 2, 2005, OMB issued Memorandum 05-22 (M-05-22), *Transition Planning for Internet Protocol Version 6 (IPv6)*, establishing the goal of transitioning federal agencies' network backbones to IPv6. The "backbone" includes an agencies' wide area network (WAN) core up to its local area network point of demarcation. OMB requires that an agency's network backbone transmit both IPv4 and IPv6 traffic and that agencies perform testing to verify its capability to pass both protocols simultaneously. To aid in transition planning, OMB M-05-22 identified several key interim milestones and the following requirements:

- By November 15, 2005:
    - Identify an IPv6 agency lead;
    - Complete inventory of routers, switches, and hardware firewalls in network backbone.

- By February 28, 2006:
    - Develop a network backbone transition plan for IPv6;
    - Submit to OMB an IPv6 progress report.

- By June 30, 2006:
    - Complete an inventory of applications and peripherals with dependencies on the network backbone;
    - Complete an IPv6 transition impact analysis.

In July 2005, DHS assigned Customs and Border Protection (CBP) as the network steward to maintain and operate DHS' unclassified WAN (DHS' network backbone), referred to as

DHS OneNet. DHS has committed to consolidating its network infrastructure to OneNet to improve network services between its components. DHS' goal is to ensure that OneNet will be IPv6 capable by June 30, 2008.

Additional Preparation Needed For IPv6 Transition

In February 2004, DHS began its efforts to transition to IPv6. The Chief Information Officer (CIO) established the requirement that all new information technology acquisitions be IPv6 compliant. In July 2005, the CIO established an IPv6 program office to lead the department-wide transition effort. In May 2006, DHS conducted an inventory of Cisco routers and switches that are IPv6 capable. However, this inventory did not include any hardware firewalls or non-Cisco network devices. In August 2006, CBP, as the steward for DHS' network backbone, reserved a block of IPv6 addresses to satisfy DHS' anticipated growth over the next 10 years based on a projection by DHS OneNet's administrator. Finally, in May 2007, DHS developed cost estimates to implement IPv6 on DHS OneNet.

Despite these efforts, DHS faces additional challenges in transitioning to IPv6. DHS should be further along in implementing its transition effort and completing the OMB interim milestones. DHS must ensure that several key activities are completed before it can fully transition to IPv6 functionality. Specifically, the department needs to (1) complete a comprehensive inventory of all IPv6 applications and devices, including hardware firewalls; (2) finalize its IPv6 transition strategy; (3) engage its components on IPv6 transition planning and activities; and (4) better coordinate with CBP officials on DHS' IPv6 transition effort.

A Complete Inventory of IPv6 Applications and Devices Is Essential

DHS has not completed an inventory of routers, switches, and firewalls for its OneNet. Further, DHS has not conducted an inventory of existing applications and other IPv6 devices. Combined, such an inventory would provide DHS with the ability to determine the controls and resources needed to mitigate the risks identified with the transition and assist the department in developing a more accurate transition cost estimate.

In May 2006, DHS conducted a scan to identify its IPv6-capable network devices. DHS used an automated network discovery tool (Cisco Network Collector) at six major components to identify Cisco devices that support IPv6. The components included in this assessment were CBP, the Federal Emergency Management Agency, Federal Law Enforcement Training Center, Immigration and Customs Enforcement, Transportation Security Administration, and United States Coast Guard. This inventory did not include any hardware firewalls or non-Cisco network devices. In addition, the inventory did not include all DHS components and offices. The results of this discovery were submitted to OMB in February 2007 as DHS' initial IPv6 inventory.

OMB required agencies to complete their initial inventory (IPv6 routers, switches, and firewalls) by November 15, 2005, and a second inventory (IPv6 applications and peripheral devices) by June 30, 2006. Without a comprehensive inventory, DHS does not have the most complete and accurate information available to assess the risks associated with its IPv6 transition.

IPv6 Transition Strategy Must Be Finalized

In January 2007, DHS drafted its initial transition plan that assigned IPv6 roles and responsibilities, established interim milestones to meet OMB's June 2008 deadline, and established working groups to coordinate technical and implementation issues. However, the plan has not been updated or finalized. For example, the plan does not include a timeline for when the department will complete its transition to IPv6 on its network backbone; indicate when the department will deploy IPv6 functionality to its components; identify the transition method and testing strategy to ensure interoperability between IPv6 and IPv4; or incorporate IPv6 training requirements for key personnel. According to program officials, DHS is now in the process of finalizing its transition plan.

A transition strategy is the first step to ensure that migration to IPv6 is done methodically and that network security is not compromised. Before DHS can begin to deploy IPv6, the department must finalize its IPv6 transition strategy. Completing key planning activities and identifying the methods of transition early can mitigate risks and assist DHS in a successful transition to IPv6. Further, lacking a transition strategy, DHS may incur additional expenses with costly upgrades and compromise network security.

Guidance Is Needed for Components' Transition to IPv6

DHS has not provided any guidance to its components and offices to assist them in planning for their transition. Further, DHS has not developed any IPv6-related security policies or established standard configurations for IPv6 devices. Also, DHS has not established a process to oversee the component's progress in migrating to IPv6. For example, DHS' draft transition plan required components to submit (1) an inventory of their network devices and applications to the program office by October 2007, and (2) their respective transition plans by December 2007. However, the department has not enforced the requirements outlined in its transition plan. While several components have begun planning their own IPv6 activities, actions taken thus far are limited. For example, only CBP and the United States Secret Service conducted an inventory of their IPv6-capable devices. CBP obtained contract support to develop its own transition planning documents. However, none of the components have developed an impact analysis to evaluate the potential risks on their network infrastructures during transition.

According to DHS program officials, the department is only in the early stage of IPv6 transition and oversight responsibilities have not been established. Further, program officials indicated that there is little incentive for the department to move forward with only a few applications taking advantage of IPv6 features. Unless DHS involves its components in the department's transition effort, DHS' migration to IPv6 may not be successful. Components that migrate to IPv6 without specific guidelines may not align with DHS' IPv6 goals.

Better Coordination With the OneNet Steward Is Needed

DHS has not coordinated effectively with its OneNet steward (CBP) to ensure that the department's IPv6 transition is planned methodically. The lack of coordination has caused confusion and duplicated planning efforts between DHS and CBP on several key decisions that affect the department's transition to IPv6. DHS program officials indicated that they selected "dual-stack" as the department's transition method to IPv6. According to CBP personnel, the transition method could not be determined until testing was conducted. Testing is needed to evaluate whether the method selected would compromise security and be compatible with DHS OneNet. Finally, CBP personnel indicated that IPv6 program officials had yet to share the most current version of the transition plan and impact analysis with them.

Improved coordination between DHS' IPv6 program office and CBP officials will allow DHS to better manage its resources and avoid duplicating planning efforts. Effective coordination with DHS' OneNet steward on key transition planning decisions will help ensure that network security is not compromised during the transition.

Unless DHS officials quickly address the challenges affecting its IPv6 transition, the department risks not meeting OMB's June 30, 2008 milestone. Despite assurances from DHS officials that the department will meet OMB's deadline to transmit both IPv4 and IPv6 traffic by June 2008, we believe that the actions DHS has taken to date do not guarantee that the department and its components can successfully demonstrate the capabilities required by OMB. As recently as December 2007, the OMB Deputy General Counsel said that agencies are expected to meet the June 2008 deadline and that no extension is anticipated. The intent of OMB M-05-22 is to ensure that the federal government is in a position to take advantage of the enhanced capabilities of IPv6 as IPv6-capable products and services become available.

Recommendations

To strengthen DHS' IPv6 planning effort, we recommend the CIO:

1. Complete a comprehensive IPv6 inventory of all existing routers, switches, hardware firewalls, applications, and other technologies department wide.

2. Finalize the transition plan with detailed interim milestones and a timeline for the department to complete its transition to IPv6.

3. Determine which transition mechanism will be employed by DHS and verify this new capability through testing activities.

4. Develops and issue necessary guidance for components to plan and align their transition effort to IPv6 with the department's goals and implement a process to monitor components' transition activities.

5. Ensure that the DHS IPv6 program office and CBP coordinate their planning and transition efforts.

Management Comments And OIG Analysis

DHS concurs with recommendation 1. DHS agrees that a complete inventory of IP devices and applications needs to be generated and an assessment needs to be made regarding the readiness state of IPv6 capabilities. A strategy to complete a comprehensive IPv6 inventory (edge router to desktop) is under development for June 2008. Also, DHS will determine what devices and applications can be upgraded for IPv6 capabilities, and identify what needs to be replaced.

We accept DHS' response to complete a comprehensive inventory and to determine its state of IPv6 readiness.

DHS concurs with recommendation 2. DHS will finalize a transition plan by September 2008. The updated transition plan will be based on a CBP transition plan that will be coordinated among technical and application transition work groups, and will include major milestones. An integrated IPv6 transition schedule will still be needed and will be developed in coordination with component IPv6 transition plans to provide insights into the dependencies and the availability of required technical solutions. The integrated transition schedule is to be completed no later than March 2009.

We accept DHS' response to finalize its transition plan. We maintain that DHS needs to outline its interim milestones and a timeline for the department to complete its transition to IPv6.

DHS concurs with recommendation 3. In March 2008, the IPv6 program office created a high-level DHS IPv6 Master Test Plan that identifies the operational criteria that need to be verified through a test and evaluation program. The criteria are intended to ensure that the selected transition mechanism will not impact operations. The criteria will be applied to IPv4 and IPv6 network transition techniques, such as dual stack and configured tunnels. Proposals to use transition mechanisms during the transition period will be evaluated on a case-by-case basis.

We accept DHS' response to identify, test, and evaluate IPv4 and IPv6 transition techniques to determine which mechanism will be employed by DHS.

DHS concurs with recommendation 4. DHS will finalize and distribute IPv6 implementation guidance to enable the network steward and components to follow a common and coordinated approach. The set of guidance documentation is targeted for completion in October 2008. These deliverables will support component planning efforts and the development of the integrated transition schedule that is to be competed by March 2009.

We accept DHS' response to distribute IPv6 guidance to the components to plan and align their transition efforts with the department's goals and implement a process to monitor components' transition activities.

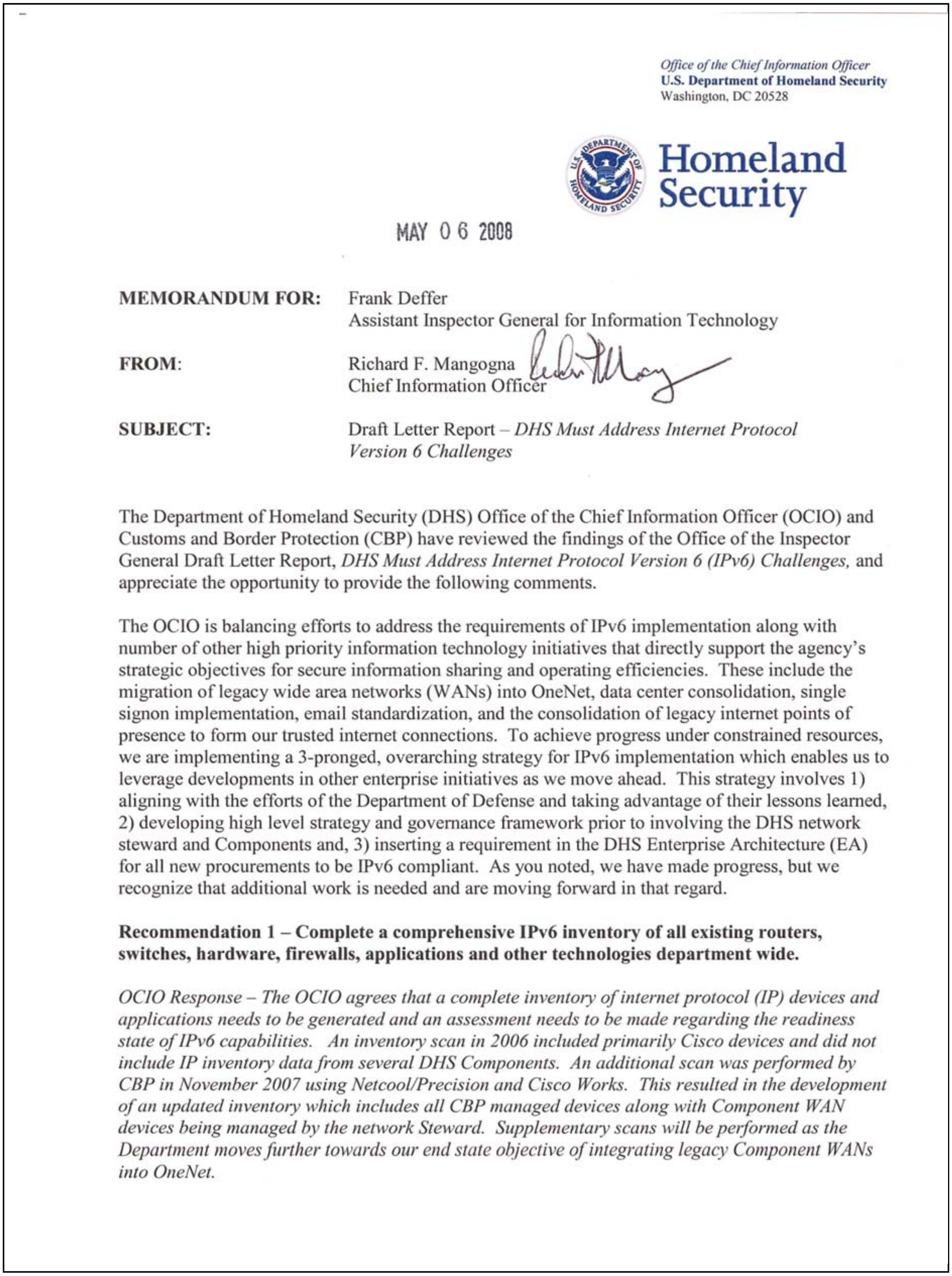
DHS concurs with recommendation 5. Efforts are underway to create a common understanding of the department's IPv6 implementation plans. The department is establishing technical and application transition work groups (to include the network steward and component representatives) to foster the planning and transition efforts. A technical workgroup will initiate in July 2008 and an application work group will initiate in October 2008.

We accept DHS' response to ensure that the DHS IPv6 program office and CBP coordinate their planning and transition efforts.

****

We conducted our audit from September to November 2007 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government audit standards.

Appendix A
Management Comments to the Draft Report



Office of the Chief Information Officer
U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

MAY 06 2008

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technology

FROM: Richard F. Mangogna
Chief Information Officer

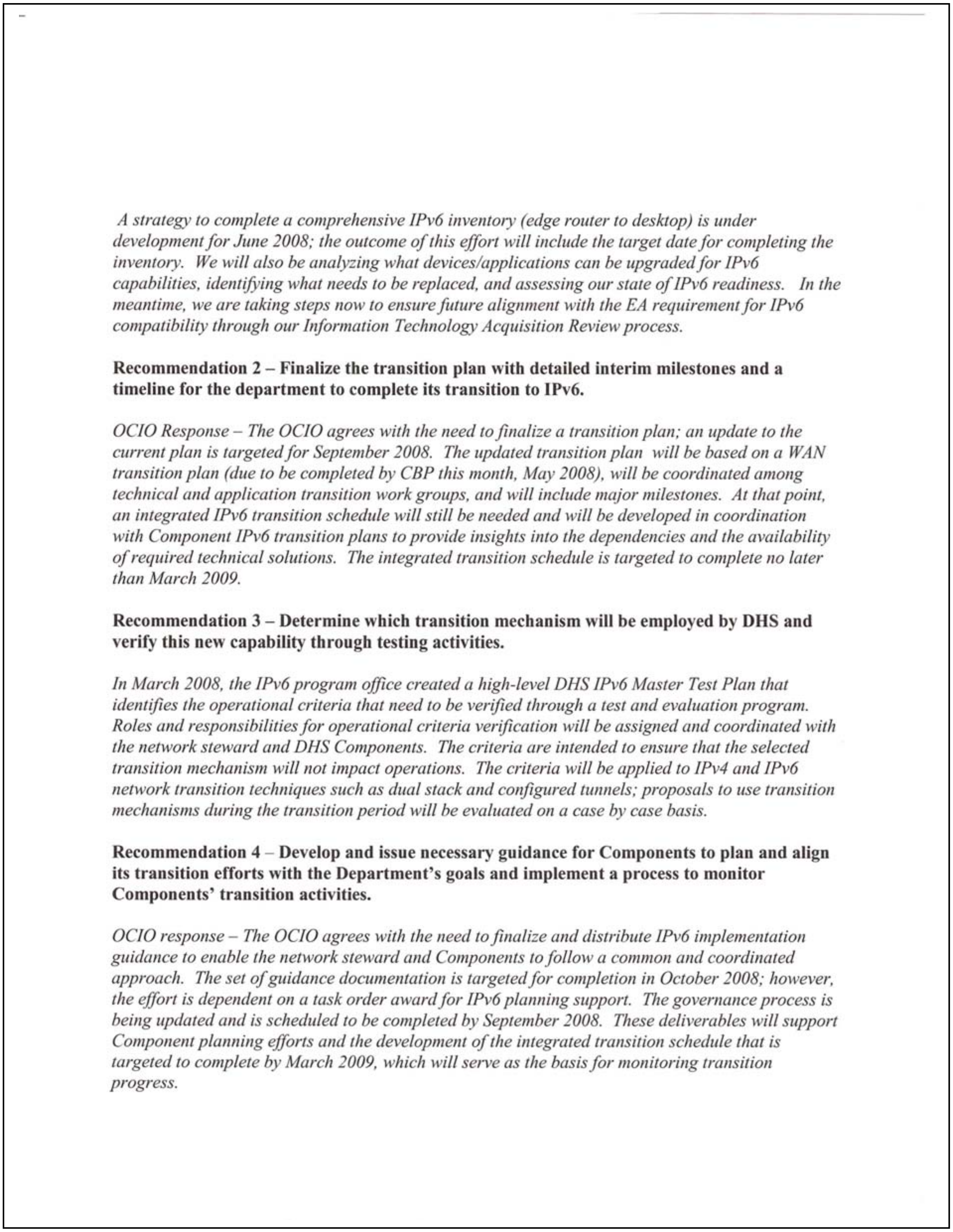
SUBJECT: Draft Letter Report – *DHS Must Address Internet Protocol Version 6 Challenges*

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) and Customs and Border Protection (CBP) have reviewed the findings of the Office of the Inspector General Draft Letter Report, *DHS Must Address Internet Protocol Version 6 (IPv6) Challenges,* and appreciate the opportunity to provide the following comments.

The OCIO is balancing efforts to address the requirements of IPv6 implementation along with number of other high priority information technology initiatives that directly support the agency's strategic objectives for secure information sharing and operating efficiencies. These include the migration of legacy wide area networks (WANs) into OneNet, data center consolidation, single signon implementation, email standardization, and the consolidation of legacy internet points of presence to form our trusted internet connections. To achieve progress under constrained resources, we are implementing a 3-pronged, overarching strategy for IPv6 implementation which enables us to leverage developments in other enterprise initiatives as we move ahead. This strategy involves 1) aligning with the efforts of the Department of Defense and taking advantage of their lessons learned, 2) developing high level strategy and governance framework prior to involving the DHS network steward and Components and, 3) inserting a requirement in the DHS Enterprise Architecture (EA) for all new procurements to be IPv6 compliant. As you noted, we have made progress, but we recognize that additional work is needed and are moving forward in that regard.

Recommendation 1 – Complete a comprehensive IPv6 inventory of all existing routers, switches, hardware, firewalls, applications and other technologies department wide.

OCIO Response – The OCIO agrees that a complete inventory of internet protocol (IP) devices and applications needs to be generated and an assessment needs to be made regarding the readiness state of IPv6 capabilities. An inventory scan in 2006 included primarily Cisco devices and did not include IP inventory data from several DHS Components. An additional scan was performed by CBP in November 2007 using Netcool/Precision and Cisco Works. This resulted in the development of an updated inventory which includes all CBP managed devices along with Component WAN devices being managed by the network Steward. Supplementary scans will be performed as the Department moves further towards our end state objective of integrating legacy Component WANs into OneNet.



A strategy to complete a comprehensive IPv6 inventory (edge router to desktop) is under development for June 2008; the outcome of this effort will include the target date for completing the inventory. We will also be analyzing what devices/applications can be upgraded for IPv6 capabilities, identifying what needs to be replaced, and assessing our state of IPv6 readiness. In the meantime, we are taking steps now to ensure future alignment with the EA requirement for IPv6 compatibility through our Information Technology Acquisition Review process.

Recommendation 2 – Finalize the transition plan with detailed interim milestones and a timeline for the department to complete its transition to IPv6.

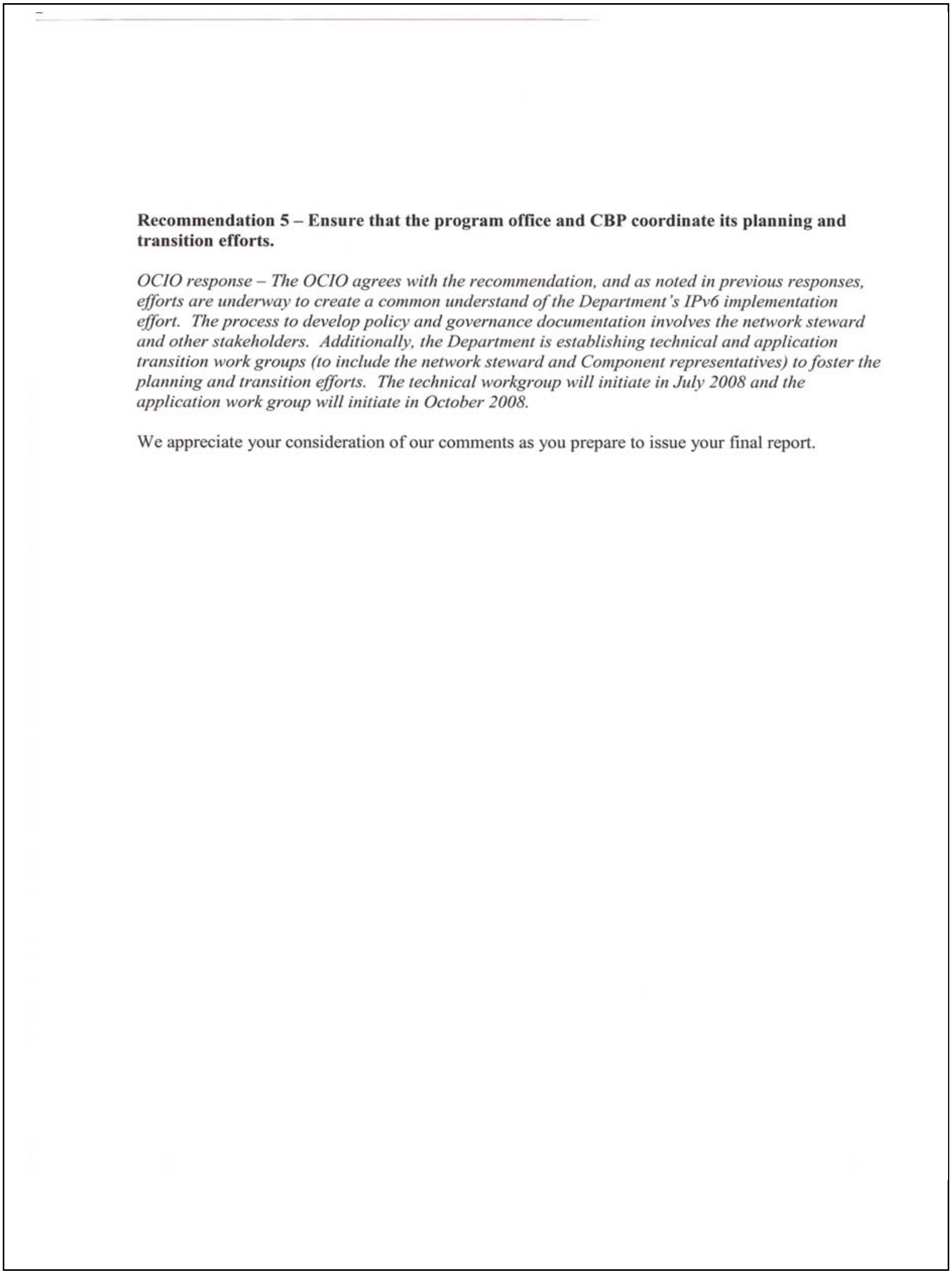
OCIO Response – The OCIO agrees with the need to finalize a transition plan; an update to the current plan is targeted for September 2008. The updated transition plan will be based on a WAN transition plan (due to be completed by CBP this month, May 2008), will be coordinated among technical and application transition work groups, and will include major milestones. At that point, an integrated IPv6 transition schedule will still be needed and will be developed in coordination with Component IPv6 transition plans to provide insights into the dependencies and the availability of required technical solutions. The integrated transition schedule is targeted to complete no later than March 2009.

Recommendation 3 – Determine which transition mechanism will be employed by DHS and verify this new capability through testing activities.

In March 2008, the IPv6 program office created a high-level DHS IPv6 Master Test Plan that identifies the operational criteria that need to be verified through a test and evaluation program. Roles and responsibilities for operational criteria verification will be assigned and coordinated with the network steward and DHS Components. The criteria are intended to ensure that the selected transition mechanism will not impact operations. The criteria will be applied to IPv4 and IPv6 network transition techniques such as dual stack and configured tunnels; proposals to use transition mechanisms during the transition period will be evaluated on a case by case basis.

Recommendation 4 – Develop and issue necessary guidance for Components to plan and align its transition efforts with the Department's goals and implement a process to monitor Components' transition activities.

OCIO response – The OCIO agrees with the need to finalize and distribute IPv6 implementation guidance to enable the network steward and Components to follow a common and coordinated approach. The set of guidance documentation is targeted for completion in October 2008; however, the effort is dependent on a task order award for IPv6 planning support. The governance process is being updated and is scheduled to be completed by September 2008. These deliverables will support Component planning efforts and the development of the integrated transition schedule that is targeted to complete by March 2009, which will serve as the basis for monitoring transition progress.



Recommendation 5 – Ensure that the program office and CBP coordinate its planning and transition efforts.

OCIO response – The OCIO agrees with the recommendation, and as noted in previous responses, efforts are underway to create a common understand of the Department's IPv6 implementation effort. The process to develop policy and governance documentation involves the network steward and other stakeholders. Additionally, the Department is establishing technical and application transition work groups (to include the network steward and Component representatives) to foster the planning and transition efforts. The technical workgroup will initiate in July 2008 and the application work group will initiate in October 2008.

We appreciate your consideration of our comments as you prepare to issue your final report.

Appendix B
Major Contributors to this Report

Edward G. Coleman, Director
Patrick Nadon, Audit Manager
Chiu-Tong Tsang, Audit Team Leader
Charles Twitty, Auditor
Nazia Khan, IT Specialist
Domingo Alvarez, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
GAO/OIG Liaison Office
Assistant Secretary for Policy
Assistant Secretary for Legislative Affairs
Assistant Secretary for Public Affairs
Deputy Under Secretary for Management
Acting Chief Information Officer
Information Systems Security Manager
Executive Director, Information Technology Services Office
Compliance and Oversight Program Director
Chief Information Officer Audit Liaison
CBP Chief Information Officer
CBP Information Systems Security Manager
CBP Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS Program Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- **Call our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**

  DHS Office of Inspector General/MAIL STOP 2600, Attention:
  Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.