United States Government Accountability Office

GAO

Testimony

Before the House Committee on Government Reform

For Release on Delivery
Expected at 2 p.m. EDT
Wednesday, June 29, 2005

INTERNET PROTOCOL VERSION 6

Federal Agencies Need to Plan for Transition and Manage Security Risks

Statement of David A. Powner
Director, Information Technology Management Issues

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

GAO
Accountability * Integrity * Reliability

GAO

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-845T, a testimony before the House Committee on Government Reform

June 29, 2005

INTERNET PROTOCOL VERSION 6

Federal Agencies Need to Plan for Transition and Manage Security Risks

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 moves 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. The new protocol is gaining increased attention from regions with limited IP addresses.

For its testimony, GAO was asked to discuss the findings and recommendations of its recent study of IPv6 (GAO-05-471). In this study, 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 in the transition to IPv6.

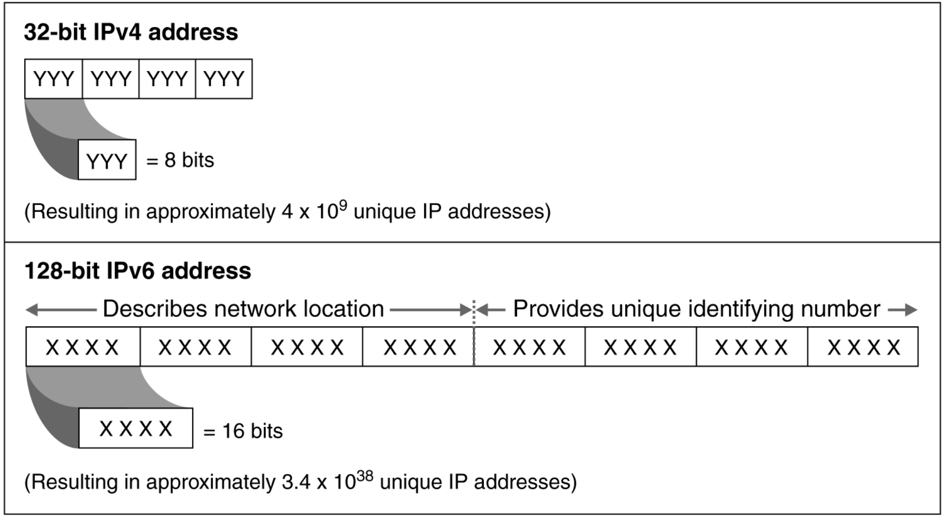
www.gao.gov/cgi-bin/getrpt?GAO-05-845T.

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 in IPv4 to approximately 3.4×10^{38} in IPv6 (see figure).

Figure: Comparison of IPv4 and IPv6 Address Space


32-bit IPv4 address
YYY
YYY
YYY
YYY
YYY
= 8 bits
(Resulting in approximately 4 x 10^9 unique IP addresses)
128-bit IPv6 address
Describes network location
Provides unique identifying number
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
= 16 bits
(Resulting in approximately 3.4 x 10^{38} unique IP addresses)

Source: GAO analysis.

Key planning considerations for federal agencies include recognizing that the transition is already under way, because agency networks already include IPv6-capable software and equipment. 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. Managing the security aspects of transition is also an important consideration because poorly managed IPv6 capabilities can put agency information and systems at risk.

DOD has made progress in developing a business case, policies, timelines, and processes for transitioning to IPv6. Unlike DOD, the majority of other major federal agencies reported that they have not yet initiated key planning efforts for IPv6.

In its report, GAO recommended, 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 the report.

Mr. Chairman and Members of the Committee:

Thank you for this opportunity to participate in the Committee's hearing on Internet protocol version 6 (IPv6). 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 define 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 is increasing interest in this new version of IP because its characteristics could allow for new products, services, and applications.

At your request, we performed a review and recently issued a report[2] that (1) described the key characteristics of IPv6; (2) identified the key planning considerations for federal agencies in transitioning to IPv6; and (3) determined the progress made by the Department of Defense (DOD) and other major federal agencies to transition to IPv6. This testimony summarizes the results of our recently issued report. All work related to this testimony was conducted in accordance with generally accepted government auditing standards.

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

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

[2] GAO, *Information Technology: Federal Agencies Need to Plan for Transition and Manage Security Risks*, GAO-05-471 (Washington, D.C.: May 20, 2005).

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 agency networks currently include IPv6-capable software and equipment. 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,[3] planning for system migration and security is 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 transition is another consideration, since IPv6 can introduce additional security risks to agency information. For example, attackers of federal networks could abuse features to allow unauthorized traffic or make agency computers directly accessible from the Internet.

Recognizing the importance of planning, the Department of Defense (DOD) has made progress in developing a business case, policies, timelines, and methods for transitioning to IPv6. These efforts

[3] GAO, *Business Systems Modernization: Internal Revenue Service Needs to Further Strengthen Program Management*, GAO-04-438T (Washington, D.C.: Feb. 12, 2004); *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); *DOD Business Systems Modernization: Longstanding Management and Oversight Weaknesses Continue to Put Investments at Risk*, GAO-03-553T (Washington, D.C.: Mar. 31, 2003).

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. We also identified the efforts undertaken by the other 23 Chief Financial Officer (CFO) Act agencies,[4] and 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 crosscutting 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 and security issues. In our report, we recommended, among other things, that the Director of the Office of Management and Budget (OMB) instruct agencies to begin addressing key planning considerations for 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 the report.

Background

The Internet is a worldwide network of networks made up of servers, routers, and backbone networks. To send a communication from one computer to another, a series of addresses is attached to information sent from the first computer to route the information to its final destination. The protocol that guides the administration of

[4] 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.

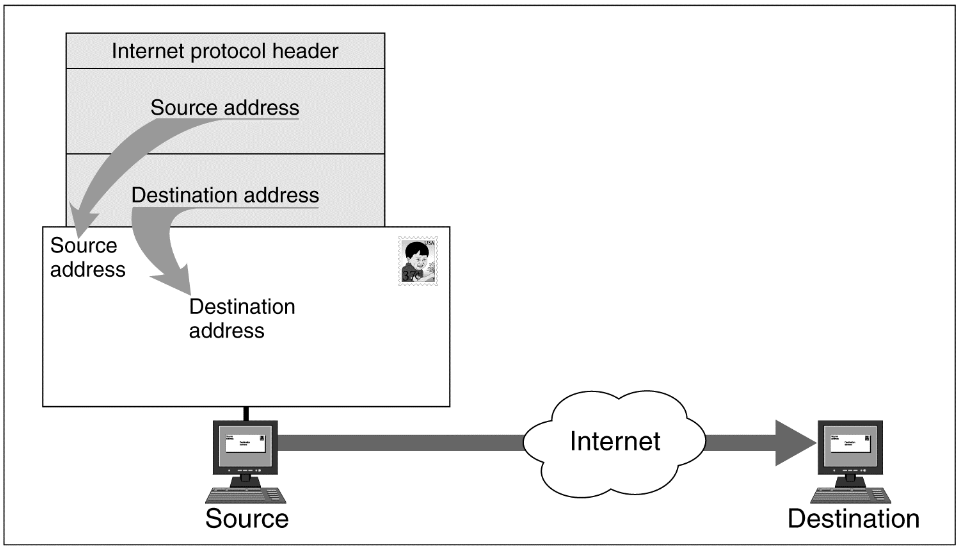
the routing addresses is the Internet protocol. The most widely deployed version of IP is version 4 (IPv4).

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.

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, 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 provides addresses for the sender and receiver. Similarly, if data are to be transmitted across the Internet from a source to a destination, IP addresses must be placed in an IP header. Figure 1 is 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 1: An Internet Protocol Header Contains IP Addresses for the Source and Destination of Information Transmitted across the Internet



Source: GAO analysis.

Limited IPv4 address space prompted organizations that need large numbers 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. In other words, to the outside world, all computers behind a device known as a network address translation router appear to have the same address. While this method 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.

Because of the limitations of IPv4, in 1994 the Internet Engineering Task Force (IETF)[5] began reviewing proposals for a successor to IPv4 that would increase IP address space and simplify routing. The IETF established a working group to be specifically responsible for developing the specifications and standardization of IPv6. Over the

[5] The 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.).

past 10 years, IPv6 has evolved into a mature standard. A complete list of the IPv6 documents can be found at the IETF Web site.[6]

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 deployments.

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 sectors. The government has helped to support the establishment of an IPv6 Promotion Council to facilitate issues related to development and deployment and is providing tax incentives to promote deployment. In addition, major Japanese corporations in the communications and consumer electronics sectors are also developing IPv6 networks and products. Further, the Chinese government has reportedly set aside approximately $170 million to develop an IPv6-capable infrastructure.

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 development and future perspectives. 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

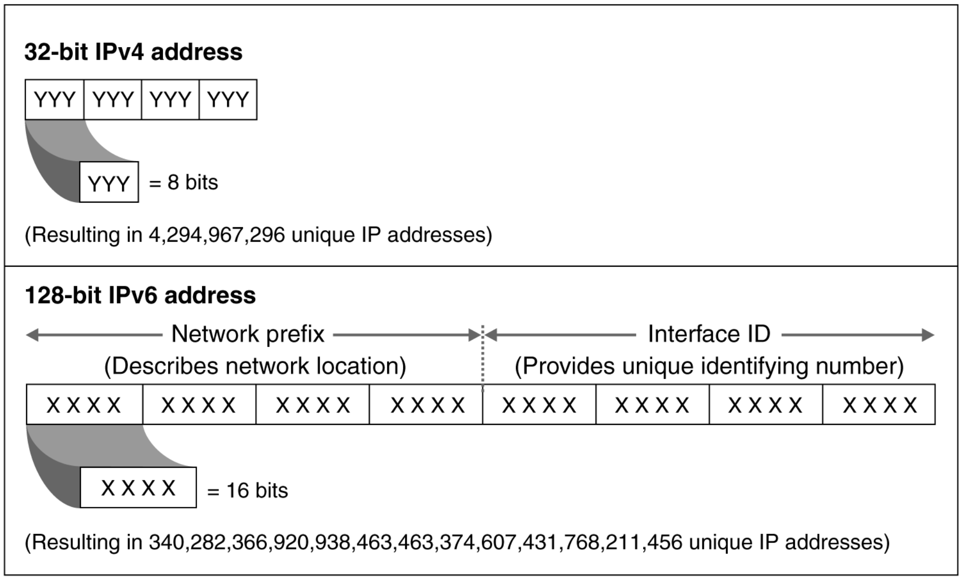
[6] The Web site for IETF is http://www.ietf.org/iesg/1rfc_index.txt

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.

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

The key characteristics of IPv6 are designed to increase address space, promote flexibility and functionality, and enhance security. For example, IPv6 dramatically increases the amount of IP address space available from the approximately 4.3 billion 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 this dramatic number of unique addresses a possibility. Figure 2 shows a comparison between the address spaces of IPv6 and IPv4.

Figure 2: Comparison of IPv6 and IPv4 Address Scheme


32-bit IPv4 address
YYY
YYY
YYY
YYY
YYY
= 8 bits
(Resulting in 4,294,967,296 unique IP addresses)
128-bit IPv6 address
Network prefix
(Describes network location)
Interface ID
(Provides unique identifying number)
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
= 16 bits
(Resulting in 340,282,366,920,938,463,463,374,607,431,768,211,456 unique IP addresses)

Source: GAO analysis.

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 other items such as cellular phones, consumer electronics, and automobiles.

In contrast to IPv4, 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 communications between devices with unique IP addresses and can better support the delivery of data-rich content such as voice and video.

In addition to the increased number of addresses, IPv6 improves the routing of data, provides mobility features for wireless, and eases automatic configuration capabilities for network administration, quality of service, and security. These characteristics are expected to enable advanced Internet communications and foster new software applications. While applications that fully exploit IPv6 are still in development, industry experts have identified various federal functions that might benefit from IPv6-enabled applications, such as border security, first responders, public health, and information sharing.

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

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, printers, and routers currently support IPv6. Therefore, it is important for agencies to note that the transition to IPv6 is different from a software upgrade because, when it is installed, its capability is also being integrated into the software and hardware.

Besides recognizing that an IPv6 transition is already under way, 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 the following:

- *Developing inventories and assessing risks*—An inventory of equipment (software and hardware) provides management with an understanding of the scope of an IPv6 transition and assists in focusing agency risk assessments. These assessments are essential steps in determining what controls are required to protect a network and what level of resources should be expended on controls.
- *Creating business cases for an IPv6 transition*—A business case usually identifies the organizational need for the system and provides a clear statement of the high-level system goals. 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. Furthermore, 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.
- *Determining the costs*—Cost benefit analyses and return-on-investment calculations can be used to justify investments. During the year 2000 (Y2K) technology challenge, the federal government amended the Federal Acquisition Regulation and mandated that all contracts for information technology include a clause requiring the delivered systems or service to be ready for the Y2K date change.[7] 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 federal agencies and ensure that federal applications are able to operate in an IPv6 environment without costly upgrades.

[7] 48 C.F.R. 39.106.

- *Identifying timelines and methods for the transition*—Timelines and process management can assist a federal agency in determining when to authorize its various component organizations to allow IPv6 traffic and features. Additionally, agencies can benefit from understanding the different types of transition methods or approaches that can allow them to use both IPv4 and IPv6 without causing significant interruptions in network services.

If Not Managed, IPv6 Features Can Be Abused

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 IPv6 features and found that, if firewalls and intrusion detection systems are not appropriately configured, IPv6 traffic may not be detected or controlled, leaving systems vulnerable to attacks by malicious hackers.

Further, in April 2005, the United States Computer Emergency Response Team (US-CERT), located at the Department of Homeland Security (DHS), issued an IPv6 cyber security alert to federal agencies based on our IPv6 test scenarios 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 that malicious users might be able to tunnel IPv6 traffic through these security devices undetected. Further, one feature of IPv6, known as automatic configuration (where a device that is IPv6 enabled will derive its own IP address from neighboring routers without an administrator's intervention), could allow devices to automatically configure themselves with an IPv6 address without authorization. US-CERT provided agencies with a series of short-term solutions including

- determining if firewalls and intrusion detection system products support IPv6 and implement additional IPv6 security measures and

- identifying IPv6 devices and disabling if not necessary.[8]

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

The Department of 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 facilitates DOD's goal of achieving network-centric operations by exploiting the key characteristics of IPv6, including

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

The department's efforts to develop policies, timelines, and methods for transitioning to IPv6 are progressing. 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. The Transition Office is in the early stages of its work and has developed a set of 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.

In parallel with the Transition Office's efforts, the Office of the DOD Chief Information Officer has created an IPv6 transition plan. The

[8] http://www.us-cert.gov/federal/archive/infoNotices/FIN05-095.html (April 5, 2005).

Chief Information Officer has responsibility for ensuring a coherent and timely transition and for establishing and maintaining the overall departmental transition plan, and is the final approval authority for any IPv6 transition waivers.

Although DOD has made substantial progress in developing a planning framework for transitioning to IPv6, the department still faces several challenges, including developing a full inventory of IPv6-capable software and hardware, finalizing its IPv6 systems engineering management plan, monitoring its operational networks for unauthorized IPv6 traffic, and developing a comprehensive enforcement strategy, including using its existing budgetary and acquisition review process.

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 to our survey, 4 agencies reported having established a date or goal for transitioning to IPv6. The majority of agencies have not addressed key planning considerations. For example,

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

Agency responses demonstrate that few efforts outside 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.

Recommendations for Addressing Federal IPv6 Challenges

To address the challenges IPv6 presents to federal networks, in our report we recommended that federal agencies begin addressing key IPv6 planning considerations. Specifically, we recommended that the Director of OMB instruct agencies to begin developing inventories and assessing risks, creating business cases for the IPv6 transition, establishing policies and enforcement mechanisms, determining the costs, and identifying timelines and methods for transition, as appropriate. To help ensure that IPv6 would not result in unexpected costs for the federal agencies, we recommended that the Director consider amending 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. Finally, because poorly configured and unmanaged IPv6 capabilities present immediate risks to federal agency networks, we recommended that agency heads take immediate action to address the near-term security risks. Such actions could include determining what IPv6 capabilities they may have and initiating steps to ensure that they can control and monitor IPv6 traffic to prevent unauthorized access.

In summary, transitioning to IPv6 is a pervasive, crosscutting challenge for federal agencies that could result in significant benefits to agency services and operations. But such benefits may be diminished if action is not taken to ensure that agencies are addressing the attendant challenges, including addressing key planning considerations and acting to ensure the security of agency information and networks. If agencies do not address these key planning issues and do not 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.

Mr. Chairman, this completes our prepared statement. We would be happy to respond to any questions you or other Members of the Committee may have at this time.

Contacts and Staff Acknowledgments

For further information, please contact David Powner at (202)-512-9286 or Keith Rhodes at (202)-512-6412. We can also be reached by e-mail at pownerd@gao.gov and rhodesk@gao.gov respectively.

Key contributors to this testimony were Scott Borre, Lon Chin, West Coile, Camille Chaires, John Dale, Neil Doherty, Nancy Glover, Richard Hung, Hal Lewis, George Kovachick, J. Paul Nicholas, Christopher Owens, Eric Trout, and Eric Winter.

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