United States Government Accountability Office

GAO

Report to the Chairman, Committee on Government Reform, House of Representatives

June 2006

# INTERNET PROTOCOL VERSION 6

# Federal Government in Early Stages of Transition and Key Challenges Remain


GAO-06-675

June 2006

# INTERNET PROTOCOL VERSION 6

# Federal Government in Early Stages of Transition and Key Challenges Remain

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-675, a report to the Chairman, Committee on Government Reform, House of Representatives

## Why GAO Did This Study

The Internet protocol (IP) provides the addressing mechanism that defines how and where information such as text, voice, music, and video move across interconnected networks. IP 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, Internet version 6 (IPv6) was developed to increase the amount of available address space. In August 2005, the Office of Management and Budget (OMB) issued a memorandum specifying activities and time frames for federal agencies to transition to IPv6. GAO was asked to determine (1) the status of federal agencies' efforts to transition to IPv6; (2) what emerging applications are being planned or implemented that take advantage of IPv6 features; and (3) key challenges industry and government agencies face as they transition to the new protocol.

## What GAO Recommends

GAO recommends that federal agencies work through two of the groups that play key roles in transitioning the federal government to IPv6 to address key challenges they face as they proceed with the transition. In oral comments on a draft of this report, OMB generally agreed with the results and described actions being taken to address GAO's recommendation.

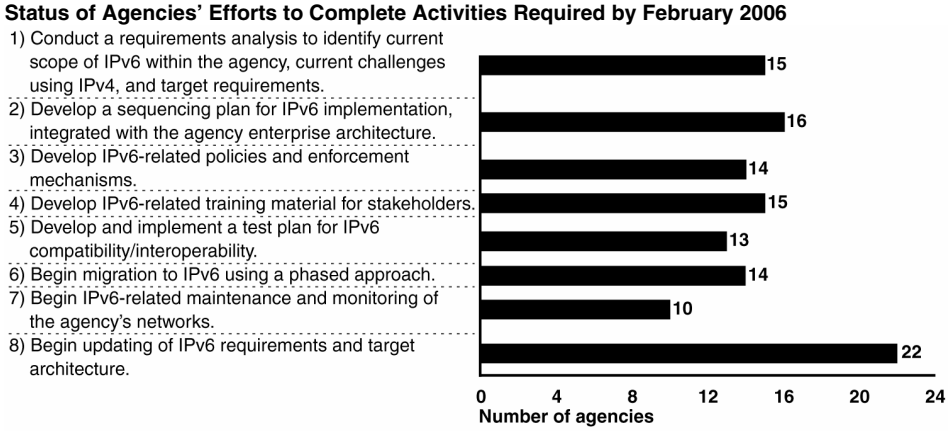
www.gao.gov/cgi-bin/getrpt?GAO-06-675.

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

## What GAO Found

Federal agencies have taken steps in planning for the transition to IPv6, but several have not completed key activities. For example, almost all of the 24 major agencies have assigned an official to lead and coordinate the IPv6 transition. However, ten agencies had not developed IPv6-related policies and enforcement mechanisms. (See figure for the status as of April 2006 of agencies' efforts in meeting OMB required activities.) Until agencies complete key activities, their transition planning efforts risk not being successful. To help address this risk, agencies are required to report their progress in completing key planning activities to OMB.

**Status of Agencies' Efforts to Complete Activities Required by February 2006**




Source: GAO analysis of agency data.

Applications that take advantage of IPv6 features are being planned or implemented both within and outside of the federal government, including applications to support emergency response, enhance warfighting capabilities, and facilitate continuity of operations planning. However, these applications are few, in large part because organizations are still in the early stages of the transition or because they lack incentives to use the new protocol.

Transitioning to IPv6 presents several challenges. Significant challenges include managing information security in an environment that is more vulnerable to threats; incorporating IPv6 features into applications' business cases to identify new and better ways of meeting mission goals; and interfacing with partners that may be in various stages of the transition. Other challenges include maintaining dual IPv4 and IPv6 environments for an extended period of time and implementing standards required by the use of the new protocol. All of these challenges could impede progress if they are not addressed by agencies as they proceed with the transition.

# Contents

## Abbreviations

| | |
|---|---|
| CIO | chief information officer |
| DOD | Department of Defense |
| 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 |

GAO
Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

June 30, 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

The Internet protocol (IP) defines how and where information such as text, voice, music, 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 devices that are using the Internet. As a result, IP version 6 (IPv6) was developed to allow millions more users by increasing the amount of available IP address space.

In May 2005, we reported on the key characteristics of IPv6 and identified important planning considerations for federal agencies in transitioning to IPv6.[1] The Office of Management and Budget (OMB) subsequently specified activities and milestones for federal agencies to follow to transition their network backbones to IPv6 by June 2008.

As agreed with your office, our objectives were to determine (1) the status of federal agencies' efforts to transition to IPv6; (2) what emerging applications are being planned or implemented that take advantage of IPv6 features; and (3) key challenges industry and government agencies face as they transition to the new protocol.

To conduct our work, we distributed a structured data collection instrument to the 24 major agencies[2] to determine their efforts in

[1]GAO, *Internet Protocol Version 6*: *Federal Agencies Need to Plan for Transition and Manage Security Risks*, GAO-05-471 (Washington, D.C.: May 2005).

[2]The 24 major 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; and 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.

completing key transition activities. We also obtained and reviewed supporting documentation, including agencies' IPv6 transition plans, to validate their responses. To identify emerging applications that are being planned and challenges organizations are facing in the transition, we researched and analyzed technical documents, reviewed relevant publications, and interviewed IPv6 experts in government and industry. We performed our work from August 2005 through May 2006 in accordance with generally accepted government auditing standards. Details of our objectives, scope, and methodology are included in appendix I.

## Results in Brief

Federal agencies have taken steps to plan for the transition to IPv6, but several agencies have not completed key activities. For example, as of April 2006, almost all of the 24 major agencies have assigned an official to lead and coordinate the IPv6 transition. However, ten agencies had not developed IPv6-related policies and enforcement mechanisms. Until agencies complete key planning activities, their transition efforts risk not being successful. To help address this, agencies are required to report to OMB their status in completing these.

Applications that take advantage of IPv6 features are being planned or implemented both within and outside of the federal government, including applications to support emergency response, enhance warfighting capabilities, and facilitate continuity of operations planning. However, these applications are few, in large part because organizations are still in the early stages of the transition or because they lack incentives to use the new protocol.

Transitioning to IPv6 presents several challenges. Significant ones include managing information security in an environment that is more vulnerable to threats; incorporating IPv6 features into applications' business cases to identify new and better ways of meeting mission goals; and interfacing with partners that may be in various stages of the transition. Other challenges include maintaining dual IPv4 and IPv6 environments for an extended period of time and implementing standards required by the use of the new protocol. All of these challenges could impede progress in transitioning to IPv6 if agencies do not address them as they proceed with the transition.

To strengthen agencies' IPv6 transition planning efforts, we recommend that the Director of OMB direct federal agencies to work through the CIO Council Architecture and Infrastructure Committee and the IPv6 Working

Group, two of the groups that play key roles in transitioning the federal government to IPv6, to address key challenges that they face as they proceed with the transition.

Representatives of OMB's Office of Information and Regulatory Affairs and Office of the General Counsel provided oral comments on a draft of this report. In these comments, OMB generally agreed with the report results and described actions being taken to address our recommendation. Specifically, they stated that IPv6 Working Group subcommittees were established in May 2006 to begin addressing challenges including security, testing, and standards, and that agencies were working with these subcommittees to find solutions to the challenges. OMB also provided technical corrections, which we incorporated as appropriate.

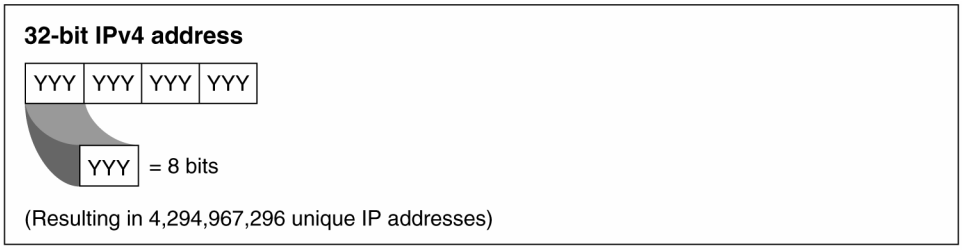
# Background

Since the early 1990s, increasing computer interconnectivity—most notably in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. A key factor in the growth of the Internet has been the protocols—such as the Internet protocol—that enable the transmission of information across a global network of networks. Currently, the most widely used version of IP is version 4 (IPv4).

## Internet Protocol Aids in the Transmission of Information across the Internet

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. The current IP version most widely used is IPv4, which uses a 32-bit address format and provides approximately 4.3 billion unique IP addresses. Figure 1 provides a conceptual illustration of an IPv4 address.

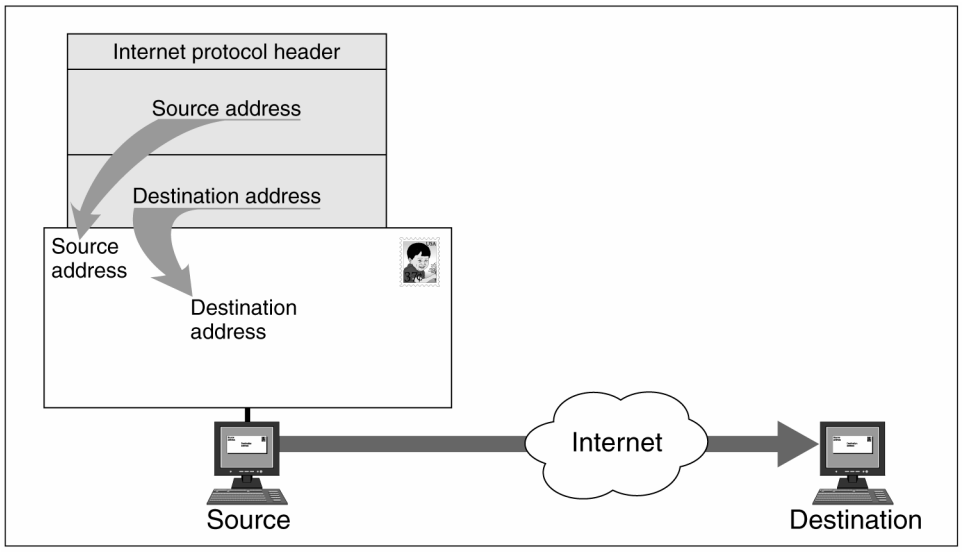
**Figure 1: Internet Protocol Version 4 Address**




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 limited address space in IPv4 prompted organizations that need large amounts of IP addresses to implement technical solutions to compensate. In 1994, the Internet Engineering Task Force (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.

## Key Characteristics of IPv6 Increase Address Space and Improve Functionality

The key characteristics of IPv6 include

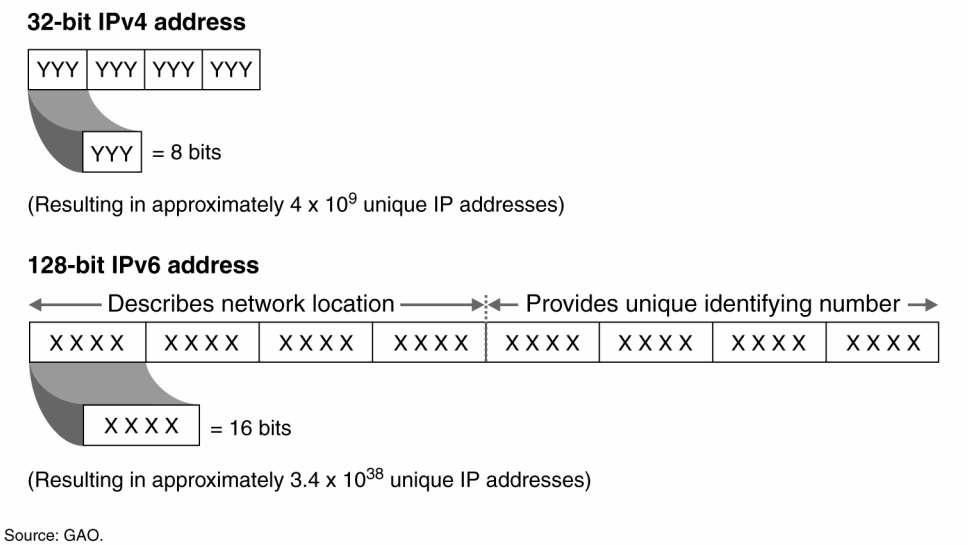
- a dramatic increase in IP address space,
- a simplified IP header for flexibility and functionality,
- improved routing of data,
- enhanced mobility features,
- easier configuration capabilities,
- improved quality of service, and
- integrated Internet protocol security.

These key characteristics of IPv6 offer various enhancements relative to IPv4 and are expected to increase Internet services and enable advanced 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 $3.4 \times 10^{38}$. 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 3 shows the difference between the length of an IPv4 address and that of an IPv6 address.

**Figure 3: Comparison of IPv4 and IPv6 Address Schema**




Source: GAO.

## Simplified Header Intended to Promote Flexibility and Functionality

The IP header contains information such as the source and destination addressee, used to transmit data across the Internet. 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. 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.

## 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 previously mentioned, 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 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.

## Previous GAO Work Noted Little Progress in Planning to Transition to IPv6

In May 2005, we reported that, with the exception of DOD, the majority of the 24 major federal agencies reported that they had not yet initiated key planning efforts for IPv6.[3] Among other things,

- 21 agencies reported not having plans for transitioning their infrastructure and applications to IPv6,
- 19 agencies reported not having inventoried their IPv6-capable equipment, and
- 22 agencies reported not having estimated costs for the transition.

Although agencies had done little to prepare for the transition to IPv6, the transition was already under way for many federal agencies because their networks already contained IPv6-capable software and equipment. Introducing this equipment into an organization allows the organization to have the capability to carry IPv6 traffic. Therefore, we recommended that the Director of OMB instruct federal agencies to acknowledge that a key step in addressing planning and security challenges includes the recognition that IPv6-capable software and equipment exists in agency networks and that agencies follow this five-step process to guide their IPv6 planning and transitioning:

[3]GAO-05-471.

1. develop inventories and assess risks,
2. create business cases for an IPv6 transition,
3. establish policies and enforcement mechanisms,
4. determine the costs, and
5. identify timelines and methods for the transition.

We further recommended that agencies take immediate action to ensure that their systems were not compromised as a result of not effectively recognizing and managing IPv6-capable software and hardware.

## OMB Specifies Activities, Deadlines for IPv6 Transition

Following the issuance of our May 2005 report on IPv6, OMB issued a memorandum[4] to federal chief information officers (CIO) specifying a series of activities and associated deadlines for federal agencies to configure their infrastructure (network backbones) to carry IPv6 traffic by June 2008. For example, the memorandum required agencies to assign an official to lead and coordinate IPv6 transition planning efforts; conduct an inventory of existing routers, switches, and hardware firewalls; and begin an analysis of fiscal and operational impacts and risks of transitioning to IPv6 by November 15, 2005. The development of policies and enforcement mechanisms, training material, and the initiation of activities including maintaining and monitoring agency networks were to be documented in a transition plan. This transition plan was to be associated with the agencies' enterprise architecture and submitted to OMB by February 2006. The impact analysis and inventory started in November are to be completed by June 30, 2006. Table 1 lists the transition activities and deadlines defined in the OMB memorandum.

[4]OMB, *Memorandum for Chief Information Officers: Transition Planning for Internet Protocol Version 6 (IPv6)*, M-05-22 (August 2005).

**Table 1: IPv6 Transition Activities Defined by OMB**

| Activity |
|---|
| **Activities due by November 15, 2005** |
| (1) Assign an official to lead and coordinate IPv6 transition planning. |
| (2) Complete an inventory of existing routers, switches, and hardware firewalls. |
| (3) Begin an inventory of all other existing IP-compliant devices and technologies not captured in the first inventory. |
| (4) Begin an impact analysis to determine fiscal and operational impacts and risks of transitioning to IPv6. |
| **Activities to be addressed by February 2006[a]** |
| (5) Conduct a requirements analysis to identify current scope of IPv6 within the agency, current challenges using IPv4, and target requirements. |
| (6) Develop a sequencing plan for IPv6 implementation, integrated with the agency's enterprise architecture. |
| (7) Develop IPv6-related policies and enforcement mechanisms. |
| (8) Develop IPv6-related training material for stakeholders. |
| (9) Develop and implement a test plan for IPv6 compatibility/interoperability. |
| (10) Begin migration to IPv6 using a phased approach. |
| (11) Begin IPv6-related maintenance and monitoring of the agency's networks. |
| (12) Begin updating IPv6 requirements and target architecture. |
| **Activities due by June 30, 2006** |
| (13) Complete an inventory of existing IP-compliant devices and technologies not captured in the first inventory. |
| (14) Complete impact analysis of fiscal and operational risks. |
| **Activities due by June 2008** |
| (15) All agency infrastructures (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. Agencies will include progress reports on meeting this target date as part of their enterprise architecture transition strategy. |

Source: OMB.

[a]OMB asked agencies to address these actions to the extent they could in a transition plan that was due to OMB by February 2006.

Collectively, the activities specified in the memorandum address four of the five planning steps we recommended agencies take to prepare for the IPv6 transition: developing inventories and assessing risks, establishing policies and enforcement mechanisms, determining transition costs, and identifying timelines and methods for the transition. The transition costs are to be identified in the impact analysis agencies were to start working on in November 2005.

Federal agencies are to report their progress in completing the required activities to OMB. Specifically, according to the *IPv6 Transition Guidance* document issued by the CIO Council Architecture and Infrastructure Committee[5] in February 2006, agencies were to submit to OMB a progress report containing the following:

- status of the second IP devices and technologies inventory;
- status of the IPv6 impact analysis;
- overall agency progress toward an IPv6 transition;
- interim milestones and dates for each of the deadlines specified by OMB; and
- challenges, issues, or risks agencies are facing with completion of the second inventory, impact analysis, or other aspects of the agency's transition to IPv6.

Following this initial submission, agencies are to submit quarterly IPv6 status reports to OMB showing progress against previously established milestones and updated transition plans.

In addition to establishing milestones for the IPv6 transition, OMB has tasked the CIO Council's Architecture and Infrastructure Committee with establishing IPv6 transition guidance for all federal agencies. As noted above, the Committee recently issued this guidance.[6] The Committee is to disseminate the guidance it issues and other information to agencies through the agency leads and the Council's Web site. OMB also established the IPv6 Working Group, which is comprised of the IPv6 lead personnel for all federal agencies as well as subject matter experts. The IPv6 Working Group meets to share lessons learned and provide seminars on functional areas relevant to the federal government transition, including standards, testing, and training.

[5]Federal CIO Council Architecture and Infrastructure Committee, *IPv6 Transition Guidance, version 1.0.* The document was issued in draft form in February 2006 and released in final form in May 2006.

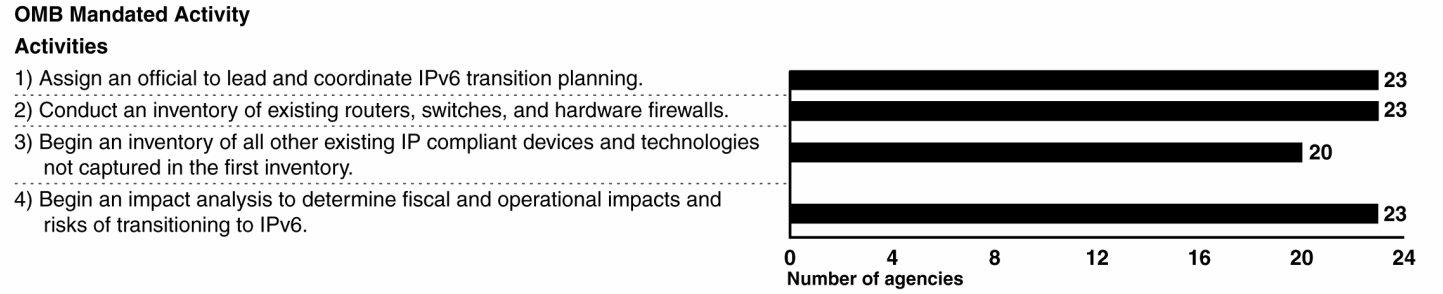
[6]A representative from OMB's Office of Information and Regulatory Affairs noted that additional guidance will be issued as deemed necessary.

## Federal Agencies Are in the Early Stages of Transitioning to IPv6

Federal agencies have taken steps to plan for the transition to IPv6, but several have not completed key planning activities by February 2006 as required by the OMB memorandum. Until agencies complete key planning activities, their transition planning efforts risk not being successful.

In response to OMB's memorandum, federal agencies have taken steps to plan for the transition to IPv6. Specifically, almost all of the 24 major agencies have assigned an official to lead and coordinate the IPv6 transition, have conducted an inventory of all routers and switches and hardware firewalls, and have begun a financial and operational impact analysis, in accordance with the requirements of the OMB memorandum. Figure 4 depicts the agencies' status as of April 2006 with completion of the OMB activities that were due by November 15, 2005.

**Figure 4: Status of Agencies' Efforts to Address Activities Required by November 15, 2005**




Source: GAO analysis of agency data.

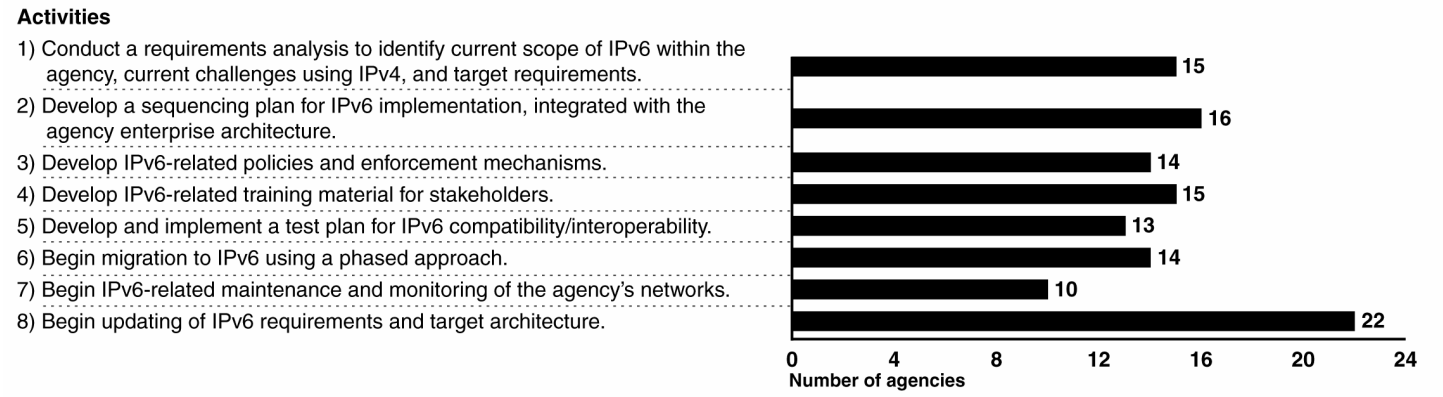
Much remains to be accomplished before agencies will have completed key planning activities. Specifically, as of February, only 9 of the 23 agencies that reported having begun an impact analysis had developed preliminary costs for the transition as required as part of this analysis. These costs ranged from $960,000 to more than $20 million. Agencies stated a variety of reasons for not being able to develop preliminary costs at this stage in the transition, including the many unknowns of the transition, the need to first complete a business case and a requirements analysis before a cost estimate was developed, and finally, the anticipation that the funding for the IPv6 transition would be accomplished using the existing agency budget. Nevertheless, until agencies can determine all costs associated with the transition as we previously recommended, they may not be able to adequately budget, among other things, for the infrastructure and application upgrades, training, and operation of multiple IP environments that are associated with IPv6 transition efforts.

In addition, as of April 2006, at least one-third of the 24 major agencies had not completed 7 of the 8 activities that OMB required to be completed by February. For example,

- 9 agencies did not conduct a requirements analysis to identify the current scope of IPv6 within their agencies, current challenges using IPv4, and target requirements;
- 10 agencies did not develop IPv6 policies and enforcement mechanisms, which, as previously noted, we also recommended in our prior IPv6 report;[7] and
- 14 agencies did not begin IPv6-related maintenance and monitoring of their networks.

Figure 5 depicts the agencies' status as of April 2006.

**Figure 5: Status of Agencies' Efforts to Address Activities Required by February 2006**




Source: GAO analysis of agency data.

In accordance with the OMB memorandum, agencies are to complete two other activities by June 30, 2006: agencies are to complete an inventory of existing IP-compliant devices and technology not captured in the first inventory that was due in November 2005 and complete an impact analysis of fiscal and operational risks. According to the 24 major agencies, as of

[7]GAO-05-471.

April, all have begun their inventories and all but one has begun to conduct an impact analysis.

Until agencies complete key planning activities, their transition efforts risk not being successful. To help address this, as previously noted, agencies are required to report their progress quarterly to OMB.

## Applications Taking Advantage of IPv6 Features Are Being Planned and Implemented, but They Are Few

Applications that take advantage of IPv6 features are being planned or implemented both within and outside of the federal government, including applications to support emergency response and warfighting capabilities.[8] However, these applications are few largely because organizations are still in the early stages of the transition or because they lack incentives to use the new protocol.

### Applications within the Federal Government

Within the federal government, the Department of Defense (DOD) has begun to develop applications that use IPv6 features to enhance warfighting capabilities.[9] The new protocol is 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.

[8]We are using the term "application" to refer to software that runs on the IPv6 infrastructure. We are not including systems software such as operating systems and other software used to manage computer networks.

[9]DOD has been planning these applications since 2003.

The increased address space of IPv6 will provide DOD with an opportunity to reconstitute its address space architecture to better respond to the future proliferation of numerous unmanned sensors and mobile assets. For example, 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 maintaining detailed information on military vehicles and individual soldiers in real time.

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, DOD 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, DOD is developing applications that take advantage of IPv6's improved quality of service features to enhance many of its other initiatives, such as voice over IP, which is the transmission of voice data over an IP-based network instead of the traditional transmission over a general purpose circuit-switched network.

Beyond DOD, applications that other agencies have begun to consider that use IPv6 features include

- hand-held devices that take advantage of IPv6's mobility feature to expedite the delivery of real time data gathered during field surveys and questionnaires, on-site investigations of industry and the work of revenue officers, security officers, auditors, and inspectors;
- the use of the IPv6 auto-configuration feature to enhance continuity of operations planning and to improve technology response time;
- the use of the end-to-end security feature of IPv6 to build more secure retail and wholesale transactions, including securities and commemoratives; and
- the use of IPv6's collective characteristics to improve existing network management schemas and reduce IT infrastructure costs.

## Applications Outside the Federal Government

Through research and interviews with experts, we identified applications that are being planned or developed outside the federal government. They include the following:

- One broadband/cable provider is currently planning to migrate to IPv6 by 2008 to use the increased address space for better management of its cable equipment.

- The telecommunications industry is working on improving customer services by developing the next generation network. This is a new network model that is based on the extensive use of Internet protocols—particularly IPv6—to accommodate the diversity of applications inherent in emerging broadband technologies. The next generation network is characterized, among other things, by a shared core network for all access and service types, packet-based transport technologies, open standardized interfaces among the different network layers (transport, control, and services), support for user-adaptable interfaces, and variable access network capacity and type. This means that a single infrastructure would be used to support multiple services and that users would be able to access these services—Web pages, e-mail, movies, or a video conference—from one mobile device.

- The North American and California IPv6 Task Forces are making plans to develop a metropolitan network in Sacramento, California, called MetroNet6 using IPv6 to enhance first responder technologies. MetroNet6 is an effort to use voice, video, graphics, intelligence, medical, and other forms of data through multimedia communications for first responders. MetroNet6 would be connected over the Internet to the Department of Homeland Security for communications updates.

- The Japanese government reported making progress in implementing several IPv6 applications to improve existing operations. According to the Japanese IPv6 Promotion Council, Japan plans to have almost all of its telecommunications run on IPv6 to support applications that would improve telephone, cable, and facility management (e.g., security and electricity) services. For example, the use of an IPv6 infrastructure for facility management would support applications that minimize energy use in industrial buildings.

## Few Applications Are Being Planned and Implemented

While applications that take advantage of IPv6 features exist, they are few. Specifically, as of February 2006, of the 24 major agencies, only DOD reported that it was developing IPv6 applications; 4 agencies stated they were considering applications; and none reported having implemented any.[10] Several federal agencies reported that, because they are in the early stages of transitioning to IPv6, they have not yet considered how IPv6 applications could be used to improve their ability to meet their missions. They added that they will begin thinking of this once they have a better understanding of the benefits they can derive from using the protocol. Our review of technical publications and interviews with IPv6 experts did not identify many IPv6 applications, either. According to these sources, this is in large part because organizations outside the federal government currently have little incentive to transition their infrastructures and thereby implement applications to take advantage of IPv6.

# Several Challenges Exist for Industry, Government Agencies during the IPv6 Transition

Transitioning to IPv6 presents several challenges. Significant challenges include managing information security in an environment that is more vulnerable to threats; incorporating IPv6 features in application business cases to identify new and better ways of meeting mission goals; and interfacing with partners that may be in various stages of the transition. Other challenges include maintaining dual IPv4 and IPv6 environments for an extended period of time and implementing standards required by the use of the new protocol. All of these challenges could impede progress if they are not addressed by agencies as they proceed with the transition.

## Managing Information Security

Federal agencies are required by law to take a risk-based approach to managing information security.[11] Further, OMB guidance requires agencies to indicate whether their security policies include special procedures for using emerging technologies including IPv6.[12] Nevertheless, for federal agencies, as well as for other organizations, managing the information

[10]These numbers reflect February 2006 responses to our information request to the 24 major agencies. When we met with OMB staff at the end of our review, they indicated that a few more agencies were considering applications as a result of developing a better understanding of the key characteristics of the new protocol.

[11]*Federal Information Security Management Act*, *Title III*, *E-Government Act of 2002*, Pub. L. 107-347 (Dec. 17, 2002).

[12]OMB, *Memorandum for the Heads of Departments and Agencies: FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-05-15 (June 2005).

security risks of IPv6 is a difficult challenge to address for the following reasons:

- *Using IPv6 features during transition could make agencies more vulnerable to security threats.* We previously reported that, 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 it is not enabled by default, it is easy for administrators to enable either intentionally or as an unintentional by-product of running a program. We previously reported on our tests of two IPv6 features—automatic configuration and tunneling—and determined that, if not properly managed, they could present serious risks to federal agencies.[13] Accordingly, we recommended that agency heads take immediate actions to manage 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.

- *Many of the current security tools are not mature enough to protect against breaches in IPv6 security.* A recent federal plan on cyber security research concluded that the immaturity of current security tools (e.g., firewall software and intrusion detection systems) results in high levels of risk for breaches of security with IPv6.[14] The report noted that not enough research has been done yet to provide a full suite of security tools and support to make IPv6 as secure as IPv4 and to fully assess the security implications of widespread IPv6 implementation. Taking the immaturity of current security tools into consideration will be critical to ensuring organizations' networks are adequately secure.

- *Adopting end-to-end security-based models will become critical whereas perimeter-based approaches were previously more widely used.* End-to-end based networking models lend themselves better to the implementation of IPv6 features and mobile technologies such as IP phones than the perimeter-based approaches that are more widely used. This presents a challenge in that many organizations will need to rethink the way they currently secure their networks. According to the Department of Commerce, most enterprises currently implement security measures at the perimeter of their corporate networks using firewalls,

[13]GAO-05-471.

[14]Interagency Working Group on Cyber Security and Information Assurance, *Federal Plan for Cyber Security and Information Assurance Research and Development* (Washington, D.C.: April 2006).

etc.[15] This perimeter approach to protect a network means there are very few devices on an enterprise's network that are connected directly to the Internet. Most devices are connected to a central location where IP traffic travels through firewalls and intrusion detection systems. However, with the transition to IPv6 and the proliferation of laptop computers, personal directory assistants, and IP phones, more and more devices will be connected directly to each other without traveling through the enterprise perimeter firewall and securing this new topology will require a lot of effort.

## Incorporating IPv6 Features into Application Business Cases

Incorporating IPv6 features into application business cases can be challenging because, as discussed earlier, there are currently few IPv6 applications available and, therefore, it is difficult for agencies to envision how IPv6 features could help them achieve their missions more efficiently or effectively. In addition, it may be very difficult for people in organizations who have been performing functions for a long time to think of how the protocol could be used to perform those functions in new ways. Further, the business executives who should be involved in determining how to incorporate IPv6 into their applications' business cases may be reluctant to commit their time to doing this if they do not see any immediate business benefit. Nevertheless, incorporating IPv6 features into applications' business cases as appropriate, as we have previously recommended, is important because it could serve to maximize the benefits of transitioning to IPv6.

## Interfacing with External Partners during the Transition Period

Interfacing with external partners during the transition can be challenging in that a great level of coordination and testing among all players involved needs to occur to ensure that problems—for example, connection delays and network insecurity—are minimized. In addition, benefits that cannot be realized until all parties are communicating using IPv6 can be difficult to attain because external partners can be in various stages of transitioning to IPv6. While operating in dual-stack mode is expected to alleviate problems with interfacing, coordinating transition plans with external partners and running appropriate tests is critical to helping identify and resolve issues and ensure that key benefits are realized.

[15]U.S. Department of Commerce, *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)* (Washington, D.C.: January 2006).

## Other Challenges

Other challenges industry and government agencies face as they transition include the following:

- Dual IPv4 and IPv6 environments will be maintained for an extended period of time. Maintaining two network protocols is challenging in that it adds complexity to network maintenance and associated costs are higher. In addition, it requires skilled personnel. Further, it may be difficult to maintain hardware and software interoperability across dual environments.

- Multi-homing using IPv6 will be a challenge. Multi-homing occurs when a host is assigned an IP address from more than one Internet service provider providing the host with more than one IP address. Multi-homing gives an organization greater reliability because, if one provider stops working, it can rely on the other provider. However, the method used to implement multi-homing in an IPv4 environment creates routing issues in an IPv6 environment. Various proposals are being explored to address this challenge including a new standard developed by the Internet Engineering Task Force.

- Implementing the new IPv6 standards will be a challenge because (1) IPv6 standards are less mature than IPv4 standards and (2) some IPv6 standards are still evolving.

  Because IPv6 standards are less mature than IPv4 standards, different vendors may interpret and implement the standards in a slightly different way and this could lead to interoperability problems. In a recent report, the Alliance for Telecommunications Industry Solutions stated that certain tests (known as conformance tests) can measure how vendors' products conform to various standards, but they also noted that these tests rarely measure every nuance of a protocol.[16]

  With IPv6 standards evolving, it is important for organizations to ensure that the IPv6 capabilities they are implementing can be upgraded to incorporate newer standards. OMB acknowledged this challenge in its IPv6 Transition Guidance and asked that agencies consider these challenges in developing their transition plans.

[16]Alliance for Telecommunications Industry Solutions, *Internet Protocol Version 6 Report and Recommendation* (Washington, D.C.: May 2006).

## Conclusions

Federal agencies have taken steps to transition to IPv6, but several have not completed key activities, including determining transition costs as part of their impact analysis and developing IPv6-related policies and enforcement mechanisms. By missing deadlines for completing key activities, agencies risk jeopardizing their ability to successfully transition their infrastructures to IPv6 by the June 2008 target specified by OMB. OMB has the means to stay abreast of the status of agencies' efforts through quarterly progress reviews these agencies are required to submit.

Applications are being planned or implemented to take advantage of IPv6 both within and outside the federal government. However, they are few, in large part because organizations are either too early in their transition efforts to begin considering them or they currently lack the incentive to do so. Nevertheless, with its key characteristics, IPv6 holds much promise for organizations as they better understand how they can take advantage of the new protocol.

Transitioning to IPv6 presents several challenges to industry and government agencies. Some of the more significant challenges include managing information security in an environment that is vulnerable to threats, incorporating IPv6 features into applications' business cases to identify new and better ways of meeting mission goals, and interfacing with partners that are in various stages of the transition. Others include maintaining dual IPv4 and IPv6 environments for an extended period of time and implementing standards required by the use of the new protocol. All of these challenges could impede progress if they are not addressed by agencies as they proceed with the transition.

## Recommendation for Executive Action

To strengthen agencies' IPv6 transition planning efforts, we recommend that the Director of OMB direct federal agencies to work through the CIO Council Architecture and Infrastructure Committee and the IPv6 Working Group to address challenges agencies face such as interfacing with external partners during the transition period as they proceed with the transition.

We have previously made recommendations that agencies take action to address security risks, determine transition costs, and develop business cases. We are, therefore, not making new recommendations on these issues in this report.

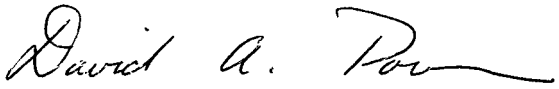
## Agency Comments and Our Evaluation

Representatives of OMB's Office of Information and Regulatory Affairs and Office of the General Counsel provided oral comments on a draft of this report. In these comments, OMB generally agreed with the report results and described actions being taken to address our recommendation. Specifically, they stated that IPv6 Working Group subcommittees were established in May 2006 to begin addressing challenges including security, testing, and standards, and that agencies were working with these committees to find solutions to the challenges. OMB also provided technical corrections, which we incorporated in the report as appropriate.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this letter. At that time, we will send copies to interested congressional committees and to the Director, Office of Management and Budget. 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; or Keith Rhodes at (202) 512-6412, or rhodesk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are listed in appendix II.

Sincerely yours,



David A. Powner, Director,
Information Technology Management Issues

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

# Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to determine (1) the status of federal agencies' efforts to transition to IPv6; (2) what emerging applications are being planned or implemented that take advantage of IPv6 features; and (3) key challenges industry and government agencies face as they transition to the new protocol.

To address our first objective, we distributed an information request to the 24 major agencies in January 2006 to inquire about their status in meeting key planning activities, including those outlined in our prior report and those laid out in the OMB memorandum. All 24 agencies responded to our information request. Throughout our engagement, we followed up with additional requests for information to stay abreast of agencies' progress in completing key planning activities and requested supporting documentation, as appropriate, to validate agencies' responses. To obtain an updated status of activities required by February, we requested and reviewed the transition plans in which these activities were to be documented. We obtained transition plans from 21 agencies. We followed up with agency officials to confirm the results of our analysis and obtained responses from 15 of the 24 agencies. One agency neither responded to our request to update the status of activities required by February nor provided us with a transition plan documenting these activities. We therefore assumed the agency had not performed the activities.

To address our second and third objectives, we used the January 2006 information request mentioned above to determine whether any emerging applications were being planned or implemented by federal agencies and to understand the challenges these agencies face in the transition to IPv6. To learn more about federal agencies' and industry applications and challenges in transitioning to IPv6, we also researched and analyzed technical documents including Juniper's *The IPv6 Best Practices World Report Series*, the CIO Council's Architecture and Infrastructure Committee's *IPv6 Transition Guidance*, the Department of Commerce's *Technical and Economic Assessment of IPv6*, and technical documents from agencies such as DOD. We interviewed IPv6 experts in government and industry, including key members of the telecommunications industry and officials from major software and hardware vendors. Organizations we interviewed include Comcast, Global Crossing, Gartner, AT&T, Internet2, MCI, New York University, Lumeta, and Microsoft. To identify which organizations to interview, we relied on our review of publications and research and on our interviews with IPv6 experts. Finally, we attended a number of IPv6 workshops and conferences featuring leaders in the field.

We performed our work from August 2005 through May 2006 in accordance with generally accepted government auditing standards.

# Appendix II: GAO Contacts and Staff Acknowledgments

## GAO Contacts

David A. Powner, 202-512-9286
Keith A. Rhodes, 202-512-6412

## Acknowledgments

In addition to the contact names above, William Carrigg, Camille Chaires, Neil Doherty, Nancy Glover, Richard Hung, Sabine Paul, Harold Podell, Teresa Smith, 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