United States Government Accountability Office

GAO

Report to Congressional Requesters

May 2005

INTERNET PROTOCOL VERSION 6

Federal Agencies Need to Plan for Transition and Manage Security Risks

GAO-05-471

May 2005

INTERNET PROTOCOL VERSION 6

Federal Agencies Need to Plan for Transition and Manage Security Risks

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-471, a report to congressional requesters

Why GAO Did This Study

The Internet protocol (IP) provides the addressing mechanism that defines how and where information such as text, voice, and video move across interconnected networks. Internet protocol version 4 (IPv4), which is widely used today, may not be able to accommodate the increasing number of global users and devices that are connecting to the Internet. As a result, IP version 6 (IPv6) was developed to increase the amount of available IP address space. It is gaining momentum globally from regions with limited address space.

GAO was asked to (1) describe the key characteristics of IPv6; (2) identify the key planning considerations for federal agencies in transitioning to IPv6; and (3) determine the progress made by the Department of Defense (DOD) and other major agencies to transition to IPv6.

What GAO Recommends

GAO recommends, among other things, that the Director of the Office of Management and Budget (OMB) instruct agencies to begin to address key planning considerations for the IPv6 transition, and that agencies act to mitigate near-term IPv6 security risks.

Officials from OMB, DOD, and Commerce generally agreed with the contents of this report and provided technical corrections, which were incorporated as appropriate.

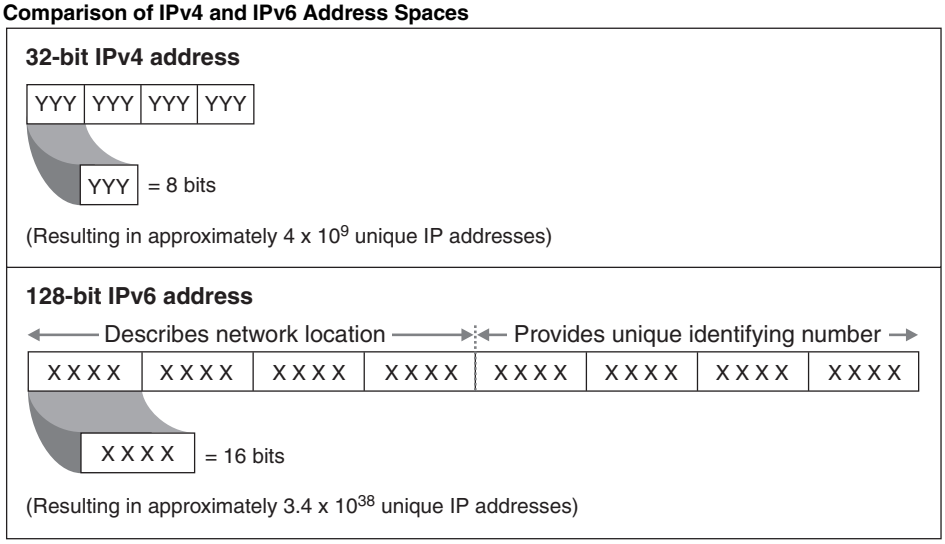
www.gao.gov/cgi-bin/getrpt?GAO-05-471.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner at (202) 512-9286 or Keith Rhodes at (202) 512-6412.

What GAO Found

The key characteristics of IPv6 are designed to increase address space, promote flexibility and functionality, and enhance security. For example, by using 128-bit addresses rather than 32-bit addresses, IPv6 dramatically increases the available Internet address space from approximately 4.3 billion addresses in IPv4 to approximately 3.4×10^{38} in IPv6 (see figure).

Comparison of IPv4 and IPv6 Address Spaces



Source: GAO.

Key planning considerations for federal agencies include recognizing that the transition is already under way, because IPv6-capable software and equipment already exists in agency networks. Other important agency planning considerations include developing inventories and assessing risks; creating business cases that identify organizational needs and goals; establishing policies and enforcement mechanisms; determining costs; and identifying timelines and methods for transition. In addition, managing the security aspects of an IPv6 transition is another consideration since IPv6 can introduce additional security risks to agency information. For example, attackers of federal networks could abuse IPv6 features to allow unauthorized traffic or make agency computers directly accessible from the Internet.

DOD has made progress in developing a business case, policies, timelines, and processes for transitioning to IPv6. Despite these efforts, challenges remain, including finalizing plans, enforcing policy, and monitoring for unauthorized IPv6 traffic. Unlike DOD, the majority of other major federal agencies reported not yet having initiated key planning efforts for IPv6. For example, 22 agencies lack business cases; 21 lack transition plans; 19 have not inventoried IPv6 software and equipment; and none had developed cost estimates.

Contents

Abbreviations

CFO	chief financial officer
DOD	Department of Defense
FAR	Federal Acquisition Regulation
GIG	global information grid
ICANN	Internet Corporation for Assigned Names and Numbers
ID	identification
IETF	Internet Engineering Task Force
IP	Internet protocol
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TCP	transmission control protocol
Y2K	year 2000
US CERT	United States Computer Emergency Response Team

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

May 20, 2005

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives
The Honorable Adam H. Putnam
House of Representatives

In 2003, the President's *National Strategy to Secure Cyberspace*[1] identified the development of secure and robust Internet mechanisms as important goals because of the nation's growing dependence on cyberspace. The Internet protocol (IP) is one of the primary mechanisms that defines how and where information such as text, voice, and video moves across networks. Internet protocol version 4 (IPv4), which is widely used today, may not be able to accommodate the increasing number of global users and devices that are connecting to the Internet. As a result, IP version 6 (IPv6) was developed to increase the amount of available IP address space. There has been increasing interest in this new version of IP and its implications for federal agencies.

As agreed with your office, our objectives were to (1) describe the key characteristics of IPv6, (2) identify the key planning considerations for federal agencies in transitioning to IPv6, and (3) determine the progress made by the Department of Defense (DOD) and other major federal agencies to transition to IPv6.

To accomplish these objectives, we researched and documented key IPv6 attributes, including security features, and analyzed technical and planning information from experts in government and industry. Additionally, we obtained and analyzed documents from the Department of Commerce. We also studied DOD plans, procedures, and actions for transitioning to IPv6. Finally, we identified efforts undertaken by the other 23 Chief Financial

[1]President George W. Bush, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

Officer (CFO) Act agencies[2] to determine their progress in addressing IPv6 transition challenges. We conducted our work from August 2004 through April 2005 in accordance with generally accepted government auditing standards. Details of our objectives, scope, and methodology are included in appendix I.

Results in Brief

The key characteristics of IPv6 are designed to increase address space, promote flexibility and functionality, and enhance security. For example, using 128-bit addresses rather than 32-bit addresses dramatically increases the available Internet address space from approximately 4.3 billion in IPv4 to approximately 3.4×10^{38} in IPv6. Other characteristics increase flexibility and functionality, including improved routing of data, enhanced mobility features for wireless, configuration capabilities to ease network administration, and improved quality of service. Further, IPv6 integrates Internet protocol security to improve authentication and confidentiality of information being transmitted. These characteristics offer various enhancements relative to IPv4 and are expected to enable advanced Internet communications and foster new software applications.

Key planning considerations for federal agencies include recognizing that an IPv6 transition is already under way because IPv6-capable software and equipment exist in agency networks. Other important agency planning considerations include: developing inventories and assessing risks; creating business cases that identify organizational needs and goals; establishing policies and enforcement mechanisms; determining costs; and identifying timelines and methods for transition. As we have previously reported, planning for system migration and security are often problematic in federal agencies. However, proactive integration of IPv6 requirements into federal contracts may reduce the costs and complexity of transition by ensuring that federal applications can operate in an IPv6 environment without costly upgrades. Managing the security aspects of the transition is another consideration, since IPv6 can introduce additional security risks to agency information. For example, attackers of federal networks could

[2]The 24 CFO departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

abuse features to allow unauthorized traffic or make agency computers directly accessible from the Internet.

Recognizing the importance of planning, DOD has made progress in developing a business case, policies, timelines, and methods for transitioning to IPv6. These efforts include creating a transition office, developing guidance and policies, drafting transition plans, and fielding a pilot. Despite these accomplishments, challenges remain, including finalizing plans, enforcing policy, and monitoring for unauthorized IPv6 traffic. Regarding other major federal agencies, most report little progress in planning for an IPv6 transition. For example, 22 agencies lack business cases; 21 lack transition plans; 19 have not inventoried IPv6 software and equipment; and 22 have not developed cost estimates.

Transitioning to IPv6 is a pervasive and significant challenge for federal agencies that could result in significant benefits to agency services. But such benefits may not be realized if action is not taken to ensure that agencies are addressing key planning considerations or security issues. Accordingly, we are recommending, among other things, that the Director of the Office of Management and Budget (OMB) instruct the federal agencies to begin addressing key IPv6 planning considerations, and that federal agency heads take immediate actions to address the near-term security risks.

In commenting on a draft of this report, officials from OMB, DOD, and Commerce generally agreed with its contents and provided technical corrections, which we incorporated, as appropriate.

Background

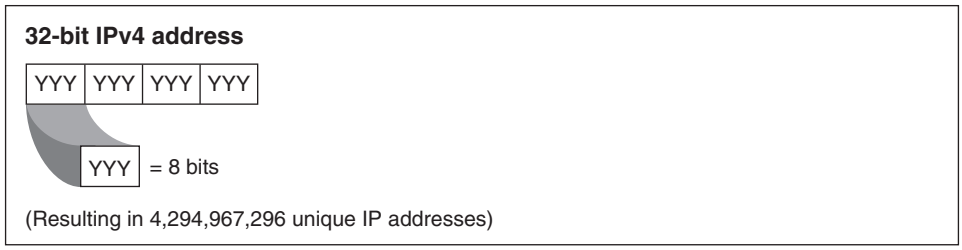
The Internet is a worldwide network of networks comprised of servers, routers, and backbone networks. Network addresses are used to help send information from one computer to another over the Internet by routing the information to its final destination. The protocol that enables the administration of these addresses is the Internet protocol (IP). The most widely deployed version of IP is version 4 (IPv4).

Internet Protocol Transmits Information across Interconnected Networks

The two basic functions of IP include (1) addressing and (2) fragmentation of data, so that information can move across networks. An IP address consists of a fixed sequence of numbers. IPv4 uses a 32-bit address format,

which provides approximately 4.3 billion unique IP addresses. Figure 1 provides a conceptual illustration of an IPv4 address.

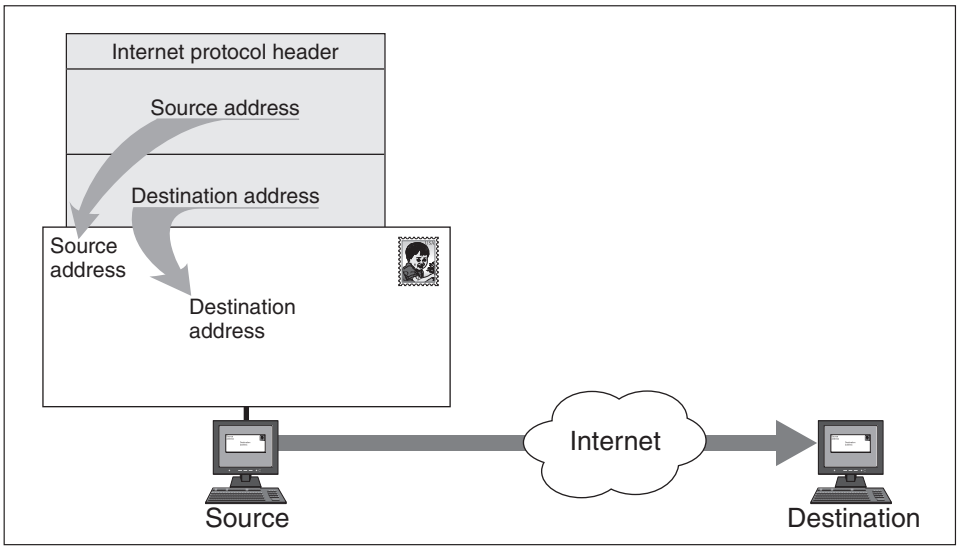
Figure 1: Internet Protocol Version 4 Address



Source: GAO.

By providing a numerical description of the location of networked computers, addresses distinguish one computer from another on the Internet. In some ways, an IP address is like a physical street address. For example, in the physical world, if a letter is going to be sent from one location to another, the contents of the letter must be placed in an envelope that contains addresses for the sender and receiver. Similarly, if data is going to be transmitted across the Internet from a source to a destination, IP addresses must be placed in an IP header. Figure 2 provides a simplified illustration of this concept. In addition to containing the addresses of sender and receiver, the header also contains a series of fields that provide information about what is being transmitted.

Figure 2: An Internet Protocol Header Contains IP Addresses for the Source and Destination of Information Transmitted across the Internet



Source: GAO.

The fields in the header are important to the protocol's second main function: fragmentation of data. IP fragments information by breaking it into manageable parts. Each part has its own header that contains the sender's address, destination address, and other information that guides it through the Internet to its intended destination. When the various packets arrive at the final destination, they are put back together into their original form.

Internet and Protocol Management and Development Involve Several Key Organizations

Several key organizations play a role in coordinating protocol development and Internet management issues, including the following:

- The Internet Corporation for Assigned Names and Numbers, (ICANN), is a nonprofit corporation responsible for Internet address space allocation and management of the Internet domain name system.[3]

[3]The Web site for ICANN is www.icann.org.

- Regional Internet Registries allocate Internet address blocks from ICANN in various parts of the world and engage in joint projects, liaison activities, and policy coordination. The registries include the African Network Information Center, Asia Pacific Network Information Centre, American Registry for Internet Numbers, Latin American and Caribbean Internet Addresses Registry, and Réseaux IP Européens Network Coordination Centre.

- Competing companies known as registrars are able to assign domain names, the mnemonic devices used to represent the numerical IP addresses on the Internet (for example, www.google.com). More than 300 registrars have been accredited by ICANN and are authorized to register domain names ending in .biz, .com, .coop, .info, .name, .net, .org, or .pro. A complete listing is maintained on the InterNIC[4] Web site.

- The Internet Society is a large, international, professional organization that provides leadership in addressing issues that may affect the future of the Internet and assists the groups responsible for Internet infrastructure standards. The Internet Society also provides legal, financial, and administrative support to the Internet Engineering Task Force (IETF).[5]

- IETF is the principal body engaged in the development of Internet standards. It is composed of working groups that are organized by topic into several areas (e.g., routing, transport, security, etc.).[6]

IPv4 Address Limitations and Mitigation Efforts

Limited IPv4 address space prompted organizations that need large amounts of IP addresses to implement technical solutions to compensate. For example, network administrators began to use one unique IP address to represent a large number of users. By employing network address translation, an enterprise such as a federal agency or a company could have large numbers of internal IP addresses, but still use a single unique address that can be reached from the Internet. In other words, all computers behind

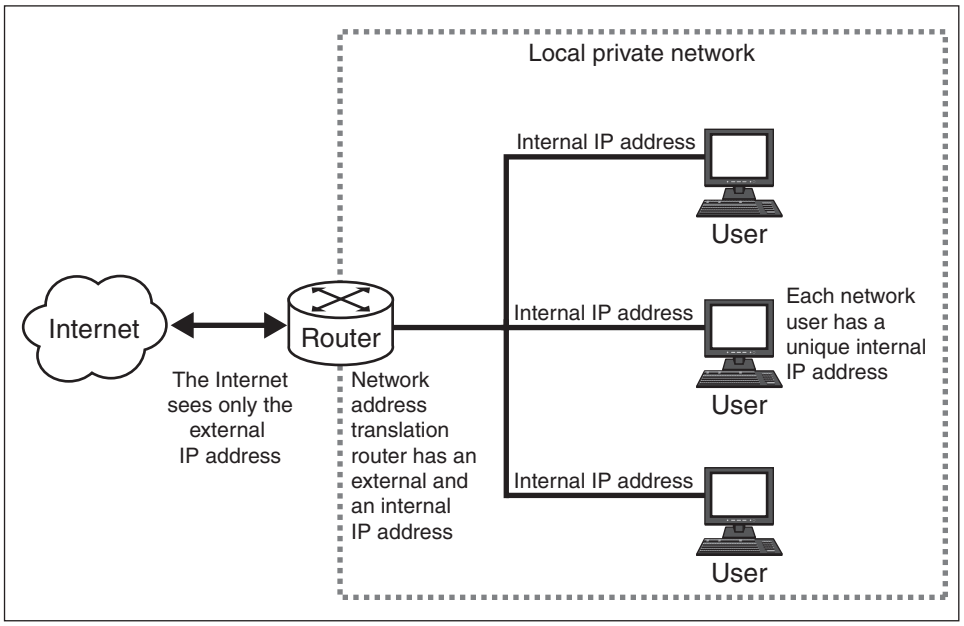
[4]InterNIC is a registered service of the U.S. Department of Commerce. It is licensed to ICANN, which operates the InterNIC Web site: http://www.internic.net/.

[5]The Web site for the Internet Society is www.isoc.org.

[6]The Web site for IETF is www.ietf.org.

the network address translation router appear to have the same address to the outside world. Figure 3 depicts this type of network configuration.

Figure 3: An Example of a Network Address Translation



Source: GAO.

While network address translation has enabled organizations to compensate for the limited number of globally unique IP addresses available with IPv4, the resulting network structure has eliminated the original end-to-end communications model of the Internet. Network address translation complicates the delivery of real-time communications over the Internet.

In 1994, IETF began reviewing proposals for a successor to IPv4 that would increase IP address space and simplify routing. IETF established a working group to be specifically responsible for developing the specifications for and standardization of IPv6. Over the past 10 years, IPv6 has evolved into a

mature standard. A complete list of IPv6 documents can be found at the IETF Web site.[7]

IPv6 Is Gaining Momentum Globally

Interest in IPv6 is gaining momentum around the world, particularly in parts of the world that have limited IPv4 address space to meet their industry and consumer communications needs. Regions that have limited IPv4 address space such as Asia and Europe have undertaken efforts to develop, test, and implement IPv6.

Asia

As a region, Asia controls only about 9 percent of the allocated IPv4 addresses, and yet has more than half of the world's population. As a result, the region is investing in IPv6 development, testing, and implementation. For example, the Japanese government's e-Japan Priority Policy Program mandated the incorporation of IPv6 and set a deadline of 2005 to upgrade existing systems in both the public and private sector. The government has helped to support the establishment of the IPv6 Promotion Council to facilitate issues related to development and deployment and to provide tax incentives to promote deployment. In addition, major Japanese corporations in the communications and consumer electronics sectors are also developing IPv6 networks and products.

The Chinese government's interest in IPv6 resulted in an effort by the China Education and Research Network Information Center to establish an IPv6 network linking 25 universities in 20 cities across China. In addition, China has reportedly set aside approximately $170 million to develop an IPv6-capable infrastructure.

Taiwan has also started to work on developing IPv6 products and services. For example, the Taiwanese government announced that it would begin developing an IPv6-capable national information infrastructure project. The planned initiative is intended to deploy an infrastructure capable of supporting 6 million users by 2007.

In September 2000, public and private entities in India established the Indian IPv6 Forum to help coordinate the country's efforts to develop and implement IPv6 capabilities and services. The forum hosted an IPv6 summit in 2005.

[7]The Web site for IETF is http://www.ietf.org/iesg/1rfc_index.txt.

Europe

The European Commission initiated a task force in April 2001 to design an IPv6 Roadmap. The Roadmap serves as an update and plan of action for the development and future perspectives of IPv6. It also serves as a way to coordinate European efforts for developing, testing, and deploying IPv6. Europe currently has a task force that has the dual mandate of initiating country/regional IPv6 task forces across European states and seeking global cooperation around the world. Europe's task force and the Japanese IPv6 Promotion Council forged an alliance to foster worldwide deployment.

Latin America

Latin America also has begun developing projects involving IPv6. Some of these projects include an IPv6 interconnection among all the 6Bone[8] sites of Latin America and a Native IPv6 Network via Internet2.[9] Also in Mexico, the National Autonomous University of Mexico has been conducting research. In 1999, the university acquired a block of address space to provide IPv6-enabled service to Mexico and Latin America.

North America

Established in 2001, the North American IPv6 Task Force promotes the use of IPv6 within industry and government and provides technical and business expertise for the deployment of IPv6 networks.[10] The task force is composed of individual members from the United States and Canada who develop white papers and deployment guides, sponsor test and interoperability events, and collaborate with other task forces from around the world. Currently, the task force, the University of New Hampshire, and DOD are collaborating on a national IPv6 demonstration/test network.

Initial Governmentwide Efforts to Address IPv6 Began in 2003

In 2003, the President's *National Strategy to Secure Cyberspace*[11] identified the development of secure and robust Internet mechanisms as important goals because of the nation's growing dependence on cyberspace. The strategy stated that the United States must understand the merits of, and the obstacles to, moving to IPv6 and, based on that understanding, identify a process for moving to an IPv6-based infrastructure.

[8]The 6bone is an IPv6 test bed created to assist in the evolution and deployment of IPv6.

[9]Internet2 is a consortium led by 207 universities working in partnership with industry and government to develop and deploy advanced network applications and technologies.

[10]The Web site for NAv6TF is http://www.nav6tf.org/.

[11]Bush, *The National Strategy.*

To better understand these challenges, the Department of Commerce formed a task force to examine the deployment of IPv6 in the United States. As co-chairs of that task force, the Commerce Department's National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration invited interested parties to comment on a variety of IPv6-related issues, including: (1) the benefits and possible uses; (2) current domestic and international conditions regarding the deployment; (3) economic, technical, and other barriers to the deployment; and (4) the appropriate role for the U.S. government in the deployment. As part of the task force's work, the Department of Commerce issued a draft report in July 2004, *Technical and Economic Assessment of Internet Protocol Version 6*,[12] that was based on the response to their request for comment. Many organizations and individuals—such as private sector software, hardware, and communications firms, and technical experts—responded, providing their views on the benefits and challenges of adopting the new protocol.

IPv6 Key Characteristics Increase Address Space, Improve Functionality, Ease Network Administration, and Enhance Security

The key characteristics of IPv6 include

- a dramatic increase in IP address space,
- a simplified IP header for flexibility and functionality,
- improved routing of data,
- enhanced mobility features,
- easier configuration capabilities,
- improved quality of service, and
- integrated Internet protocol security.

These key characteristics of IPv6 offer various enhancements relative to IPv4 and are expected to increase Internet services and enable advanced

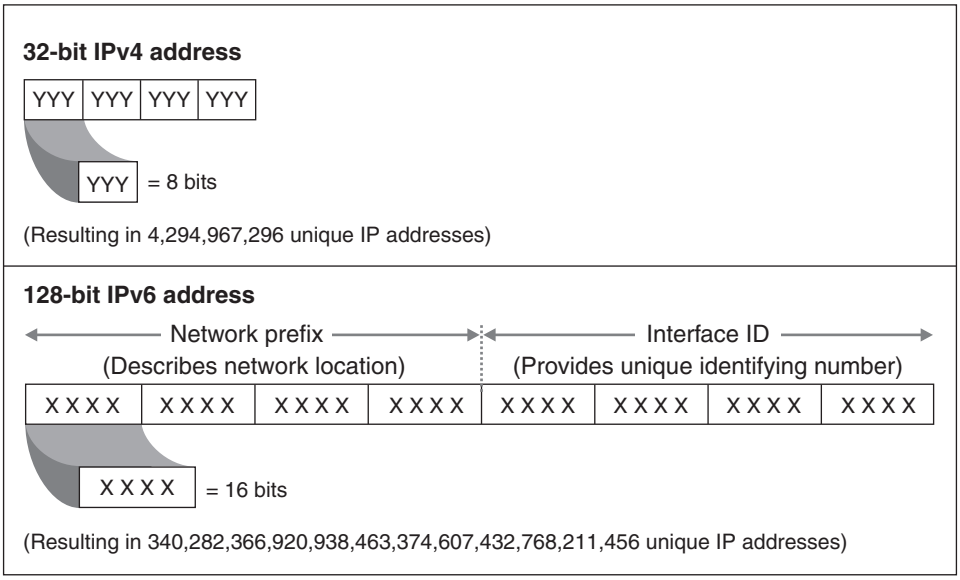
[12]Department of Commerce, *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)* (Washington, D.C.; July 2004).

Internet communications that could foster new software applications for federal agencies.

IPv6 Dramatically Increases Address Space

IPv6 dramatically increases the amount of IP address space available from the approximately 4.3 billion addresses in IPv4 to approximately 3.4×10^{38}. Because IPv6 uses a 128-bit address scheme rather than the 32-bit address scheme used in IPv4, it is able to allow many more possible addresses. The increase in the actual bits in the address and the immense number of possible combinations of numbers make the dramatic number of unique addresses a possibility. Figure 4 shows the difference between the length of an IPv4 address and that of an IPv6 address.

Figure 4: Comparison of IPv6 and IPv4 Address Scheme



Source: GAO.

This large number of IPv6 addresses means that almost any electronic device can have its own address. While IP addresses are commonly associated with computers, they are increasingly being assigned to communications devices such as phones and other items such as consumer electronics and automobiles.

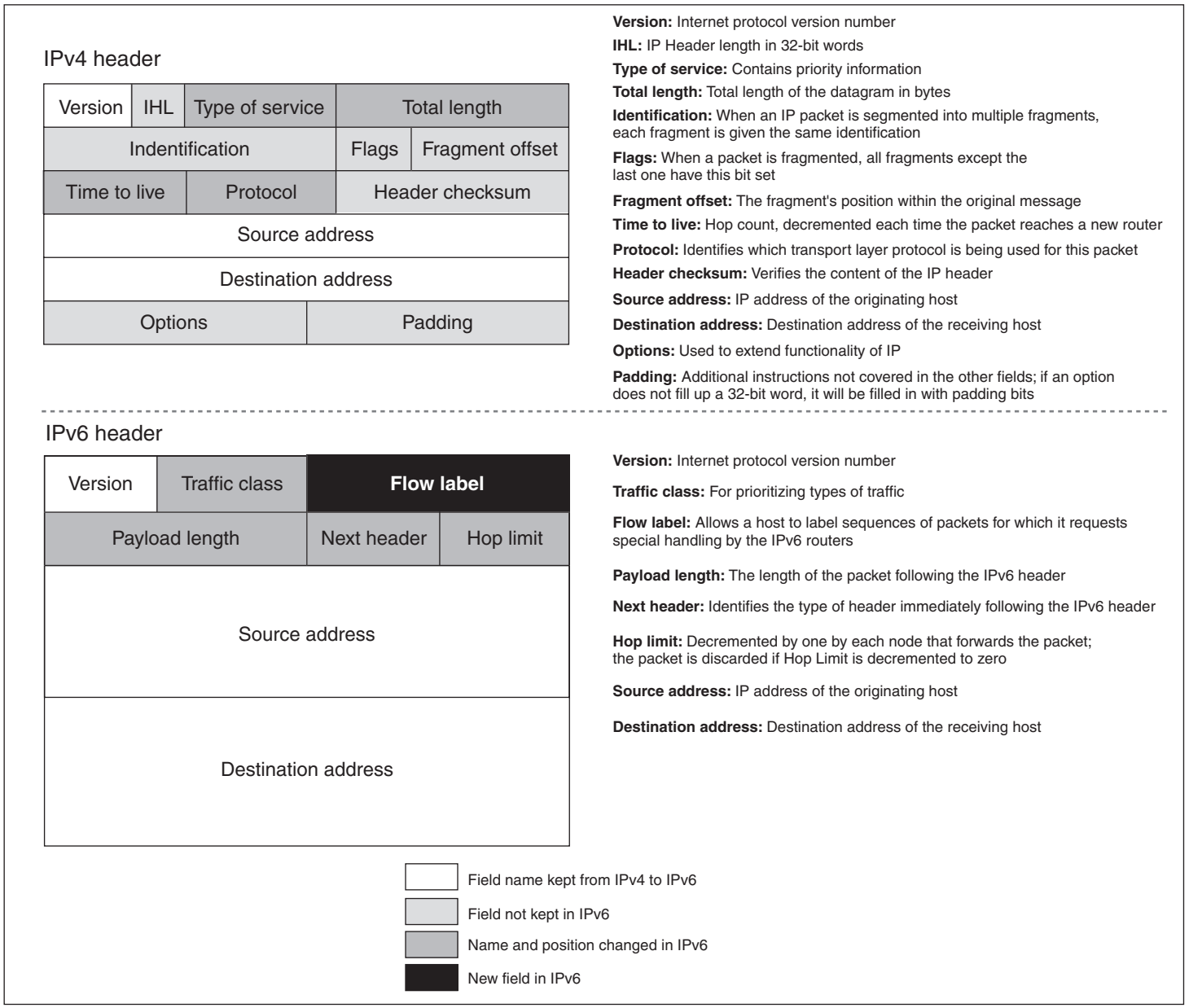
IPv6 addresses are characterized by a network prefix that describes the location of an IPv6-capable device in a network and an interface ID that provides a unique identification number (ID) for the device. The network prefix will change based on the user's location in a network, while the interface ID can remain static. The static interface ID allows a device with a unique address to maintain a consistent identity despite its location in a network. In IPv4, the limited address space has resulted in a plethora of network address translation devices, which severely limits the possibilities for end-to-end communications. In contrast, the massive address space available in IPv6 will allow virtually any device to be assigned a globally reachable address. This change fosters greater end-to-end communication abilities between devices with unique IP addresses and can better support the delivery of data-rich content such as voice and video.

Simplified Header Intended to Promote Flexibility and Functionality

Simplifying the IPv6 header promotes flexibility and functionality for two reasons. First, the header size is fixed in IPv6. In the previous version, header sizes could vary, which could slow routing of information. Second, the structure of the header itself has been simplified. While the IPv6 addresses are significantly larger than in IPv4, the header containing the address and other information about the data being transmitted has been simplified. The 14 header fields from IPv4 have been simplified to 8 fields in IPv6. Figure 5 illustrates the differences between the two IP headers, including the various data fields that were eliminated, renamed, or reorganized.

Another benefit of the simplified header is its ability to accommodate new features, or extensions. For example, the next header field provides instructions to the routers transmitting the data across the Internet about how to manage the information.

Figure 5: Major Differences between the IPv6 and IPv4 Headers



Source: GAO.

Improved Routing Offers More Efficient Movement of Information

The improved routing, or movement of information from a source to a destination, is more efficient in IPv6 because it incorporates a hierarchal addressing structure and has a simplified header. The large amount of address space allows organizations with large numbers of employees to obtain blocks of contiguous address space. Contiguous address space allows organizations to aggregate addresses under one prefix for identification on the Internet. This structured approach to addressing reduces the amount of information Internet routers must maintain and store and promotes faster routing of data. In addition, as shown in figure 5, IPv6 has a simplified header because of the elimination of six fields from the IPv4 header. The simplified header also contributes to faster routing.

Enhanced Mobility Features Provide Seamless Connectivity

IPv6 improves mobility features by allowing each device (wired or wireless) to have a unique IP address independent of its current point of attachment to the Internet. As previously discussed, the IPv6 address allows computers and other devices to have a static interface ID. The interface ID does not change as the device transitions among various networks. This enables mobile IPv6 users to move from network to network while keeping the same unique IP address. The ability to maintain a constant IP address while switching networks is cited as a key factor for the success of a number of evolving capabilities, such as evolving telephone technologies, personal digital assistants, laptop computers, and automobiles.

Enhanced Configuration Capabilities Can Ease Aspects of Network Administration

IPv6 enhancements can ease difficult and time-consuming aspects of network administration tasks in today's IPv4 networks. For example, two new configuration enhancements of IPv6 include automatic address configuration and neighbor discovery. These enhancements may reduce network administration burdens by providing the ability to more easily deploy and manage networks.

IPv6 supports two types of automatic configuration: stateful and stateless. Stateful configuration uses the dynamic host configuration protocol. This stateful configuration requires another computer, such as a server, to reconfigure or assign numbers to network devices for routing of information, which is similar to how IPv4 handles renumbering.

Stateless automatic configuration is a new feature in IPv6 and does not require a separate dynamic host configuration protocol server as in IPv4.

Stateless configuration occurs automatically for routers and hosts. Another configuration feature—neighbor discovery—enables hosts and routers to determine the address of a neighbor or an adjacent computer or router.

Together, automatic configuration and neighbor discovery help support a plug-and-play Internet deployment for many devices, such as cell phones, wireless devices, and home appliances. These enhancements help reduce the administrative burdens of network administrators by allowing the IPv6-enabled devices to automatically assign themselves IP addresses and find compatible devices with which to communicate.

Enhanced Quality of Service Can Prioritize Information Delivery

IPv6's enhanced quality of service feature can help prioritize the delivery of information. The flow label is a new field in the IPv6 header. This field can contain a label identifying or prioritizing a certain packet flow, such as a video stream or a videoconference, and allows devices on the same path to read the flow label and take appropriate action based on the label. For example, IP audio and video services can be enhanced by the data in the flow label because it ensures that all packets are sent to the appropriate destination without significant delay or disruption.

Enhanced Integration of IP Security Can Assist in Data Protection

IP Security—a means of authenticating the sender and encrypting the transmitted data—is better integrated into IPv6 than it was in IPv4. This improved integration, which helps make IP Security easier to use, can help support broader data protection efforts.

IP Security consists of two header extensions that can be used together or separately to improve authentication and confidentiality of data being sent via the Internet. The authentication extension header provides the receiver with greater assurance of who sent the data. The encapsulating security header provides confidentiality to messages using encrypted security payload extension headers.

IPv6 Characteristics Can Contribute to More Advanced Communications and Applications

IPv6's increased address space, functionality, flexibility, and security help to support more advanced communications and software applications than are thought to be possible with the current version of IP. For example, the ability to assign an IP address to a wide range of devices beyond computers creates many new possibilities for direct communication. While applications that fully exploit IPv6 are still in development, industry

experts have identified various federal functions that might benefit from IPv6-enabled applications:

- Border security: could deploy wireless sensors with IPv6 to help provide situational awareness about movements on the nation's borders.
- First responders: could exploit the hierarchal addressing of IPv6 to promote interoperability and rapid network configuration in responding to emergencies.
- Public health and safety: could exploit IPv6 end-to-end communications to deliver secure telemedicine applications and interactive diagnoses.
- Information sharing: could benefit from various features of IPv6, including securing data in end-to-end communications, quality of service, and the extensibility of the header to accommodate new functions.

IPv6 Considerations Include Significant Planning Efforts and Immediate Actions to Ensure Security

Key planning considerations for federal agencies include recognizing that an IPv6 transition is already under way because IPv6-capable software and equipment exist in agency networks. Other key considerations for federal agencies to address in an IPv6 transition include significant IT planning efforts and immediate actions to ensure the security of agency information and networks. Important planning considerations include

- developing inventories and assessing risks,
- creating business cases for an IPv6 transition,
- establishing policies and enforcement mechanisms,
- determining costs, and
- identifying timelines and methods for the transition.

Furthermore, specific security risks could result from not managing IPv6 software and equipment in federal agency networks.

Recognizing That an IPv6 Transition Is Already Under Way for the Federal Government

The transition to IPv6 is under way for many federal agencies because their networks already contain IPv6-capable software and equipment; for example, most major operating systems currently support IPv6, including Microsoft Windows, Apple OS X, Cisco IOS, mainframe software, and UNIX variants including Sun Solaris and Linux. In addition, many routers, printers, and other devices are now capable of being configured for IPv6 traffic.

The transition to IPv6 is different from a software upgrade because the protocol's capability is being integrated into the software and hardware. As a result, agencies do not have to make a concerted effort to acquire it because it will be built into agencies' core communications infrastructure. However, as IPv6-capable software and hardware accumulates in agency networks, it can introduce risks that may not be immediately obvious to the network administrators or program officials. For example, agency employees might begin using certain IPv6 features that are not addressed in agency security programs and could therefore inadvertently place agency information at risk of disclosure.

Developing an Inventory and Risk Assessment

Developing an IPv6 inventory and risk assessment is an important action for agencies to consider in addressing IPv6 decision making. An inventory of equipment (software and hardware) provides management with an understanding of the scope of an IPv6 transition occurring at the agency and assists in focusing agency risk assessments.

Risk assessments are essential steps in determining what controls are required to protect a network and what level of resources should be expended on controls. Moreover, risk assessments contribute to the development of effective security controls for information systems and much of the information needed for the agency's system security plans. These assessments are even more important when transitioning to a new technology such as IPv6. Knowing what risks there are and how to mitigate them appropriately will lessen problems in the future.

Creating a Business Case for Transition

Creating a business case for transition to IPv6 is another important consideration for agency management officials to address. A business case usually identifies the organizational need for the system and provides a clear statement of the high-level system goals.[13] Best practices for IT investment recommend that, prior to making any significant project investment, information about the benefits and costs of the investment should be analyzed and assessed in detail. One key aspect to consider while drafting the business case for IPv6 is to understand how many devices an agency wants to connect to the Internet. This will help in determining how much IPv6 address space is needed for the agency. Within the business case, it is crucial to include how the new technology will integrate with the agency's existing enterprise architecture.

Establishing Policies and Enforcement Mechanisms

Developing and establishing IPv6 transition policies and enforcement mechanisms are important considerations for ensuring an efficient and effective transition. For example, IPv6 policies can address

- agency management of the IPv6 transition,
- roles and responsibilities of key officials and program managers,
- guidance on planning and investment,
- authorization for using IPv6 features, and
- configuration management requirements and monitoring efforts.

Further, because of the scope, complexities, and costs involved in an IPv6 transition, effective enforcement of agency IPv6 policies is an important consideration for management officials. Enforcement considerations could include

- collaboration among the chief information officer and senior contracting officials to ensure IPv6 issues are addressed in information technology acquisitions in accordance with agency policy;

[13]GAO, *Technology Assessment*, *Cybersecurity for Critical Infrastructure Protection*, GAO-04-321 (Washington, D.C.: May 2004).

- role definitions for the chief information officer, inspector general, and program officials, to review current IPv6 capabilities in agency systems and what, if any, future requirements might be needed; and

- policies for configuration management methods, to ensure that agency information and systems are not compromised because of improper management of information technology and systems.

Without appropriate policies and effective enforcement mechanisms, federal agencies could incur significant cost and security risks. As we have previously reported,[14] planning for system migration and security are often problematic in federal agencies. IPv6 planning efforts and security measures can be managed using the federal government's existing framework, which includes enterprise architecture, investment management processes, and security policies, plans, and risk assessments. The potential scope of an IPv6 transition makes development of robust policies and enforcement mechanisms essential.

Determining IPv6 Costs

Considering the costs of IPv6 and estimating the impact on agency IT investments can be challenging. Cost benefit analyses and return-on-investment calculations are the normal methods used to justify investments.[15] Initially, IPv6 may appear to have a minimal cost impact on an organization because IPv6 functionality is being built into operating systems and routers. However, the costs to upgrade existing software applications so they can benefit from IPv6 functionality could be significant. Additional costs to consider include

- human capital costs associated with training,

- operational costs of multiple IP environments,

[14]GAO, *Business Systems Modernization: Internal Revenue Service Needs to Further Strengthen Program Management*, GAO-04-438T (Washington, D.C.: Feb. 12, 2004); and *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls*, GAO-04-722 (Washington, D.C.: July 30, 2004).

[15]GAO, *DOD Business Systems Modernization: Longstanding Management and Oversight Weaknesses Continue to Put Investments at Risk*, GAO-03-553T (Washington, D.C.: March 31, 2003).

- existing IT infrastructure, and

- timing of an IPv6 transition.

These costs can be managed through a gradual, rather than an accelerated, transition process. For example, long-range planning can help to mitigate costs and position an agency to benefit from IPv6's characteristics and applications. Early adopters of IPv6 have determined that transitioning can be coordinated with an organization's ongoing technical refreshments or upgrades. Accordingly, agencies can ensure that IPv6 compatibility is integrated into their IT contracts and acquisition process. Officials from OMB's Office of E-Government and Information Technology stated that they recognize the challenges associated with determining cost and are taking action. For example, OMB required federal agencies to submit the following items by January 31, 2005:

- an updated enterprise architecture documentation and a revised Information Resource Management strategic plan to illustrate how IPv6 is being incorporated into the agency's plans and

- a joint memorandum from the agency's chief information officer and chief procurement official describing how the agency will address the acquisition of technology with IPv6 as part of the life cycle of existing investments.

During the year 2000 (Y2K) technology challenge, the federal government amended the *Federal Acquisition Regulation* (FAR) and mandated that all contracts for IT include a clause requiring the delivered systems or service to be ready for the Y2K date change.[16] This helped prevent the federal government from procuring systems and services that might have been obsolete or that required costly upgrades. Similarly, proactive integration of IPv6 requirements into federal acquisition requirements can reduce the costs and complexity of the IPv6 transition of the federal agencies and ensure that federal applications are able to operate in an IPv6 environment without costly upgrades.

[16]48 C.F.R. 39.106.

Identifying Timelines and Methods for Transition

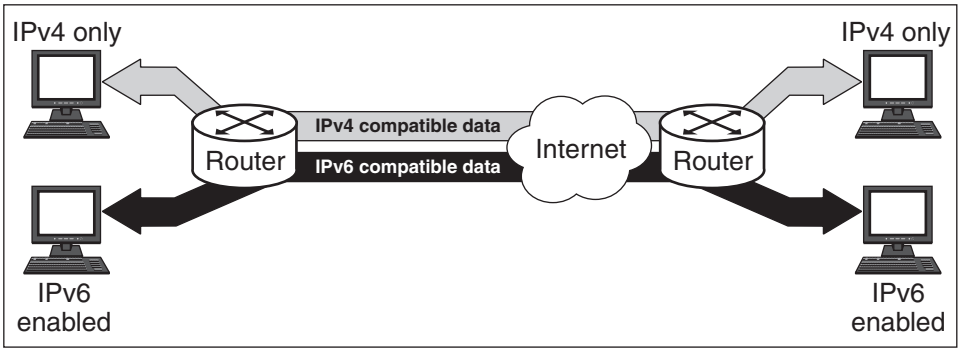
Identifying timelines and the various methods available to agencies for transitioning to IPv6 are important management considerations. The timeline can help keep transition efforts on schedule and can provide for status updates to upper management. Having a timeline and transition management strategy in place early is important to mitigating risks and ensuring a successful transition to IPv6. Such timelines and process management can help a federal agency determine when to authorize its various component organizations to allow IPv6 traffic and features.

Various transition methods exist to ensure that a computer running IPv6 can communicate with a computer running IPv4. These transition methods or techniques include the following:

Dual Stack Networks

In a dual stack network, hosts and routers implement both IPv4 and IPv6. Figure 6 depicts how dual stack networks can support both IPv4 and IPv6 services and applications during the transition period. Currently, dual stack networks are the preferred mechanism for transitioning to IPv6.

Figure 6: Example of a Dual Stack Network

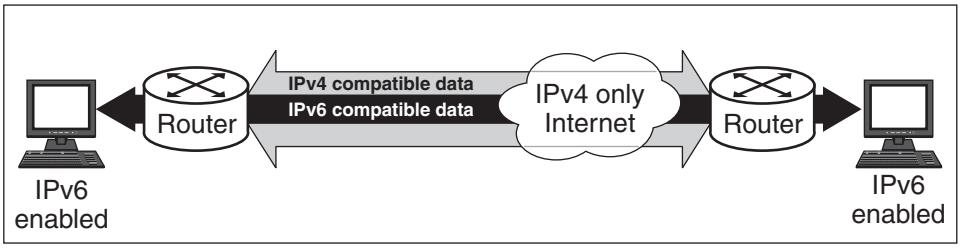


Source: GAO.

Tunneling

Tunneling allows separate IPv6 networks to communicate via an IPv4 network. For example, for one type of tunneling method, IPv6 packets are encapsulated by a border router, sent across an IPv4 network, and decoded by a border router on the receiving IPv6 network. Figure 7 depicts the tunneling process of IPv6 data inside an IPv4 network.

Figure 7: Example of Tunneling IPv6 Traffic inside an IPv4-Only Internet



Source: GAO.

Translation

Translation allows networks using only IPv4 and networks using only IPv6 to communicate with each other by translating IPv6 packets to IPv4 packets. The use of a translator allows new systems to be deployed as IPv6 only, while older systems remain IPv4 only. While this method may result in bottlenecks while packets are being translated, it can provide a high level of interoperability.

These transition methods represent a few of the common approaches for ensuring interoperability between IPv6 and IPv4 communications. They can be used alone or in concert to enable communication among IPv4 and IPv6 networks. However, while such techniques mitigate interoperability challenges, in some instances, they may result in increased security risks if not analyzed and managed.

IPv6 Creates New Opportunities for Network Abuse

As IPv6-capable software and devices accumulate in agency networks, they could be abused by attackers if not managed properly. For example, IPv6 is included in most computer operating systems and, if not enabled by default, is easy for administrators to enable either intentionally or as an unintentional byproduct of running a program. We tested two IPv6 features—automatic configuration and tunneling—and found that, if not properly managed, they could present serious risks to federal agencies.

Automatic Configuration Can Facilitate Network Attacks If Not Managed

Automatic configuration can facilitate attacks because a rogue or unauthorized router may reconfigure neighboring devices by assigning them new addresses and routes. Once IPv6 is enabled, almost all operating systems will automatically configure IPv6 addresses, and most will automatically configure additional IPv6 addresses (including global ones) and routes provided by IPv6 routers. For example, with IPv6 enabled, most

systems we tested would automatically accept IPv6 router advertisements. This results in hosts automatically adding IPv6 addresses and routes. This can be mitigated by the signing of router renumbering updates with IP Security. We tested the security issues surrounding the automatic configuration and found that, if a computer on the internal network had turned IPv6 on, that computer could use IPv6 services on other systems using IPv6 locally. This activity would not be seen by a typical IPv4 network intrusion detection system, because it would only be looking for anomalous or inappropriate IPv4 behavior and would not detect the IPv6 activity.

Tunneling Can Permit Unauthorized Traffic

As previously discussed, tunneling is a transition mechanism that allows IPv6 packets to be sent between computers via IPv4 traffic. When IPv6 packets are tunneled through IPv4, they are invisible to typical network intrusion detection systems and firewalls that are configured for IPv4 traffic but not for IPv6 traffic. As a result, intrusion detection systems and firewalls configured for IPv4 may not identify or prevent tunneled traffic. Once tunnels are established, traffic can penetrate the network undetected. This can allow attackers to access agency information and resources that are protected only by IPv4 filters and tools. Even worse, if a computer on an internal network acted as an IPv6 router and was able to tunnel IPv6 to the IPv4 Internet, other nearby machines could be automatically configured with global IP addresses. As a result, internal agency computers—never intended to directly provide services to other computers on the Internet—are suddenly globally reachable and may lack the requisite security for Internet-accessible hosts.

Although new tools are being developed, the security considerations associated with an IPv6 transition make configuration management of federal systems extremely important. We determined that common IPv6 tunneling techniques could be controlled by implementing best practices for IPv4 security, specifically by tightening the firewalls to deny direct outbound connections and by requiring proxies for allowed protocols and ports. We also noted that tighter configuration management, including restricting user privileges, could help control IPv6 usage by end hosts and that network intrusion detection systems could be tuned to detect IPv6 traffic and common tunneling techniques.

US-CERT Issued a Security Alert for Federal Agencies

In April 2005, the United States Computer Emergency Response Team (US-CERT), located at the Department of Homeland Security, issued an IPv6 cyber security alert to federal agencies based on our testing and discussions with DHS officials. The alert warned federal agencies that

unmanaged, or rogue, implementations of IPv6 present network management security risks. Specifically, the US-CERT notice informed agencies that some firewalls and network intrusion detection systems do not provide IPv6 detection or filtering capability, and malicious users might be able to tunnel IPv6 traffic through these security devices undetected. US-CERT provides agencies with a series of short-term solutions, including

- determining if firewalls and intrusion detection systems support IPv6 and implement additional IPv6 security measures and
- identifying IPv6 devices and disabling if not necessary.[17]

Progress Has Been Made at Defense but Is Lacking at Other Federal Agencies

Recognizing the importance of planning, DOD has made progress in developing a business case, policies, a timeline, and methods for transitioning to IPv6, but similar efforts at the majority of the other CFO agencies are lacking. Despite these efforts, Defense still faces major challenges in managing its transition to IPv6. The majority of the other CFO agencies report they have not begun to address key transition planning issues, such as developing plans, business cases, and estimating costs.

DOD Has Established a Business Case for Transitioning to IPv6

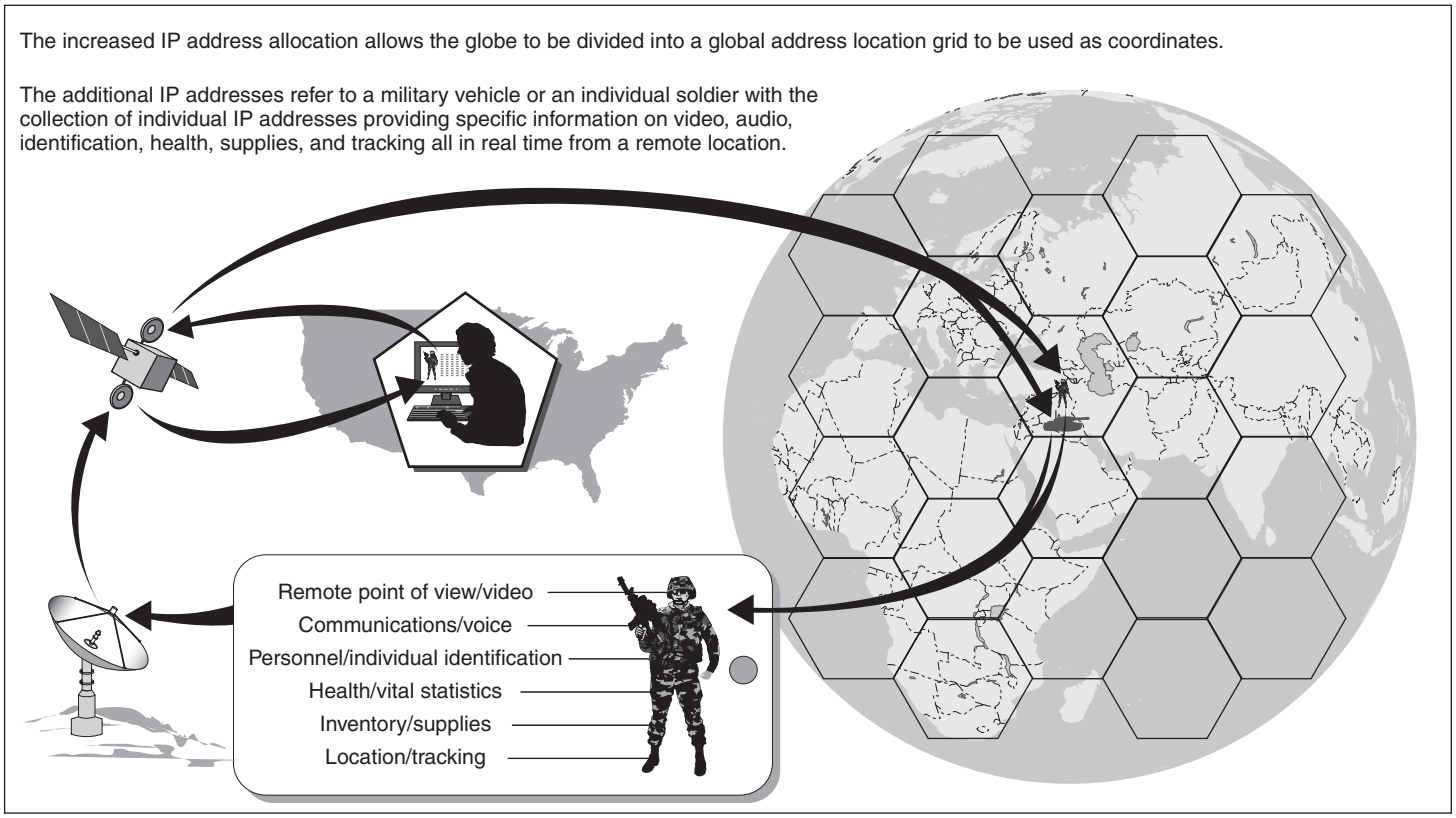
Defense's transition to IPv6 is a key component of its business case to improve interoperability among many information and weapons systems, known as the Global Information Grid (GIG). The IPv6 component of GIG is to facilitate DOD's goal of achieving network-centric operations by exploiting these key characteristics of IPv6:

- increased address space,
- enhanced mobility features,
- enhanced configuration features,
- enhanced quality of service, and
- enhanced security features.

[17]US-CERT Federal Informational Notice FIN05-095 (Arlington, Virginia; April 2004).

The increased address space provides DOD with an opportunity to reconstitute its address space architecture to better address the future proliferation of numerous unmanned sensors and mobile assets. Using this architecture, the department plans to use IPv6 as part of the GIG. Although no final decisions have been made, DOD could use the increased address space to render a three-dimensional map of the globe, or theater of combat, using IP addresses as coordinates. This, along with other GIG components, would allow tracking movements of, and maintain detailed information on, military vehicles and individual soldiers in real time.

Figure 8: DOD Envisions Mapping the Globe with Unique IP Addresses



Sources: GAO (analysis), MapArt.

Permitting devices to directly communicate on the move is essential, because DOD wants to use the enhanced mobility and automatic configuration to rapidly deploy networks across the globe. Further, Defense believes that the return to an end-to-end communications security model will allow it to provide greater information assurance by, among other things, providing for more secure peer-to-peer communications. Finally, Defense requires IPv6's improved quality of service features to enhance many of its other initiatives, such as voice over IP.

DOD Has Made Progress Developing Policies, a Timeline, and Methods for Transition

DOD's efforts to develop policies, timelines, and methods for transitioning to IPv6 are progressing. Some of the department's efforts to transition to IPv6 have been under way for approximately 10 years, including the following:

- In 1995, the Department of the Navy first began working with IPv6, and subsequently deployed IPv6 test beds in 2000 and 2001.
- In 1998, DOD began, along with our North Atlantic Treaty Organization partners, joint action on IPv6-related issues.
- In 2003, one of the Navy's early test beds, the Defense Research and Engineering Network, was selected to be the overall DOD IPv6 pilot.
- In 2003, the Office of the DOD Chief Information Officer issued a mandate that, as of October 2003, all assets developed, procured, or acquired must be IPv6-capable and, in addition, the assets must maintain interoperability with IPv4 systems capabilities.
- In 2004, Defense established an IPv6 transition office to provide the overall coordination, common engineering solutions, and technical guidance across the department to support an integrated and coherent transition to IPv6.

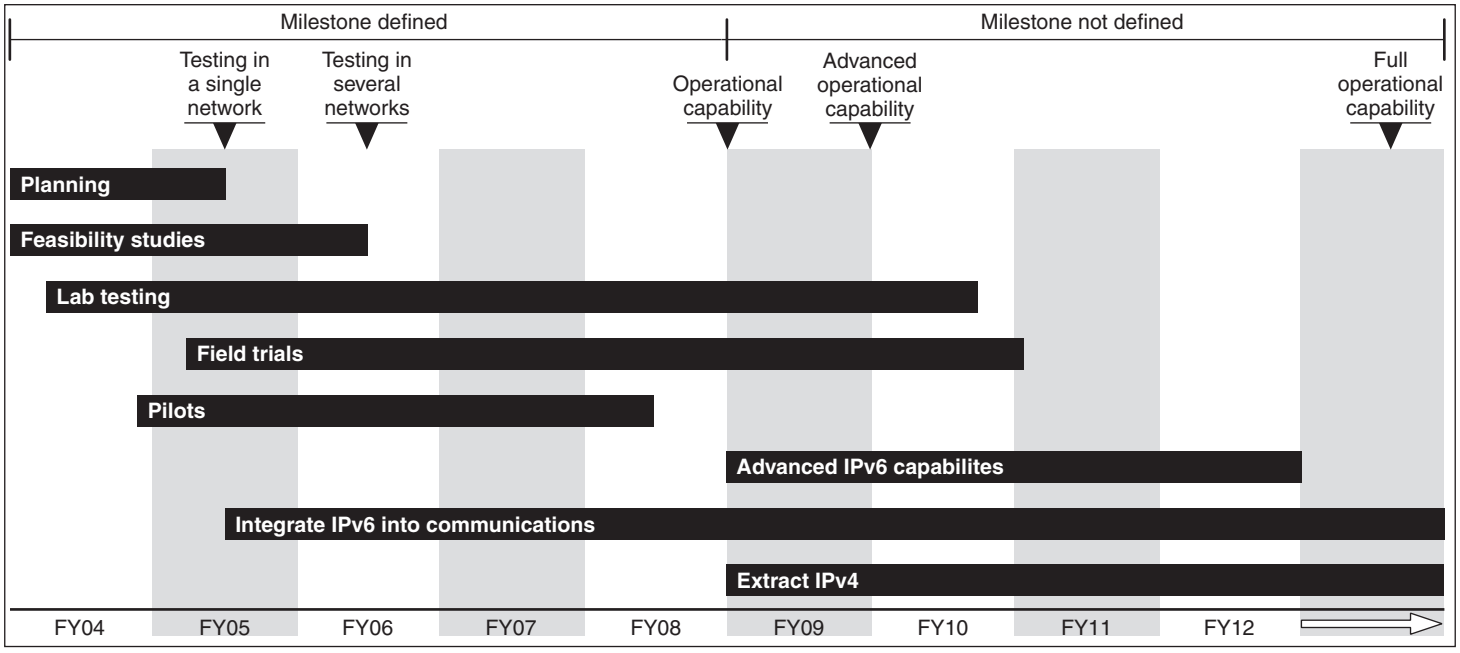
IPv6 Transition Office Performs Central Role in Coordination of Transition Planning

DOD's Transition Office performs a central role in coordination of IPv6 planning, including developing detailed guidance and policies for implementing schedules and designs for DOD. This guidance includes deriving departmentwide requirements, technical guidance—including IPv6 addressing—transition techniques, network architecture guidance, and applications development guidance. While the Transition Office provides the overall planning framework, the accountability for the actual transition resides within each of the individual services and defense

agencies. These DOD components are to use the core planning guidance, time frames, and metrics that the Transition Office develops within their respective transition models.

The Transition Office, under the authority of the Defense Information Systems Agency, is in the early stages of its work and has developed an early set of work products, including a draft system engineering management plan, risk management planning documentation, budgetary documentation, requirements criteria, and a master schedule. The management schedule includes a set of implementation milestones that include DOD's goal of transitioning to IPv6 by fiscal year 2008. A senior Transition Office official stated that the department plans to develop an end-to-end communications security model by fiscal year 2008 as well.

Figure 9: DOD's Schedule for Transitioning to IPv6



Source: DOD IPv6 Transition Office.

In addition to its internal IPv6 coordination-related activities, the Transition Office has built relationships with other federal agencies, North Atlantic Treaty Organization partners and coalition allies, IETF, and academic institutions, and is currently working with the American Registry of Internet numbers to allocate the requisite IPv6 address space for the department.

In parallel with the Transition Office's efforts, the Office of the DOD Chief Information Officer has created a transition plan that includes sections on transition governance, acquisition and procurement, transition tasks and milestones, and program and budget. The Chief Information Officer has responsibility for ensuring a coherent and timely transition, establishing and maintaining the overall departmental transition plan, and is the final approval authority for any IPv6 transition waivers. Other key players in the department's transition are the Defense Information Systems Agency, Joint Forces Command, the National Security Agency, and the Defense Intelligence Agency.

DOD IPv6 Efforts Face Challenges

Although DOD has made substantial progress in developing a planning framework for transitioning to IPv6, it still faces challenges, including

- developing an inventory of GIG systems that have IPv6-capable software and hardware,
- finalizing its IPv6 transition plans,
- monitoring its operational networks for unauthorized IPv6 traffic, and
- developing a comprehensive enforcement strategy, including leveraging its existing budgetary and acquisition review process.

According to DOD officials, the department recognizes the need to monitor IPv6 traffic and has taken steps to minimize this risk. For example, it has established policies addressing IPv6 use in an operational environment.

Majority of Federal Agencies Have Not Initiated Transition Planning Efforts

Unlike DOD, the majority of other federal agencies reporting have not yet initiated transition planning efforts for IPv6. For example, of the 22 agencies that responded, only 4 agencies reported having established a date or goal for transitioning to IPv6. The majority of agencies have not addressed key planning considerations (see table 1). For example,

- 22 agencies report not having developed a business case,
- 21 agencies report not having plans,
- 19 agencies report not having inventoried their IPv6-capable equipment, and
- 22 agencies report not having estimated costs.

Agency responses demonstrate that few efforts outside of DOD have been initiated to address IPv6. If agency planning is not carefully monitored, it could result in significant and unexpected costs for the federal government.

Table 1: IPv6 Reported Actions of 23 CFO Agencies to Address an IPv6 Transition

Department or agency	Business case	Plan	Inventory	Estimated costs
Agriculture	○	○	○	○
Commerce	○	○	○	○
Education	○	○	○	○
Energy	○	○	○	○
Health and Human Services	○	○	○	○
Homeland Security	○	○	○	○
Housing and Urban Development	—	—	—	—
Interior	○	○	○	○
Justice	○	○	○	○
Labor	○	○	○	○
State	○	○	●	○
Transportation	○	○	●	○
Treasury	○	○	○	○
Veterans Affairs	○	○	○	○
Environmental Protection Agency	○	○	○	○
General Services Administration	○	○	○	○
National Aeronautics and Space Administration	○	○	○	○
National Science Foundation	○	●	○	○
Nuclear Regulatory Commission	○	○	○	○
Office of Personnel Management	○	○	○	○
Small Business Administration	○	○	●	○
Social Security Administration	○	○	○	○
U.S. Agency for International Development	○	○	○	○

○ = No ● = Yes — = No response

Source: GAO analysis of agency data.

Conclusions

The increase in IPv6 address space and the other new features of the protocol are designed to promote flexibility, functionality, and security in networks. IPv6 can facilitate the development of a variety of new applications that take advantage of the end-to-end communications it provides. Through the use of IPv6 and associated new applications, federal

agencies can have new ways of delivering business service and conducting operations.

Nevertheless, transitioning to IPv6 presents federal agencies with challenges, including addressing key planning considerations and taking immediate actions to ensure the security of agency information and networks. By recognizing that an IPv6 transition is under way, agencies can begin developing risk assessments, business cases, policies, cost estimates, timelines, and methods for the transition. If agencies do not address these key planning issues and seek to understand the potential scope and complexities of IPv6 issues—whether agencies plan to transition immediately or not—they will face potentially increased costs and security risks. For example, if federal contracts for IT systems and services do not require IPv6 compatibility, agencies may need to make costly upgrades. Finally, if not managed, existing IPv6 features in agency networks can be abused by attackers who have access to federal information and resources without being detected. Undetected penetrations of federal networks can have far-reaching impacts on the security of both information and the operations it supports.

Transitioning to IPv6 is a pervasive challenge for federal agencies that could result in significant benefits to agency services. But such benefits may not be realized if action is not taken to ensure that agencies are addressing the attendant challenges. Recognizing the importance of planning, DOD has made progress addressing some key planning considerations, but still faces challenges. However, the vast majority of federal agencies have not yet started this process. If their respective progress is not monitored closely, it could result in significant costs for the federal government.

Recommendations for Executive Action

We recommend that the Director of OMB take the following two actions:

1. Instruct federal agencies to begin addressing key IPv6 planning considerations, including
   - developing inventories and assessing risks,
   - creating business cases for the IPv6 transition,
   - establishing policies and enforcement mechanisms,

- determining costs, and
- identifying timelines and methods for transition, as appropriate.

2. Amend the Federal Acquisition Regulation with specific language that requires that all information technology systems and applications purchased by the federal government be able to operate in an IPv6 environment.

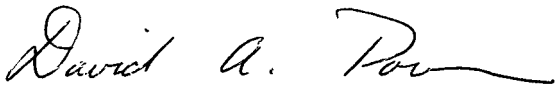
Because of the immediate risk that poorly configured and unmanaged IPv6 capabilities present to federal agency networks, we are recommending that agency heads take immediate actions to address the near-term security risks, including determining what IPv6 capabilities they may have, and initiate steps to ensure that they can control and monitor IPv6 traffic.

Agency Comments and Our Evaluation

We provided a draft of this report to DOD, Commerce, and OMB for review and comment. In providing oral comments, officials from DOD's IPv6 Transition Office, Commerce's National Institute of Standards and Technology, and OMB's Offices of Information and Regulatory Affairs and General Counsel generally agreed with the contents of the report and provided technical corrections, which we incorporated, as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to interested congressional committees; the Director, Office of Management and Budget; and the heads of all major departments and agencies. Copies of this report will be made available to others on request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you have any questions about this report, please contact David Powner at (202) 512-9286, or pownerd@gao.gov; Keith Rhodes at (202) 512-6412, or rhodesk@gao.gov; or J. Paul Nicholas at (202) 512-4457, or nicholasj@gao.gov. Major contributors to this report are listed in appendix II.



David A. Powner
Director, Information Technology Management Issues

Keith A. Rhodes
Chief Technologist
Director, Center for Technology and Engineering

Objectives, Scope, and Methodology

The objectives of our review were to

- describe the key characteristics of Internet Protocol version 6 (IPv6);
- identify the key planning considerations for federal agencies in transitioning to IPv6; and
- determine the progress made by the Department of Defense (DOD) and other major federal agencies to transition to IPv6.

For our first two objectives, the scope included the Department of Commerce, the Office of Management and Budget, and various federal and nonfederal technical experts. For our third objective, we focused on DOD and the other 23 major federal departments and agencies.

To describe the key characteristics of IPv6 and identify the key considerations for the federal agencies in transitioning to IPv6, we researched and analyzed technical documents and gathered data from IPv6 experts in government and industry. Specifically, we reviewed a number of key documents and text, including IPv6-related documents from the Internet Engineering Task Force, technical papers on IPv6 capabilities and security issues, the *President's National Strategy to Secure Cyberspace*, and responses to the Department of Commerce's request for comment on the IPv6 transition. In addition, we documented IPv6 characteristics and transition considerations with officials from the National Institute of Standards and Technology, the National Telecommunication and Information Administration, the chief technical officer of the IPv6 Forum, a co-author of the TCP/IP protocol suite, key members of the telecommunications industry, members of the Internet Engineering Task Force and Internet Society, and officials from major software and hardware vendors. Further, we conducted computer security tests using our lab to identify potential IPv6 security challenges, including testing stateful packet filtering firewalls, network intrusion detection systems, and hosts representing a variety of operating systems, including Windows XP/2003, Sun Solaris, Linux variants, and IBM z/OS. We used IPv4 firewall rules that "default deny all" inbound and "default permit all" outbound, and network intrusion detection systems with default signatures.

To determine the progress made by DOD and other relevant federal agencies to transition to IPv6, we analyzed DOD's IPv6 transition plans, guidelines, and transition schedule. In addition, we met with the Office of the DOD Chief Information Officer, members of the DOD IPv6 Transition

Office, and the Defense Information Systems Agency, and reviewed transition challenges and approaches being undertaken by DOD. We also surveyed the other 23 chief financial officer agencies to determine the extent to which they had established a transition date for converting to IPv6; developed IPv6 business cases or transition plans; estimated costs or allocated money for the transition; and identified resource challenges.

We performed our work from August 2004 through April 2005 in accordance with generally accepted government auditing standards.

GAO Contacts and Staff Acknowledgments

GAO Contacts

Dave A. Powner, (202) 512-9286
Keith A. Rhodes, (202) 512-6412
J. Paul Nicholas, (202) 512-4457

Staff Acknowledgments

Camille Chaires, West Coile, Jamey Collins, John Dale, Neil Doherty, Nancy Glover, Richard Hung, Hal Lewis, Harold Podell, David Plocher, and Eric Winter made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548