OFFICE OF THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION'S IMPLEMENTATION OF INTERNET PROTOCOL VERSION 6

August 2008 **A-14-08-18064**

AUDIT REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: August 27, 2008 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Implementation of Internet Protocol Version 6 (A-14-08-18064)

OBJECTIVE

The objective of this review was to evaluate the compliance of the Social Security Administration's (SSA) implementation of Internet Protocol Version 6 (IPv6) with Federal standards and guidelines.

BACKGROUND

Internet Protocol (IP) is the "language" and set of rules computers use to communicate with one another over the Internet. The protocol that supports the Internet today - Internet Protocol Version 4 (IPv4) – provides approximately 4 billion[1] IP addresses worldwide. This limits the number of devices that can be given a unique Internet address. IPv6 will provide exponentially more[2] IP addresses that will be essential to the continued growth of the Internet and the development of new applications that leverage mobile Internet connectivity. Although the information technology (IT) community has worked around this IP address shortage in the IPv4 environment, the community views IPv6 as the true, long-term solution to the shortage. As such, the Federal Chief Information Officer (CIO) Council Architecture and Infrastructure Committee recommended[3] that Federal agencies (including SSA) prepare for the future of networking and Internet technology by enabling their networks to support IPv6.

---

[1] IPv4 provides about 4,300,000,000 addresses.

[2] IPv6 provides about 340 undecillion or 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses.

[3] "IPV6 Transition Guidance" was issued by the Federal CIO Council Architecture and Infrastructure Committee in February 2006.

On August 2, 2005, the Office of Management and Budget (OMB) issued guidance[4] on transitioning to IPv6 and established a June 30, 2008 deadline by which all agencies' networks[5] must be using[6] IPv6.

On February 22, 2007, the National Institute of Standards and Technology (NIST) issued draft guidance[7] to assist Federal agencies in the implementation of IPv6. This guidance defines standards for IPv6 that include a list of common network devices and their minimal capabilities. The standards address host devices,[8] routers, and network protection devices (including firewalls and intrusion detection/prevention devices that examine and selectively block or modify network traffic). As such, every device connected to the network will be impacted.

Over the past several years, the Internet Engineering Task Force (IETF)[9] and Federal CIO Council Architecture and Infrastructure Committee[10] have provided additional guidelines[11] to further assist in the successful implementation of IPv6.

---

[4] OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6*, August 2, 2005.

[5] The deadline applies to the network backbone (also referred to as the core network) only. The backbone (core) is the part of the network infrastructure that connects sub-networks to provide a path for exchanging data. For SSA, the core network connects the National Computer Center and the six Remote Operation Communication Centers.

[6] To be using IPv6, agencies must have their network backbone (core) operating in a dual stack (IPv4 and IPv6) or in a pure IPv6 mode that is IPv6-compliant and configured to carry operational IPv6 traffic. Throughout this document implementation will denote using IPv6 on the network backbone in a dual-stack environment.

[7] NIST, Special Publication (SP) 500-267 (Draft), *A Profile for IPv6 in the U.S. Governmen*t - Version 1.0. The draft was issued on February 22, 2007. Draft 2 was issued on January 23, 2008.

[8] Host devices are nodes that are not routers. A node is a point in a network at which lines intersect or branch, a device attached to a network, or a terminal or other point in a computer network where messages can be created, received, or transmitted.

[9] The IETF is a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet; its works are referenced in Federal CIO Council guidelines.

[10] The Federal CIO Council Architecture and Infrastructure Committee develops policy, direction, and guidance in concert with the Federal Enterprise Architecture Program Management Office in OMB to drive business process improvement, investment management, and technical decisions.

[11] IETF, Request for Comment (RFC) 3513, IPv6 Addressing Architecture, April 2003; IETF RFC 3587, IPv6 Global Unicast Address Format, August 2003; IETF RFC 4057, IPv6 Enterprise Network Scenarios, June 2005; CIO Council, IPv6 Transition Guidance, February 2006; Federal CIO Council Architecture and Infrastructure Committee, Demonstration Plan to Support Agency IPv6 Compliance, January 28, 2008.

RESULTS OF REVIEW

SSA implemented IPv6[12] and met the Federal standards and guidelines. On December 10, 2007, SSA performed tests that demonstrated its network backbone (core) was capable of transporting[13] IPv6 traffic. Furthermore, SSA provided the required IPv6 documentation to OMB on February 28, 2008, 4 months ahead of the June 30, 2008 deadline.

Additionally, after SSA completed its initial IPv6 implementation, it took the initiative to work with the Internal Revenue Service, the Veterans Administration, and NIST to build an IPv6 data exchange mechanism to send and receive IPv6 data. Each participating agency will be able to demonstrate its ability to exchange data with an external partner using IPv6 capabilities. This testing should facilitate SSA's continued implementation of IPv6. In the future, SSA needs to ensure it continues to purchase IPv6-compliant equipment per NIST standards.

Compliance with IPv6 NIST Standards

NIST standards[14] require that SSA purchase IPv6-compliant equipment. SSA's phased implementation of IPv6[15] allows it to introduce IPv6 capability to the network environment through its normal, planned-technology refresh cycles, avoiding a substantial initial cost. Although SSA is ready to implement IPv6, it still needs to operate in an IPv4 environment because it has a significant number of devices that work under IPv4. Therefore, SSA acknowledges[16] that IT assets and systems procured, developed, or acquired must be able to operate in both IPv6 and IPv4 environments.[17]

---

[12] Federal CIO Council Architecture and Infrastructure Committee's *Demonstration Plan to Support Agency IPv6 Compliance,* issued January 28, 2008 (pp. 2 and 3).

[13] SSA is capable of receiving, processing and forwarding IPv6 traffic.

[14] NIST, SP 500-267 (Draft), *A Profile for IPv6 in the U.S. Governmen*t - Version 1.0, Draft 2 dated January 23, 2008, page 3 states: "This publication seeks to assist Federal Agencies in formulating plans for the acquisition of IPv6 technologies. To achieve this, we define a standards profile for IPv6 in the USG that is intended to be applicable to all future uses of IPv6 in non-classified, non-national security federal IT systems."

[15] Phase 1: Network Core IPv6 Capability, was expected to be accomplished by June 2008. Phase 2: Extranet IPv6 Capability is expected to be accomplished by the end of Fiscal Year (FY) 2009/early FY 2010, and Phase 3: Edge-to-Edge IPv6 Capability is expected to be done in FY 2011/2012.

[16] IPv6 *Integrated Project Plan*, February 27, 2006.

[17] This is considered a dual-stack environment.

As the Agency moves forward, it needs control measures in place to ensure any new IT assets work with both IPv6 and IPv4 systems. This minimizes the cost of the Agency-wide conversion to IPv6 by ensuring that relevant IT products are procured or developed and are capable of operating in both environments.

As part of SSA's IPv6 Integrated Project Plan, the Agency ensured it was complying with NIST, the IETF, and Federal CIO Council Architecture and Infrastructure Committee guidelines. These guidelines serve as the Agency's strategic planning for future acquisitions of networks that will be operational in 2010 and beyond.

CONCLUSION AND RECOMMENDATIONS

We found SSA appropriately implemented IPv6 in accordance with Federal standards and guidelines. In the future, SSA plans to complete the transition to IPv6 while taking into consideration the costs and impacts on business operations. Therefore, we recommend SSA:

1. Continue to ensure all additional IT products that are procured or developed are capable of operating in IPv6 networks to minimize further cost to the Agency during its transition.

AGENCY COMMENTS AND OIG RESPONSE

SSA agreed with our recommendation. See Appendix C for the full text of the Agency's comments.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

CIO	Chief Information Officer
EA	Enterprise Architecture
FEA	Federal Enterprise Architecture
FY	Fiscal Year
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRM	Information Resources Management
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OS	Office of Systems
PMO	Project Management Office
RFC	Request for Comment
SP	Special Publication
SSA	Social Security Administration

Scope and Methodology

Our objective was to evaluate the Social Security Administration's (SSA) implementation of Internet Protocol Version 6 (IPv6) and its compliance with Federal standards and guidelines.

To meet our objective, we examined SSA's Office of Management and Budget (OMB) documentation, project plans, and assessments as well as its progress report on the IPv6 implementation. Specifically, we examined:

- IPv6 Phase 2 Network Inventory, February 28, 2006.
- IPv6 Business Impact Assessment, February 27, 2006.
- IPv6 Integrated Project Plan, February 27, 2006.
- IPv6 Progress Status Report, February 27, 2006.
- SSA Enterprise Architecture Transition Strategy for 2007 through 2012 (Version 2.0), February 28, 2007.
- IPv6 Capability Inventory for Routers, Switches & Firewalls, October 19, 2005.
- SSA's OMB submission from the Chief Information Officer (CIO) identifying a lead for the IPv6 initiative, November 10, 2005.
- OMB's "Federal Enterprise Architecture (FEA) Program Management Office (PMO) Assessment for Social Security Administration (SSA) Q2 FY2006 – March 2006," April 27, 2006 and OMB's "FEA PMO Enterprise Architecture (EA) Assessment for Social Security Administration (SSA) Q2 FY2007 – March 2007," November 19, 2007.
- OMB's FEA PMO Quarterly Reports for June 1, 2007; September 1, 2007; and December 1, 2007.
- Social Security Administration Network Core IPv6 Capability Demonstration report, December 10, 2007.

We also reviewed the following:

- OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, August 2, 2005.
- *IPv6 Transition Guidance*, CIO Council, Federal CIO Council Architecture and Infrastructure Committee, February 2006.
- *Demonstration Plan to Support Agency IPv6 Compliance,* Federal CIO Council Architecture and Infrastructure Committee, January 28, 2008, Version 1.0.

- National Institute of Standards and Technology Special Publication 500-267 (Draft), *A Profile for IPv6 in the U.S. Government – Version 1.0, Draft 1 dated* January 2007 and Draft 2 dated January 23, 2008.
- *Internet Protocol Version 6 -- Federal Government in Early Stages of Transition and Key Challenges Remain,* General Accountability Office, June 2006.
- *Router Security Configuration Guide Supplement - Security for IPv6 Routers*, National Security Agency, May 23, 2006.
- SSA's Information Resources Management (IRM) Strategic Plan Fiscal Year 2007.

We interviewed representatives from the following SSA components.

- The Office of the Chief Information Officer (OCIO) directs and manages SSA's enterprise information technology security program. This includes establishing Agency-wide security policies, managing the reporting, and monitoring processes to ensure compliance.
- The Office of Systems (OS), Office of Telecommunications and Systems Operations researches network prototypes, performs testing of new network technologies, and implements and monitors network standards.
- OS, Office of Enterprise Support, Architecture and Engineering, modifies the EA for the day-to-day operations. The EA may require additions, alterations, and improvements to not only meet the requirements set forth by OMB directives but to accurately reflect the architectural products being used to manage IRM resources.

We performed our field work in SSA Headquarters from November 2007 through March 2008. We determined the information used in this review was sufficiently reliable to meet our audit objectives. The audited entities were the OCIO and OS. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: August 19, 2008 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: David V. Foster /s/
Executive Counselor to the Commissioner

Subject: Office of the Inspector General (OIG) Draft Report, "The Social Security Administration's Implementation of Internet Protocol Version 6" (A-14-08-18064)--INFORMATION

We appreciate OIG's efforts in conducting this review. Attached is our response to the recommendation.

Please let me know if we can be of further assistance. Please direct staff inquiries to Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at (410) 965-4636.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "THE SOCIAL SECURITY ADMINISTRATION'S IMPLEMENTATION OF INTERNET PROTOCOL VERSION 6" (A-14-08-18064)

Thank you for the opportunity to review and provide comments on this draft report.

Recommendation 1

"Continue to ensure all additional information technology (IT) products that are procured or developed are capable of operating in Internet Protocol Version 6 (IPv6) networks to minimize further cost during its transition."

Comment

We agree. As part of the IPv6 implementation initiative, we developed policies and procedures that are closely tied to the National Institute of Standards and Technology publication of IPv6 technical profiles. The content of both the policies and the procedures will establish consideration of IPv6 capability for relevant IT products and components. We are currently reviewing the documents for final approval. We are developing similar procedures for micropurchases. We believe these actions will ensure that the introduction of IPv6-based technology is cost-effective for the agency.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kitt Winter, Director, Information Technology Audit Division (410) 965-9702

Mary Ellen Moyer, Acting Audit Manager (410) 966-1026

Acknowledgments

In addition to those named above:

Jan Kowalewski, Senior Program Analyst

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-08-18064.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.