AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

TO LEAD OR TO FOLLOW: THE NEXT GENERATION INTERNET AND THE TRANSITION TO IPv6

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JUNE 29, 2005

Serial No. 109–41

Printed for the use of the Committee on Government Reform



Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

22–510 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

CHRISTOPHER SHAYS, Connecticut
DAN BURTON, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
GIL GUTKNECHT, Minnesota
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
CANDICE S. MILLER, Michigan
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
GINNY BROWN-WAITE, Florida
JON C. PORTER, Nevada
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
CHARLES W. DENT, Pennsylvania
VIRGINIA FOXX, North Carolina

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. DUTCH RUPPERSBERGER, Maryland
BRIAN HIGGINS, New York
ELEANOR HOLMES NORTON, District of Columbia

BERNARD SANDERS, Vermont
(Independent)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

CONTENTS

Page

Hearing held on June 29, 2005 1

Statement of:

Curran, John, chairman, American Registry for Internet Numbers; Jawad Khaki, corporate vice president, Microsoft Corp.; Stan Barber, vice president, Verio, Inc.; and Alex Lightman, chief executive officer, Charmed Technologies, Inc. 56

Barber, Stan 83

Curran, John 56

Khaki, Jawad 65

Lightman, Alex 91

Evans, Karen, Administrator, Electronic Government and Information Technology, Office of Management and Budget; David Powner, Director, Information Technology Management Issues, Government Accountability Office; Keith Rhodes, Chief Technologist and Director, Center for Technology and Engineering, Government Accountability Office; George Wauer, Director, Architecture and Interoperability, Office of the Assistant Secretary of Defense for Networks and Information Integration and Office of the Chief Information Officer, U.S. Department of Defense, accompanied by Major General Dennis Moran, Vice Director, Command, Control, Communications and Computer Systems, Joint Chiefs of Staff, U.S. Department of Defense 11

Evans, Karen, ... 11

Powner, David 18

Rhodes, Keith 45

Wauer, George 45

Letters, statements, etc., submitted for the record by:

Barber, Stan, vice president, Verio, Inc., prepared statement of 86

Cummings, Hon. Elijah E., a Representative in Congress from the State of Maryland, prepared statement of 109

Curran, John, chairman, American Registry for Internet Numbers, prepared statement of 59

Davis, Chairman Tom, a Representative in Congress from the State of Virginia, prepared statement of 4

Evans, Karen, Administrator, Electronic Government and Information Technology, Office of Management and Budget, prepared statement of 14

Khaki, Jawad, corporate vice president, Microsoft Corp., prepared statement of 67

Lightman, Alex, chief executive officer, Charmed Technologies, Inc., prepared statement of 94

Porter, Hon. Jon C., a Representative in Congress from the State of Nevada, prepared statement of 108

Powner, David, Director, Information Technology Management Issues, Government Accountability Office, prepared statement of 19

Wauer, George, Director, Architecture and Interoperability, Office of the Assistant Secretary of Defense for Networks and Information Integration and Office of the Chief Information Officer, U.S. Department of Defense, prepared statement of 47

Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of 8

TO LEAD OR TO FOLLOW: THE NEXT GENERATION INTERNET AND THE TRANSITION TO IPv6

WEDNESDAY, JUNE 29, 2005,

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 2:15 p.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis (chairman of the committee) presiding.

Present: Representatives Davis of Virginia, Gutknecht, Dent, Waxman, Cummings, Kucinich, Higgins and Norton.

Staff present: Melissa Wojciak, staff director; David Marin, deputy staff director/communications director; Chas Phillips, policy counsel; Rob White, press secretary; Drew Crockett, deputy director of communications; Victoria Proctor, senior professional staff member; Teresa Austin, chief clerk; Sarah D'Orsie, deputy clerk; Leneal Scott, computer systems manager; Kristin Amerling, minority general counsel; Nancy Scola, minority professional staff member; and Earley Green, minority chief clerk.

Chairman TOM DAVIS. The committee will come to order.

I apologize for starting late, we were supposed to have a vote on the floor. I was over there so I could leave at the beginning of the vote and they ended up with just a voice vote.

Welcome to today's hearing on the Next Generation Internet and the transition to Internet protocol version 6 [IPv6].

Nearly 30 years ago in a Department of Defense lab, the Internet was born. Originally designed to facilitate communications after a nuclear strike, as the protocols were tested, refined and implemented, people began to recognize the possibilities for far broader applications. Today, these protocols underpin the Internet.

American ingenuity developed, fostered, and fielded these simple open protocols to solve a narrow set of problems, but this seemingly small network solution has sparked a global revolution in communications. Over the past decade, cyberspace has grown into a dynamic nervous system that controls our Nation's critical cyber and physical infrastructures.

Within an hour's drive of Fairfax County, there are about one quarter of all Internet Service Providers on the entire planet. About a quarter of all the Internet packets in the world are going through a hub in northern Virginia. If you drive down the Dulles Access Road, you can see the physical impact of the Internet on

Virginia, but the current Internet, and the protocols and networks that underpin it, may have reached its limits.

Internet protocol version 6 [IPv6], offers benefits for expanded addressing, greater security, and new products, services, and missions for Next Generation Internet applications. However, it presents several challenges including: one, understanding the international implications; two, preparing the Federal Government; and three, ensuring a secure transition.

Not surprisingly, interest in IPv6 is gaining momentum around the world, particularly areas 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 aggressive efforts to deploy IPv6. Asian countries have been aggressive in adopting IPv6 technology, because Asia controls only about 9 percent of the allocated IPv4 addresses, and yet has more than half of the world's population.

Asian governments have invested hundreds of millions of dollars in IPv6 technology. China has been extremely aggressive and Japan has set up an IPv6 Promotion Council, using tax incentives to encourage research and adoption of IPv6 by its private sector.

Europe currently has a task force that has the dual mandate of initiating country and regional IPv6 task forces across European states and seeking global cooperation around the world, and Europe's Task Force and the Japanese IPv6 Promotion Council forged an alliance to foster worldwide deployment.

Here at home, challenges such as procurement, information technology management, and modernization are often addressed deliberately by the Federal Government and change often takes years to implement, but these are the challenges we take up on this committee.

Federal Government IT expenditures are on track to surpass $65 billion in fiscal year 2006, making the Federal Government once again the largest purchaser of IT products and services in the world. In addition, a recent report forecasts that IT spending will continue to rise throughout the decade, reaching over $90 billion in fiscal year 2010. With this buying power, we need to make sure that the best and most secure technology is a priority when the Government acquires IT goods and services.

I believe that we all want the United States to have the world's best information technology infrastructure, including maintaining the world's best Internet industry. I believe we all want U.S. defense capabilities to perform with maximum effectiveness and efficiency, and to realize the full potential of net-centric warfare.

I believe we all want the best Homeland Security systems, including cameras, sensors, and first responder systems intelligently integrated together. I believe we all want fiscally responsible Federal spending, including spending on information infrastructures that will deliver multiple returns on investment and preserve taxpayer dollars.

Today, we will hear about Federal efforts to transition to IPv6. Our purpose here is to learn from the public and private sectors, to hear if IPv6 can help us achieve long-term economic, defense, homeland security, and technological leadership. If it can play a part in reaching those goals, then I want to know what support the

Government Reform Committee, the Congress, and the U.S. Federal Government need to provide.

I also want to learn about the risks. Every day brings news of another computer intrusion or data theft. I hope to hear about the security risks that exist under the current protocol, how IPv6 might address these risks, and whether the transition presents its own risks.

Finally, I hope to learn if the United States is at competitive risk with respect to the Next Generation Internet. My committee held a hearing recently about the lengths to which the Chinese government would go to make sure that only Chinese software is purchased by Chinese government agencies. The Chinese government not long ago announced that CERNET2, the first network based on pure IPv6 technology, was going into formal operation. An official from China's National Development Reform Commission said China's Next Generation Internet will bring huge benefits to their national economy and increase the country's competitiveness in national defense, economy, science and technology.

Last year, I asked GAO to look at IPv6 and its implications for the Federal Government. Today, we are here, in part, to review their report, which highlights the fundamental challenges facing the Federal agencies, the White House, and Congress.

However, to reap the benefits from IPv6 Federal agencies must first begin to plan and develop requirements that will take full advantage of what the new protocol offers. I hope that the Office of Management and Budget will continue its leadership role in information policy and begin to address some essential issues, including how much IP address space the Federal agencies may require, whether the Federal Government is ready for the transition, and how much it will cost.

At this stage, I am gathering input on IPv6. I was pleased to receive a copy of the Department of Defense IPv6 Transition Plan recently. I am looking forward to receiving the Department of Commerce's report as soon as possible, and see how IPv6 can help America's economy and help America's exports.

The vast majority of the technology we know and use is rooted in the United States. Many of these innovations were a result of the ideas and hard work from individuals who came from other countries to live, to work, or to be educated, some of whom are here today.

America draws the best and the brightest from around the globe, they produce their best work here, and then we share those efforts with the rest of the world. I am confident that we can meet the challenge of this transition.

I would now recognize the distinguished ranking member, Mr. Waxman, for an opening statement.

[The prepared statement of Chairman Tom Davis follows:]

Opening Statement of Chairman Tom Davis
"To Lead or To Follow: The Next Generation Internet and the Transition to IPv6"
2:00 pm
June 29, 2005
Committee on Government Reform
2154 Rayburn House Office Building

Welcome to today's hearing on the Next Generation Internet and the transition to Internet protocol version 6, also known as IPv6.

Nearly thirty years ago in a Department of Defense lab the Internet was born. Originally designed to facilitate communications after a nuclear strike, as the protocols were tested, refined and implemented, people began to recognize the possibilities for far broader applications. Today, these protocols underpin the Internet.

American ingenuity developed, fostered, and fielded these simple open protocols to solve a narrow set of problems. But this seemingly small network solution has sparked a global revolution in communications. Over the past decade, cyberspace has grown into a dynamic nervous system that controls our nation's critical cyber and physical infrastructures.

Within an hour's drive of Fairfax County, there are about one quarter of all Internet Service Providers on the entire planet. About a quarter of all the Internet packets in the world are going through a hub in Northern Virginia. If you drive down the Dulles Access Road, you can see the physical impact of the Internet on Virginia.

But the current Internet, and the protocols and networks that underpin it, may have reached its limits. Internet protocol version 6 (IPv6) offers benefits for expanded addressing, greater security, and new products, services, and missions for Next Generation Internet applications. However, it presents several challenges including: (1) understanding the international implications, (2) preparing the federal government, and (3) ensuring a secure transition.

Not surprisingly, interest in IPv6 is gaining momentum around the world, particularly areas 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 aggressive efforts to deploy IPv6.

Asian countries have been aggressive in adopting IPv6 technology, because Asia controls only about 9% of the allocated IPv4 addresses, and yet has more than half of the world's population.

Asian governments have invested hundreds of millions of dollars in IPv6 technology. China has been extremely aggressive and Japan has set up an IPv6 Promotion Council, using tax incentives

to encourage research and adoption of IPv6 by its private sector.

Europe currently has a task force that has the dual mandate of initiating country and regional IPv6 task forces across European states and seeking global cooperation around the world. And Europe's Task Force and the Japanese IPv6 Promotion Council forged an alliance to foster worldwide deployment.

Here at home, challenges such as procurement, information technology management, and modernization are often addressed deliberately by the federal government and change often takes years to implement. But these are the challenges we take up on this Committee.

Federal Government IT expenditures are on track to surpass $65 billion in FY06 – making the federal government once again the largest purchaser of IT products and services in the world. In addition, a recent report forecasts that IT spending will continue to rise throughout the decade, reaching over $90 billion in fiscal 2010. With this buying power, we need to make sure that best and most secure technology is a priority when the government acquires IT goods and services.

I believe that we all want the United States to have the world's best Information Technology infrastructure, including maintaining the world's best Internet industry.

I believe we all want US defense capabilities to perform with maximum effectiveness and efficiency, and to realize the full potential of net-centric warfare.

I believe we all want the best Homeland Security systems, including cameras, sensors, and first responder systems intelligently integrated together.

I believe we all want fiscally responsible federal spending, including spending on information infrastructures that will deliver multiple returns on investment and preserve taxpayer dollars.

Today, we will hear about federal efforts to transition to IPv6. Our purpose here is to learn from the public and private sectors, to hear if IPv6 can help us achieve long-term economic, defense, homeland security, and technological leadership. If it can play a part in reaching those goals, then I want to know what support the Government Reform Committee, the Congress, and the US federal government need to provide.

I also want to learn about the risk. Every day brings news of another computer intrusion or data theft. I hope hear about the security risks that exist under the current protocol, how IPv6 might address these risks, and whether the transition presents its own risks.

Finally, I hope to learn if the US is at competitive risk with respect to the Next Generation Internet. My committee held a hearing recently about the lengths to which the Chinese government would go to make sure that only Chinese software is purchased by Chinese government agencies. The Chinese government not long ago announced that CERNET2, the first network based on pure IPv6 technology, was going into formal operation. An official from China's National Development Reform Commission said China's Next Generation Internet will

bring huge benefits to their national economy and increase the country's competitiveness in national defense, economy, science and technology.

Last year, I asked GAO to look at IPv6 and its implications for the federal government. Today, we are here, in part, to review their report, which highlights the fundamental challenges facing the federal agencies, the White House, and Congress.

However, to reap the benefits from IPv6 federal agencies must first begin to plan and develop requirements that will take full advantage of what the new protocol offers.

I hope that the Office of Management and Budget will continue its leadership role in information policy and begin to address some essential issues, including how much IP address space the federal agencies may require, whether the federal government is ready for the transition, and how much it will cost.

At this stage, I am gathering input on IPv6. I was pleased to receive a copy of the Department of Defense IPv6 Transition plan recently. I am looking forward to receiving the Department of Commerce's report as soon as possible, and see how IPv6 can help America's economy and help America's exports.

The vast majority of the technology we know and use is rooted in the United States. Many of these innovations were a result of the ideas and hard work from individuals who came from other countries to live, to work, or to be educated -- some of whom are here today. America draws the best and the brightest from around the globe, they produce their best work here, and then we share those efforts with the rest of the world. I am confident that we can meet the challenge of this transition.

* * * *

Mr. WAXMAN. Mr. Chairman, thank you for holding today's hearing on Internet protocol version 6, what is often called the "Next Generation Internet."

The architecture of the Internet was first developed more than 30 years ago, but the Internet of today is far different than it was then. Whereas the early Internet joined together a small number of computers, the Internet today connects desktop computers, laptop computers, network servers, handheld Blackberries, cell phones and cars. Even dishwashers and refrigerators are beginning to go online.

The Internet is not yet breaking down under the strain, but there are limitations that need to be addressed. The current system has the capacity to connect together 4 billion different computers and devices at any one time. This may seem like a lot, but consider the computers and cell phones one typical family might own today, or all the desktops, laptops, and Blackberries in use in the Federal Government.

Four billion seems even smaller in light of the growing Internet use worldwide. In fact, it is only because of network administrator ingenuity that the current protocol's technological limitations are not paralyzing the Internet.

The Next Generation Internet eliminates major existing technological limitations. This new system increases access to the Internet exponentially while also offering the added benefits of more sophisticated security and improved connectivity.

Consumers will reap these benefits, but it is the Federal Government that may well be the greatest beneficiary. A recent GAO study found that Next Generation Internet could help DOD to create more advanced weapons and information systems. Other potential uses include wireless border security sensors and interoperable networks for first-responders.

Unfortunately, the Government is not taking full advantage of this opportunity. GAO found that few agencies beyond the Defense Department have even begun to ready themselves for the Next Generation Internet. Meantime, the rest of the world is taking Next Generation Internet seriously. China is building a nationwide network that will run on the new system. India's private sector is actively moving to take advantage of these new technologies.

The Next Generation Internet is coming. I look forward to hearing from witnesses about what we can do to take the lead in developing the Internet as we did 30 years ago or we can wait for this evolution to pass us by and then play catch up.

Thank you, Mr. Chairman, for the opportunity to make an opening statement. I look forward to the testimony of the witnesses today.

[The prepared statement of Hon. Henry A. Waxman follows:]

Statement of Rep. Henry A. Waxman, Ranking Minority Member
Committee on Government Reform
Hearing on "To Lead or To Follow: The Next Generation Internet and the Transition to IPv6"

June 29, 2005

Mr. Chairman, thank you for holding today's hearing on Internet Protocol version 6, what is often called the "Next Generation Internet."

The architecture of the Internet was first developed more than 30 years ago. But the Internet of today is far different than it was then. Whereas the early Internet joined together a small number of computers, the Internet today connects desktop computers, laptop computers, network servers, handheld Blackberries, cell phones and cars. Even dishwashers and refrigerators are beginning to go online.

The Internet is not yet breaking down under the strain. But there are limitations that need to be addressed. The current system has the capacity to connect together 4 billion different computers and devices at any one time. This may seem like a lot. But consider the computers and cell phones one typical family might own today. Or all the desktops, laptops, and Blackberries in use in the federal government.

Four billion seems even smaller in light of the growing Internet use worldwide. In fact, it is only because of network administrator ingenuity

that the current protocol's technological limitations are not paralyzing the Internet.

The Next Generation Internet eliminates major existing technological limitations. This new system increases access to the Internet exponentially while also offering the added benefits of more sophisticated security and improved connectivity.

Consumers will reap these benefits. But it is the federal government may well be the greatest beneficiary. A recent GAO study found that Next Generation Internet could help DOD to create more advanced weapons and information systems. Other potential uses include wireless border security sensors and interoperable networks for first-responders.

Unfortunately, the government is not taking full advantage of this opportunity. GAO found that few agencies beyond the Defense Department have even begun to ready themselves for the Next Generation Internet.

Meantime, the rest of the world is taking Next Generation Internet seriously. China is building a nationwide network that will run on the new system. India's private sector is actively moving to take advantage of these new technologies.

The Next Generation Internet is coming. I look forward to hearing from witnesses about what we can do to take the lead in developing the

Internet as we did 30 years ago. We shouldn't let this evolution to pass us by and then play catch up.

Thank you, Mr. Chairman.

Chairman TOM DAVIS. Mr. Waxman, thank you very much.

The Members will have 7 days to submit opening statements for the record.

I will now recognize our first panel, a very distinguished panel. We have: the Honorable Karen Evans, Administrator, Electronic Government and Information Technology, Office of Management and Budget; David Powner, Director, Information Technology Management Issues, Government Accountability Office; Keith Rhodes, Chief Technologist and Director, Center for Technology and Engineering, Government Accountability Office; George Wauer, Director, Architecture and Interoperability, Office of the Assistant Secretary of Defense for Networks and Information Integration and Office of the Chief Information Officer, U.S. Department of Defense. Mr. Wauer is accompanied by Major General Dennis Moran, Vice Director, Command, Control, Communications and Computer Systems, Joint Chiefs of Staff, U.S. Department of Defense. General Moran, thank you for being with us today.

It is the policy of the committee to swear all witnesses before you testify.

[Witnesses sworn.]

Chairman TOM DAVIS. We will start the testimony with Ms. Evans. Karen, you know the rules. We try to keep it to 5 minutes. Your entire statement is in the record. Questions will be based on your entire statement but you have 5 as a summary.

Karen, thanks a lot for being with us again.

STATEMENTS OF KAREN EVANS, ADMINISTRATOR, ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET; DAVID POWNER, DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE; KEITH RHODES, CHIEF TECHNOLOGIST AND DIRECTOR, CENTER FOR TECHNOLOGY AND ENGINEERING, GOVERNMENT ACCOUNTABILITY OFFICE; GEORGE WAUER, DIRECTOR, ARCHITECTURE AND INTEROPERABILITY, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION AND OFFICE OF THE CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF DEFENSE, ACCOMPANIED BY MAJOR GENERAL DENNIS MORAN, VICE DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

STATEMENT OF KAREN EVANS

Ms. EVANS. Thank you for inviting me to speak about the Federal Government's efforts in preparing for the transition to Internet protocol version 6. This afternoon, I would like to briefly identify the steps we are taking in preparation for transition.

As I mentioned in my April 7, 2005 testimony before this committee regarding our efforts to safeguard the Government's information systems, late last fall OMB directed the agencies to provide a preliminary report on their planning activities for the transition to IPv6. Only the Department of Defense had undertaken any significant effort in this area.

Given the lack of government-wide progress and our concern regarding the complexities of transition, we recognize the need to begin developing a comprehensive transition planning guide and process.

We are about to take the first step and issue a policy memorandum providing guidance to the agencies to ensure an orderly and secure transition to IPv6. The purpose of the guidance will be to ensure effective planning and to raise the level of awareness and urgency of preparing for IPv6.

The overarching challenge facing us is ensuring continued, uninterrupted functionality of Federal agencies during the transition while providing continued and improved information assurance. This will require major changes in the architecture of many agency networks. Since there is a large embedded base of IPv4-compatible equipment and applications, transitioning to IPv6 will also require large capital investments and labor resources. While the challenges are significant, they are not insurmountable, especially if we approach them methodically and in phases. The guidance will lay out five important actions the agencies should take.

First, agencies will have to familiarize themselves to the transitions issues by reviewing the GAO report, the Commerce report, and particularly the Department of Homeland Security's US-CERT advisory of security issues concerning IPv6. Since IPv6 is already present in many Federal agency networks, it is important that agencies begin addressing the security risks associated with IPv6 now.

Second, agencies will have to assign a specific individual to lead and coordinate agency planning. This person will be responsible for monitoring, enforcing, and reporting on the transition and implementation of IPv6 within the agency.

Third, agencies will develop an inventory of existing IP capable devices and technologies. To ensure an orderly transition from IPv4 to IPv6, we must establish a baseline and determine the size of the problem. While we know IPv6 technologies are deployed throughout the Government, but like other organizations, we do not know specifically which ones, how many there are, or precisely where they are located. We are planning for each agency to file a report of their inventory of IP capable devices and technologies to OMB in the first quarter of fiscal year 2006.

Fourth, agencies will conduct an impact analysis to determine fiscal and operational impacts and risks during the transition to IPv6. We are planning for each agency to report the results of this impact analysis to OMB in the first quarter of fiscal year 2006, and it should include analysis on cost and risk. For cost, the agencies must report on estimates for planning, infrastructure acquisition, above and beyond normal expenditures, training, and risk mitigation.

Fifth, the policy will direct the CIO Council to develop before the end of the calendar year, more detailed IPv6 implementing guidance. It will include guidance for developing detailed prioritized schedules and milestones, integrating IPv6 with the agency enterprise architecture, developing necessary IPv6-related policies and compliance mechanisms, training material, and test plans for IPv6 compatibility and interoperability. To the extent the agencies are

currently capable of addressing the elements of the future CIO Council guidance, they have been instructed to begin doing so now. We will also use the OMB EA Assessment Framework to measure the degree to which agencies are effectively performing this planning element.

Our policy will also set June 2008 as the date by which all agencies' infrastructure, network backbones, must be using IPv6 and agency networks must interface with this infrastructure. Once the network backbones are ready, the applications and other elements will follow. Setting this firm date is necessary to maintain focus on this important issue. Overall the actions set out in our policy will begin to address the many challenges that come with IPv6 transition.

I would like to take one moment to discuss one aspect of the implementation guidance. Later in this hearing, you may be hearing testimony that says IPv6 poses a problem associated with the capability called tunneling. In fact, tunneling is extremely widely used throughout the Government and industry and facilitates cost effective and safe communications.

During the question period, I would be happy to answer your questions about the aspect of IPv6 tunneling and how it could be controlled and any other questions you have.

Thank you for this opportunity to talk about the administration's strategy.

[The prepared statement of Ms. Evans follows:]

STATEMENT OF THE HONORABLE KAREN EVANS ADMINISTRATOR
FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

June 29, 2005

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to speak about the Federal government's efforts in preparing for the transition to Internet Protocol version 6 (IPv6).

This morning I would like to briefly discuss some benefits of IPv6, highlight some challenges in making the transition, and identify the steps we are taking to address those challenges.

The transition to IPv6 is more than an upgrade of the existing protocol. IPv6 is replete with new features and functions such as expanded address space, improved flexibility and functionality, improved information routing, enhanced mobility features, simplified activation, configuration and operation of networks and services, and once fully implemented, improved security. IPv6 when fully functional will ultimately result in a number of benefits, but more importantly a new communication paradigm.

Some benefits of IPv6 will be directly to logistics and consumers. IPv6, combined with Radio Frequency Identification Tags and integrated into mobile phones and consumer electronics, will support new ways of thinking about the way business is conducted and the way consumers could buy goods and services. Other benefits of IPv6 will be directly to commuters and first responders. For example, IPv6 combined with Dedicated Short-Range Communication technology, could lead to smarter and safer cars, fewer traffic delays, and an improved ability for first responders to signal drivers of their rapid approach while controlling the stop lights at an intersection.

Actually, the paradigm shift has already started in the Federal government because IPv6 capable software and hardware already exist in Federal government networks (and elsewhere). Most current computer operating systems support IPv6 and many installed base of routers and switches already have IPv6 built-in. In other words, the transition to IPv6 is already taking place, but it has many challenges -- including planning for system migration, security aspects of the transition, and as yet undefined privacy concerns of the technology itself.

As I mentioned in my April 7, 2005, testimony before this committee regarding our efforts to safeguard the government's information and systems, late last fall OMB directed the agencies to provide a preliminary report on their planning activities for the transition to IPv6. Only the Department of Defense had undertaken any significant effort in this area. Given the lack of government-wide progress and our concern regarding the complexities of transition, we recognized the need to begin developing a comprehensive transition planning guide and process.

We are about to take the first step and issue a policy memorandum providing guidance to the agencies to ensure an orderly and secure transition to IPv6. The purpose of the guidance will be to ensure effective planning and to raise the level of awareness and urgency of preparing for IPv6. Later in my testimony I will discuss the key elements of the policy.

As you know, the Government Accountability Office (GAO) recently released a report identifying a number of significant IPv6 challenges. A draft report, published for public notice and comment by the Department of Commerce, also identifies many of the same challenges. Both reports describe careful planning as a key for Federal agencies to make an orderly transition and both emphasize the need to ensure the security of agency information and networks during the transition.

On the security issue, and to underscore the complexity of planning for the transition, not all experts agree on the extent of the security risk involved in the IPv6 transition. The most telling example of these differing views comes from experts developing today's most commonly used computer operating system. They have expressed skepticism regarding the level of risk highlighted in the GAO report. We continue to discuss this issue with them at staff and senior levels and are awaiting their comments on the GAO report and will provide those comments to GAO as well.

The overarching challenge facing us is ensuring continued uninterrupted functionality of Federal agencies during the transition while providing continued and improved information assurance. This will require major changes in the architecture of many agency networks. Since there is a large embedded base of IPv4-compatible equipment and applications, transitioning to IPv6 will also require large capital investments and labor resources. While the challenges are significant, they are not insurmountable, especially if we approach them methodically and in phases.

Let me begin by sharing with you what we are doing to address these challenges.

As I mentioned earlier, we are about to issue a policy memorandum providing guidance to the agencies to ensure an orderly and secure transition to IPv6. The guidance will lay out five important actions the agencies should take.

First, agencies will have to familiarize themselves to the transitions issues by reviewing the GAO report, Commerce report, and particularly the Department of Homeland Security's US-CERT advisory of security issues concerning IPv6. Since IPv6 is already present in many Federal networks, it is important that agencies begin addressing the security risks associated with IPv6 now.

Second, agencies will have to assign a specific individual to lead and coordinate agency planning. This person will be responsible for monitoring, enforcing, and reporting on the transition and implementation of IPv6 within the agency.

Third, agencies will develop an inventory of existing IP capable devices and technologies. To ensure an orderly transition from IPv4 to IPv6, we must establish a baseline and determine the size of the problem. While we know IPv6 technologies are deployed throughout the government,

but like other organizations, we do not know specifically which ones, how many there are, or precisely where they are located. We are planning for each agency to file a report of their inventory of IP capable devices and technologies to OMB in the first quarter of FY 2006.

Fourth, agencies will conduct an impact analysis to determine fiscal and operational impacts and risks during the transition to IPv6. We are planning for each agency to report the results of this impact analysis to OMB in the first quarter of FY 2006, and it should include analysis on cost and risk. For cost, the agencies must report on estimates for planning, infrastructure acquisition (above and beyond normal expenditures), training, and risk mitigation.

As for all other planning for investments in information technology, agencies' IPv6 analyses will include a risk inventory and assessment using the criteria set forth in existing OMB capital planning and investment control policy found in OMB Circular A-11, Section 300. This policy requires agencies to discuss a range of risks and present a plan to eliminate, mitigate, or manage them, with milestones and completion dates. Assessments will include areas such as life-cycle costs, schedules, reliability of systems, dependencies and interoperability between systems, asset and information protection, and information privacy.

Fifth, the policy will direct the CIO Council to develop before the end of the calendar year, more detailed IPv6 implementing guidance. It will include guidance for developing detailed prioritized schedules and milestones (e.g., a sequencing plan), integrating IPv6 with the agency enterprise architecture, developing necessary IPv6-related policies and compliance mechanisms, training material, and test plans for IPv6 compatibility and interoperability. To the extent the agencies are currently capable of addressing the elements of the future CIO Council guidance, they have been instructed to begin doing so now.

Developing detailed prioritized schedules and milestones is especially important for integrating agency IPv6 transition activities with their enterprise architectures and thus ensure the transition is consistent with and supporting of their mission and business needs. We will use the OMB EA Assessment Framework to measure the degree to which agencies are effectively performing this planning element.

Our policy will also set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. Once the network backbones are ready, the applications and other elements will follow. Setting this firm date is necessary to maintain focus on this important issue. Overall the actions set out in our policy will begin to address the many challenges that come with IPv6 transition.

We are also now discussing with the National Institute for Standards and Technology whether we need a Federal Information Processing Standard for IPv6 and are preparing an amendment to the Federal Acquisition Regulation to include language on IPv6.

Conclusion

Thank you for this opportunity to discuss the Administration's strategy on IPv6. As we continue to work with the agencies to move toward an IPv6 environment, we will continue to look for new

opportunities to refine our oversight of this important initiative. We appreciate your interest in OMB's role in IPv6 and will continue our efforts to drive improved performance and results throughout the Executive branch agencies.

Thank you. I will be happy to answer any questions at this time.

Chairman TOM DAVIS. Thank you very much, Ms. Evans.
Mr. Powner.

STATEMENT OF DAVID POWNER

Mr. POWNER. We appreciate the opportunity to testify on Internet protocol version 6.

With me today is Keith Rhodes, GAO's Chief Technologist who will discuss the security aspects of transitioning to this new protocol.

The initial benefits of IPv6 is that it will immediately remedy the shortage of worldwide Internet addresses and will greatly increase the number of devices that can connect to the Internet. IPv6 is clearly gaining momentum globally, especially in regions such as Asia where address space is limited and concerns exist about the U.S.'s adoption of the new protocol as it pertains to global competitiveness.

This morning, I would like to leave you with three thoughts before Mr. Rhodes discusses the need to mitigate security transition risks.

First, there are many benefits to the new protocol; second, Government transition has been slow; and third, key planning efforts are essential. In addition to the increased address space that will accommodate the growing number of users and mobile devices, IPv6 will, among other things, allow for an efficient and possibly faster routing, simplify network administration and enhance IP security by improving authentication and confidentiality of data sent over the Internet.

The Department of Defense plans to utilize IPv6 features. For example, it envisions our future soldiers equipped with multiple IP addresses for communications and to monitor vital signs. Other Federal agencies, for the most part, have not initiated IPv6 planning efforts. Because of this, we recommended to OMB that they instruct Federal agencies to begin addressing key planning efforts. These include developing inventories and assessing risks, creating business cases and identifying timelines and methods for transition.

Mr. Chairman, we have been working with the Office of Management and Budget and we recognize Ms. Evans' efforts that earlier this year called for Federal agencies to update strategic plans, enterprise architectures and acquisition strategies to address IPv6 transition. Although Ms. Evans' statement is encouraging, more effective leadership is needed.

In addition, we also recommended that Federal agencies take immediate action to address near term security risks. Ironically, this new protocol that in the long term will improve network security creates several near term vulnerabilities if not properly managed, as Mr. Rhodes will now demonstrate.

Before turning it over, Mr. Chairman, I would like to thank you for your leadership in this area and for jump starting the Federal Government's transition to this new protocol.

[The prepared statement of Mr. Powner follows:]

United States Government Accountability Office

GAO

Testimony
Before the House Committee on Government Reform

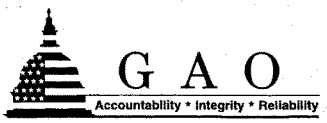
For Release on Delivery
Expected at 2 p.m. EDT
Wednesday, June 29, 2005

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-05-845T

GAO
Accountability · Integrity · Reliability

Highlights

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

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.

June 29, 2005

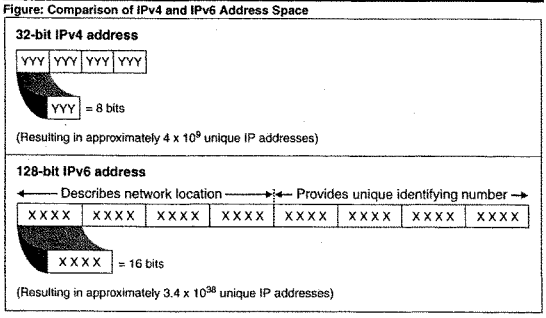
INTERNET PROTOCOL VERSION 6

Federal Agencies Need to Plan for Transition and Manage Security Risks

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



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.

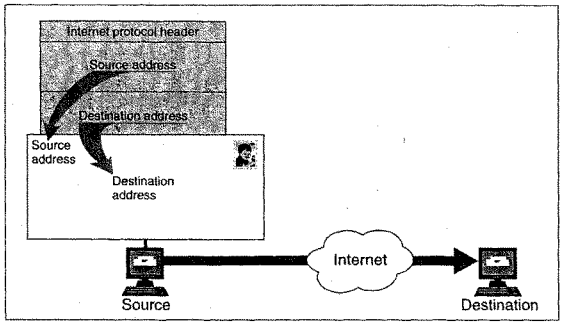
the routing addresses is the Internet protocol. The most widely deployed version of IP is version 4 (IPv4).

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

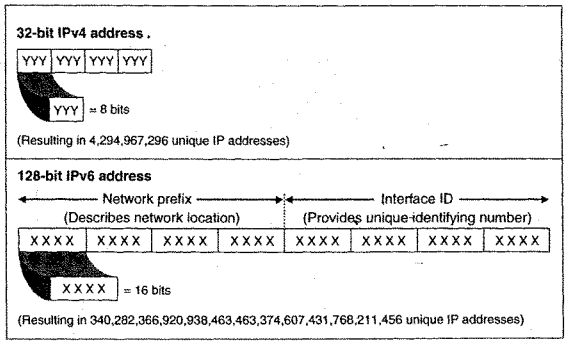
[6]The Web site for IETF is http://www.ietf.org/iesg/1rfc_index.txt

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



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

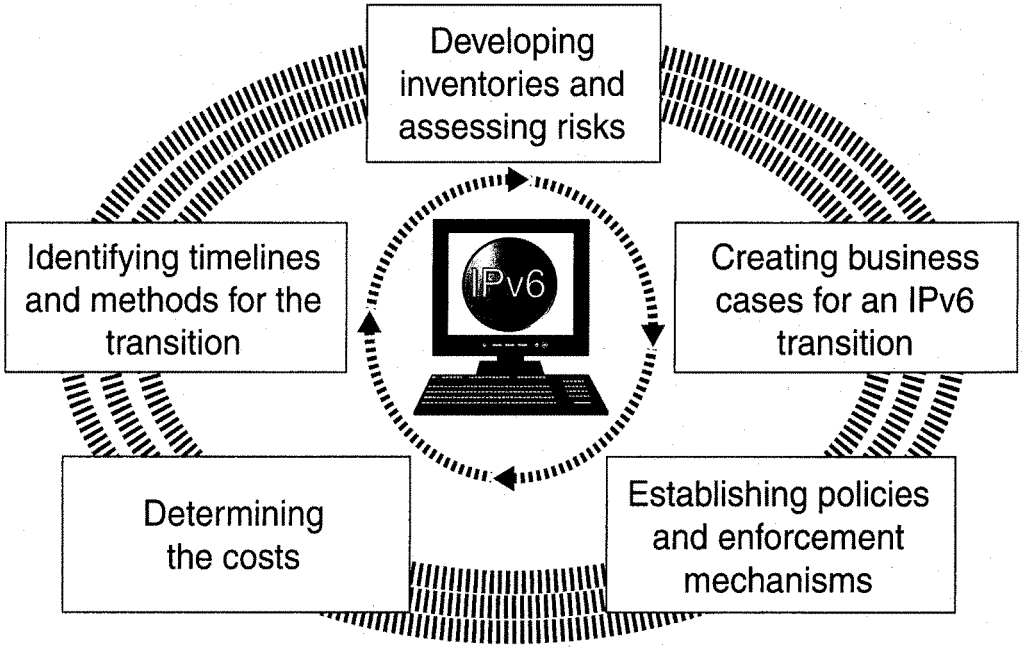
PRINTED ON RECYCLED PAPER

GAO
Accountability * Integrity * Reliability

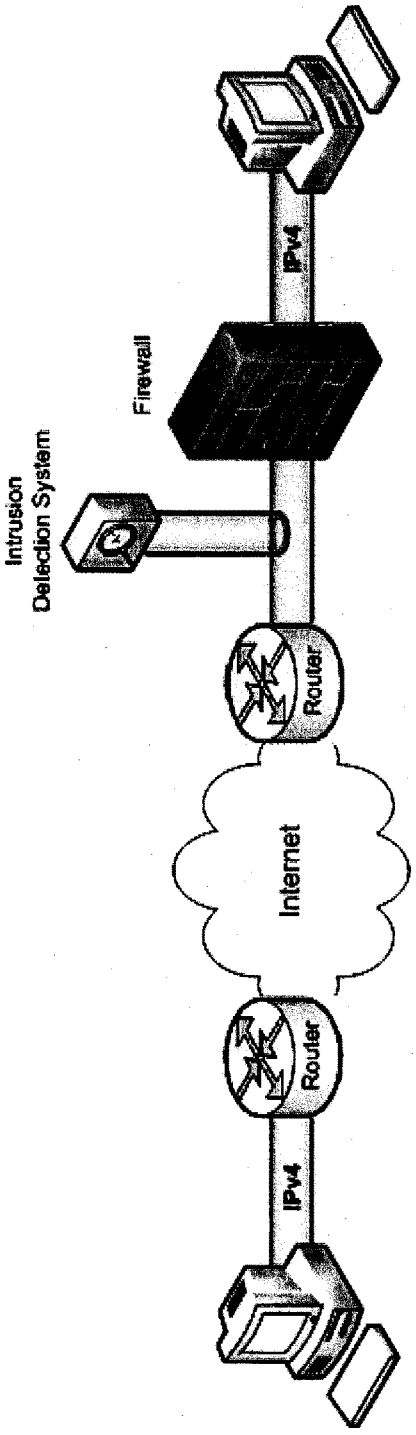
Internet Protocol Version 6

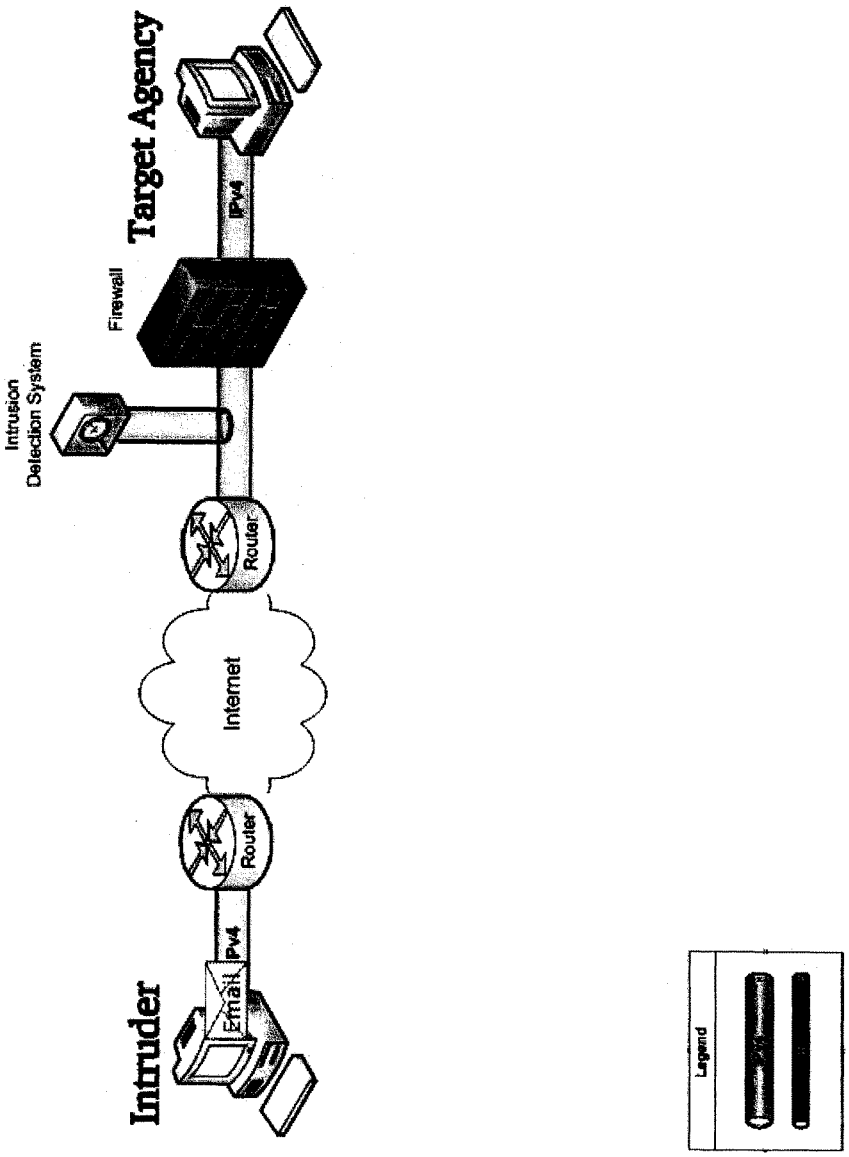
Federal Agencies Need to Plan for Transition and Manage Security Risks

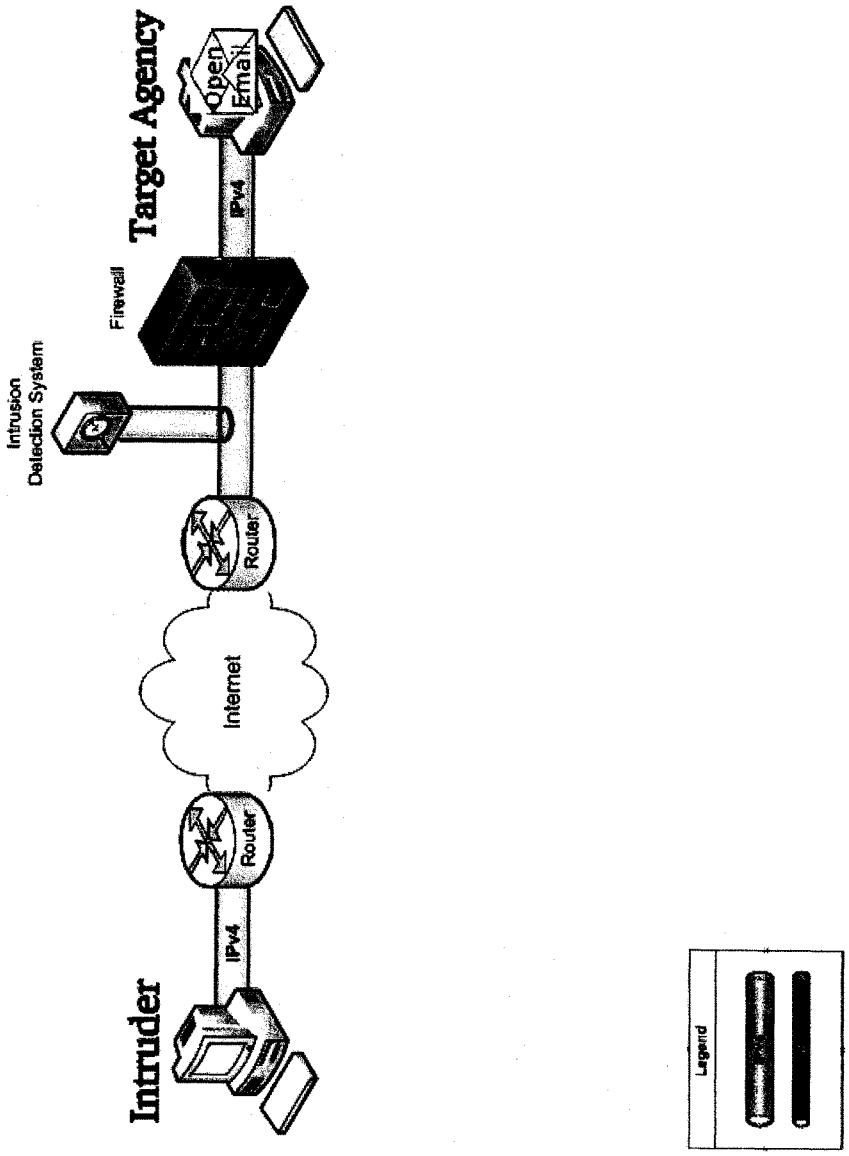
IPv6 Planning Considerations

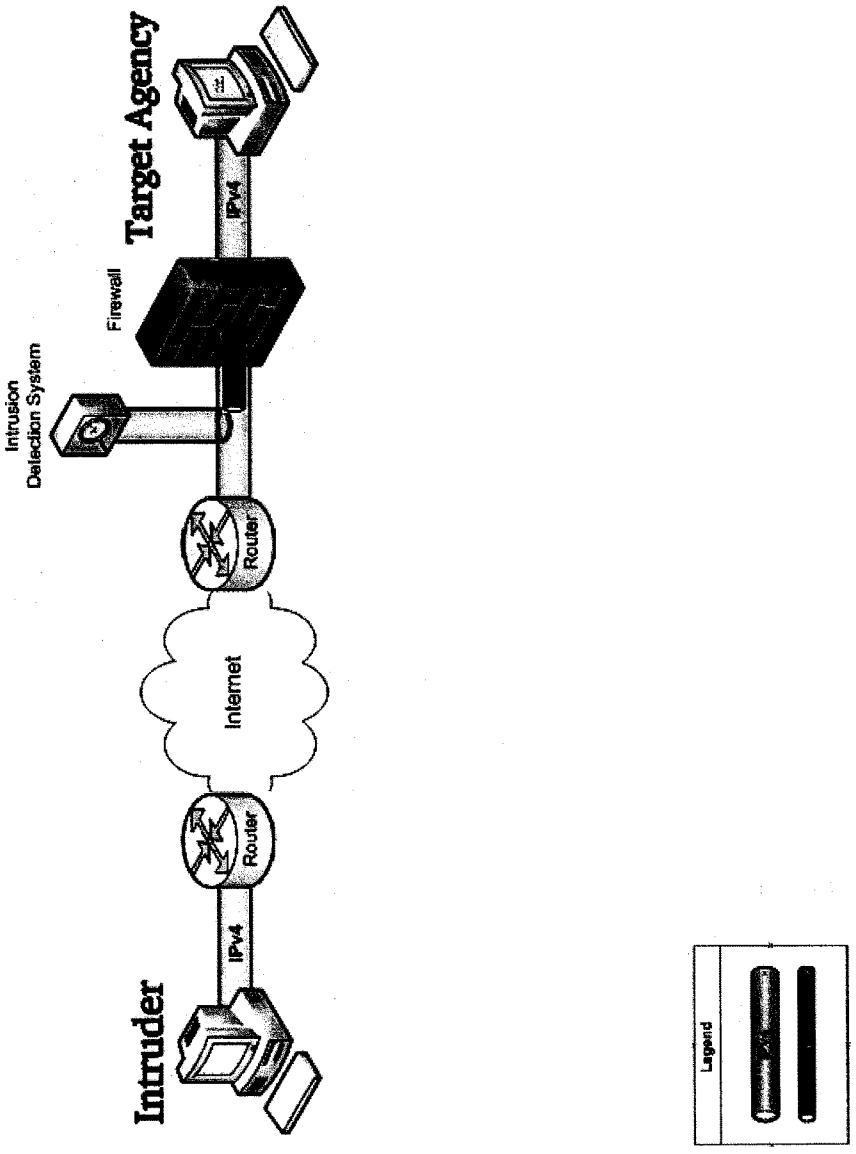


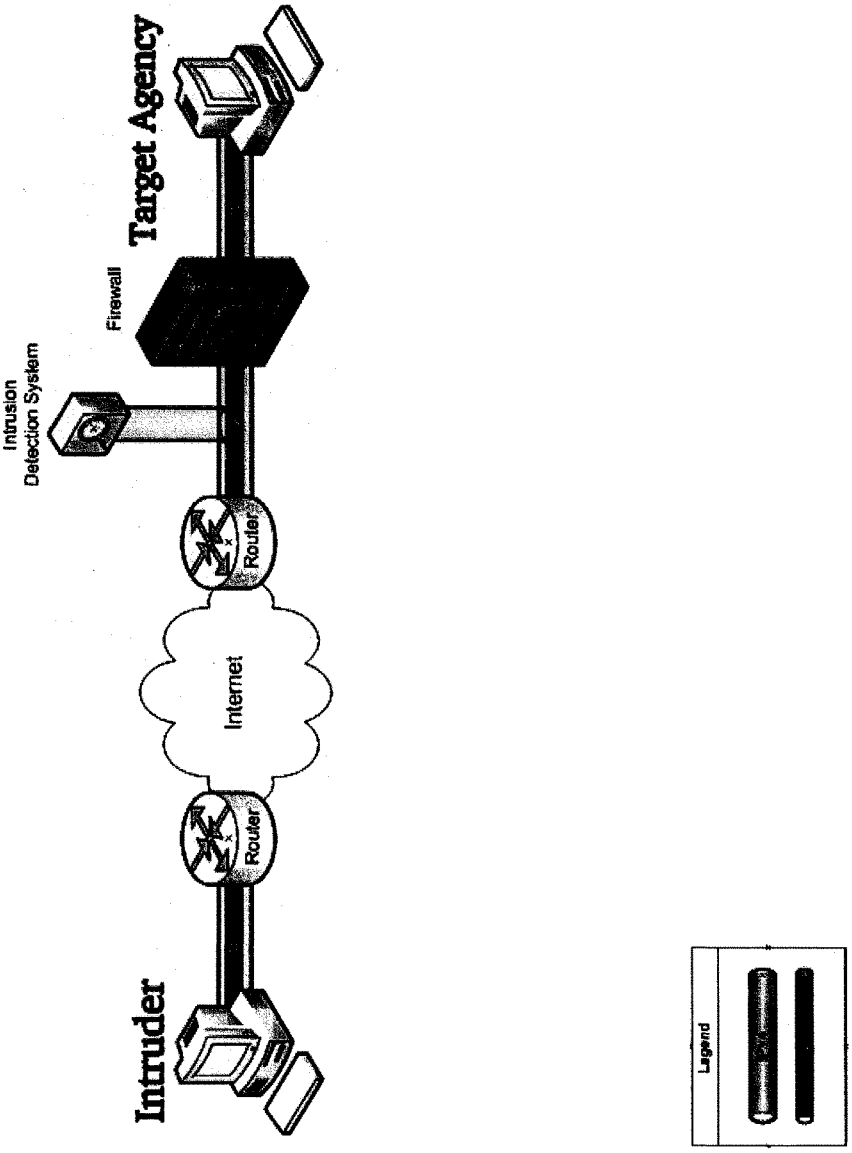
Source: GAO.

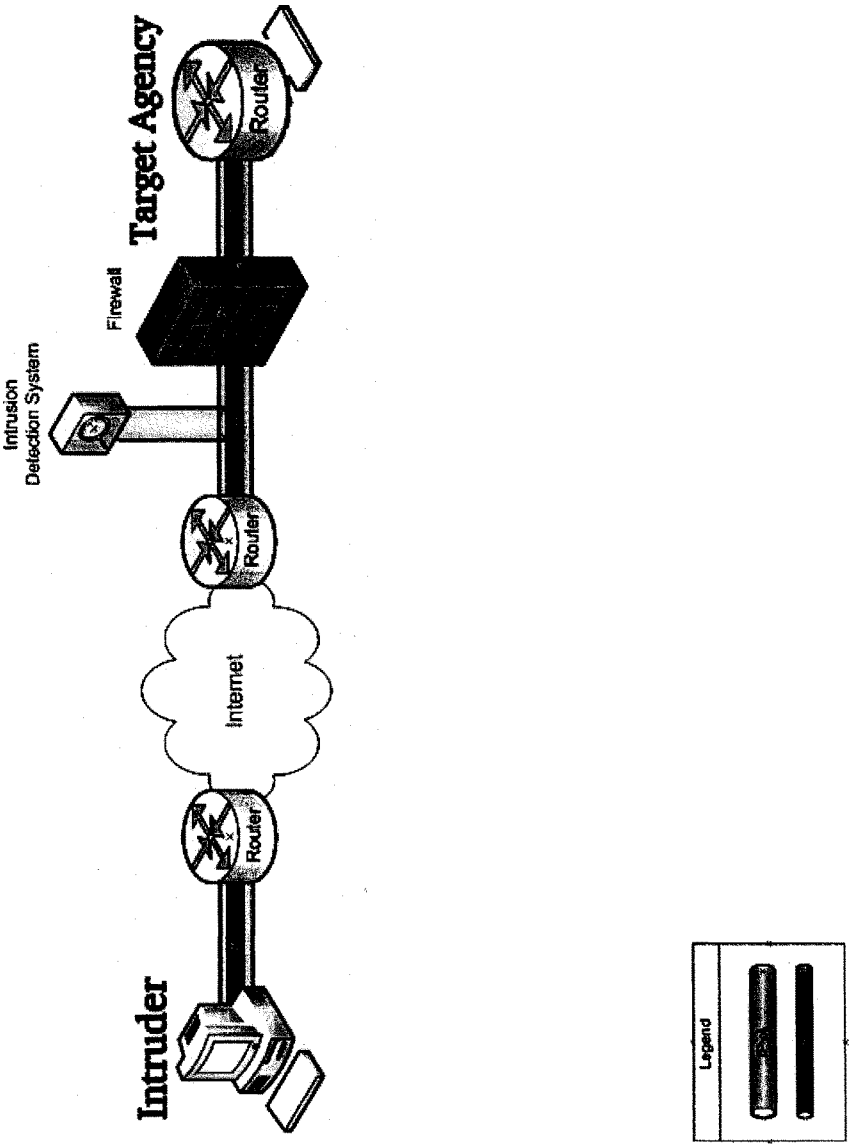

IPv4
Firewall
Intrusion
Detection System
Router
Internet
Router
IPv4

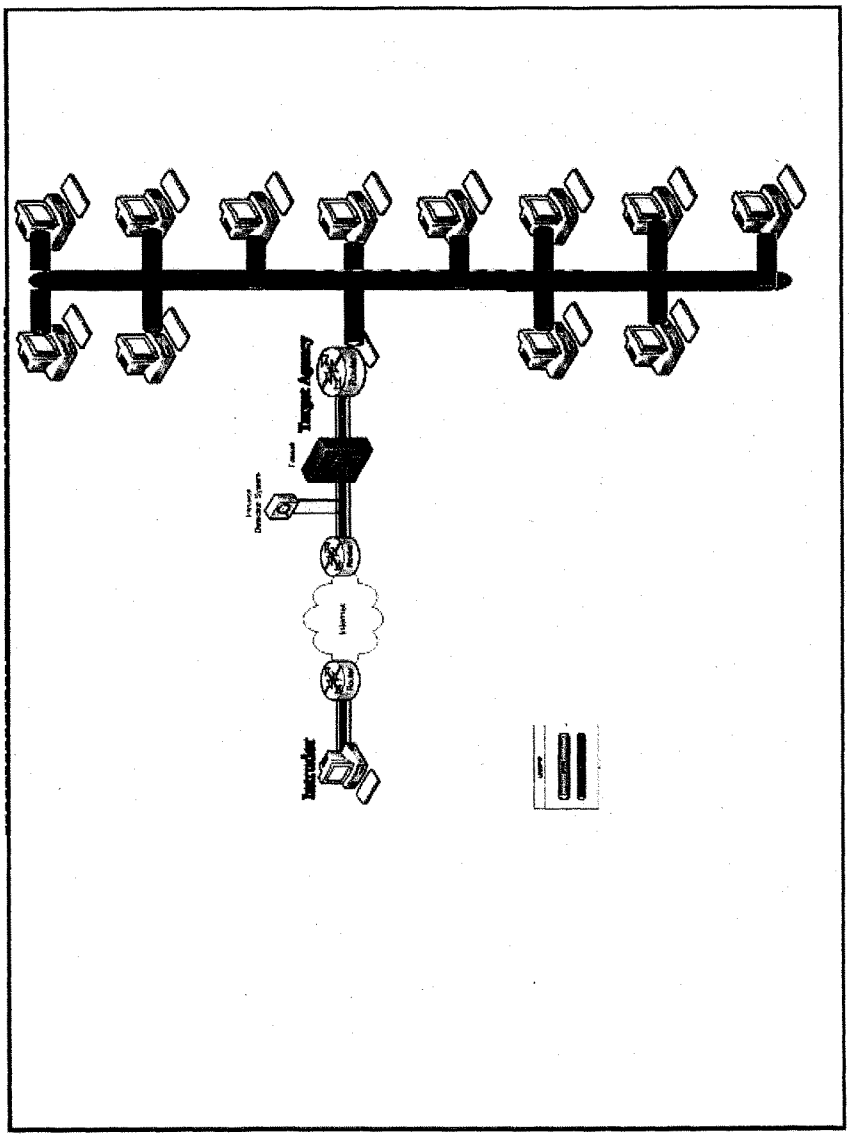

Intruder
IPv4
Email
Router
Internet
Router
Intrusion
Detection System
Firewall
Target Agency
IPv4
Legend


Intruder
IPv4
Router
Internet
Router
Intrusion
Detection System
Firewall
Target Agency
IPv4
Open
Email
Legend


Intruder
IPv4
Router
Internet
Router
Intrusion Detection System
Firewall
Target Agency
IPv4
Legend


Intruder
Router
Internet
Router
Intrusion
Detection System
Firewall
Target Agency
Legend


Intruder
Router
Internet
Router
Intrusion Detection System
Firewall
Target Agency
Router
Legend


Target Agency
Internet
Intruder

STATEMENT OF KEITH RHODES

Mr. RHODES. What I am going to explain to you is an exploit that we have used when we are testing Federal departments and agencies and one we have proven and documented in our own laboratory.

The first slide is a typical IPv4 configuration. You see a router, intrusion detection, a firewall, all working together to protect a system that is connected to the Internet.

The intruder on the left sends the target agency on the right a specially crafted e-mail. The targeted user opens the e-mail thinking it is a normal e-mail. Let me note here this attack does not require the user to double click on an attachment as is common with most MOU ware. If the e-mail is Web-based, that is, it is written in the language of the World Wide Web, the hypertext mark up language, then even if the user just previews it in the window in their mail system, the attack will launch.

The e-mail looks normal to the target but deep inside the computer, the IPv6 stack is turned on, given an address and a mission. The mission is to send a shell back to the intruder using IPv6 inside IPv4. This means that the shell request is sent back to the intruder via tunnel which is carried by the IPv4 packets. The shell request is totally invisible to the firewall, the intrusion detection system and the Internet, just some normal looking IPv4 packets.

Now there is a new network, a dedicated network between the intruder and the target agency unseen by most current firewall and IDS technologies.

As the intruder explores the target agency, the intruder's software converts the PC to a router and many other computers answer the IPv6 call. Now there is a covert IPv6 network invisible to the target agency.

My final point is this could have been avoided using available technology and best practices, for example, closing Port 41 to outbound traffic on your firewall. The transition to IPv6 can be done safely and securely with proper precautions. Otherwise, the intruders are out there and they know how to do this.

Thank you, Mr. Chairman, and I will accept any questions.

Chairman TOM DAVIS. Thank you very much.

Mr. Wauer.

STATEMENT OF GEORGE G. WAUER

Mr. WAUER. Good afternoon. Thank you for the invitation to testify before the committee.

In the interest of time, I will submit my formal written testimony for the record. I would, however, like to make the following key points.

The Department of Defense views version 6 as a critical enabler in achieving our vision of global net-centric operations. Modifying version 4 to accomplish this version would have been, at best, problematical. Version 6 provides specific features that can make the net-centric vision a reality.

In June 2003, the Department established the goal of transitioning to version 6 by 2008. We are defining phase timelines that include specific system implementations that address increasingly complex end-to-end functionality. However, due to the critical

nature of the Department's mission, it is imperative that this transition not imperil our current operational capabilities.

Our strategy and the position of the Department is to complete the transition with minimal additional costs by using phase timelines and relying primarily on already-scheduled and planned technology refreshments. In fact, since October 2003, we have required version 6 capability on all new acquisitions and procurements. This strategy allows the Department to leverage ongoing commercial and industry version 6 efforts.

However, even with this transition strategy, there will be some additional costs for this major technology insertion. These additional costs are expected to be in the area of planning, engineering, technical assessments and training. Implementing version 6 across the Department is complex and presents many challenges. Careful and early planning has been necessary to ensure the transition to version 6 is accomplished in an effective and controlled manner. Version 6 must not be disruptive to the everyday, strategic tactical and business operations of the Department.

DOD is firmly committed to the expeditious transition to version 6 in a manner that is affordable and protects the interoperability, security and performance of the existing requirements we have on our plate.

Thank you and I appreciate the committee's interest in the transition for the Department and I would be happy to answer any questions.

[The prepared statement of Mr. Wauer follows:]

FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE
HOUSE COMMITTEE
ON GOVERNMENT REFORM

STATEMENT BY

GEORGE G. WAUER

DIRECTOR, ARCHITECTURE AND INTEROPERABILITY

OFFICE OF THE

ASSISTANT SECRETARY OF DEFENSE

FOR NETWORKS AND INFORMATION INTEGRATION

AND

DOD CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

JUNE 29, 2005

FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE
HOUSE COMMITTEE
ON GOVERNMENT REFORM

Mr. Chairman and Members of the Committee:

Thank you for the invitation to testify before this committee. I appreciate the opportunity to update you on DoD's progress in transitioning to Internet Protocol version 6 (IPv6). We see IPv6 as a critical enabler in achieving our vision for global, net-centric operations. We seek to build a more agile, robust, interoperable and collaborative DoD, where warfighters, and intelligence and business users all share knowledge on a secure, dependable and global network that enables superior decision-making and effective operations. In short, we must transition to IPv6 to achieve DoD's net-centric vision.

What follows is the Department's IPv6 transition strategy, benefits of transitioning, transition costs and challenges, and an assessment of the Department's transition to date.

DoD's Transition Strategy

In June 2003, the DoD established a goal of transitioning to IPv6 by 2008. We are defining phased timelines that include specific system implementations that address increasingly complex, end-to-end functionality. However, due to the critical nature of the Department's mission, it is imperative that this transition not imperil our current operational capabilities. Achieving this goal will be influenced by the following key tenets:

- Controlling transition costs by relying primarily on already scheduled or planned technology refreshments, and by requiring IPv6 capability for acquisitions or procurements after October 2003.

- Managing transition risks in the areas of interoperability, performance, and security by a measured and controlled approach to fielding IPv6 capabilities using pilot implementations and testing and evaluation activities.

- Satisfying operational criteria, defined by the Joint Staff, that must be met before the DoD can fully transition to IPv6.

- Completing transition and implementation planning to include the development of milestone objectives to manage and control the transition.

- Availability of tested, scalable, affordable IPv6 capable, commercial products that meet the DoD's performance and assurance needs.

Benefits of Transitioning to IPv6

The Internet Protocol (IP) is becoming the foundation of interoperability across the DoD, enabling the connection of people and systems, independent of time and location. Today, sensors, platforms, weapons, and units are being built as "net-ready" nodes, incorporating IP-based protocols. The IPv6 features most important to achieving DoD net-centric operations include:

- **Nearly Unlimited, Unique Addresses**, making everything reachable, provided the authority exists.
- **End-to-End Security**, ensuring that all communications are authenticated and encrypted.
- **Mobile Communications**, allowing communications on the move and dynamic, ad-hoc networks.
- **Improved Network Operations**, permitting the creation of theater communications in significantly less time.
- **New End-to-End Functionality**, including policy-based networking and quality of service with priority and preemption.

Costs of Transitioning to IPv6

As stated previously, the DoD IPv6 transition strategy positions the DoD to complete the transition with minimal additional costs. However, even with this transition strategy there will be some additional costs for this major technology insertion, which we will address through the normal budget process. These additional costs are expected to be in the areas of:

- Planning, engineering, technical assessments, and training to support the transition to IPv6.
- Pilot implementations and testbeds to demonstrate IPv6 technology readiness and scalability.
- Modifications to ongoing developmental efforts to make them IPv6 capable.
- Upgrades to legacy equipment or software where timely technology refreshments are not programmed.

This strategy allows DoD to leverage ongoing commercial and industry IPv6 efforts to better meet DoD needs.

Challenges of Transitioning to IPv6

There are challenges in implementing IPv6 across the DoD. Careful and early planning is necessary to ensure that the DoD transitions to IPv6 are accomplished in an effective and controlled manner that optimizes end-to-end performance, interoperability, security, scalability, and reliability. The IPv6 transition must not be disruptive to everyday strategic, tactical, or business operations of the DoD. The issues that must be addressed during transition include:

- Maintaining end-to-end network and application interoperability.
- Maintaining interoperability with Allies and Coalition partners.
- Ensuring no additional security vulnerabilities are introduced.

Current DoD policy prohibits using IPv6 on networks that carry operations traffic, for example, tactical operations, today. As we continue to understand the vulnerabilities and to manage the risks, we will provide additional Information Assurance guidance that will permit deployments of IPv6 with recommended security configurations.

IPv6 Transition Assessment

The DoD has accomplished significant, critical planning activities including the development of the DoD IPv6 Transition Plan, which was formally approved in March 2005. Building on this plan, the DoD Components are developing their own transition plans. Additionally, the following have been accomplished building towards IPv6 transition:

- Established the DoD IPv6 Transition Office at the Defense Information Systems Agency to support the overall DoD enterprise transition. This Office is critical for ensuring common transition solutions, technical guidelines, knowledge-sharing and coordinating IPv6 issues. Additionally, the Services have each established their own Transition Offices to address any Service-unique issues.
- Integrated the requirement for IPv6 capability into the Defense acquisition process. Today, we are buying IPv6 capable Information Technology.
- Established an IPv6 standards profile to be used in procuring IPv6 capable products and services.
- Collaborated with industry and academia to identify and resolve IPv6 product interoperability issues.
- Established an IPv6 research and development environment using the Defense Research and Engineering Network.

Conclusion

The DoD is firmly committed to expeditiously transitioning to IPv6 in a manner that is affordable and protects interoperability, security and performance requirements. We welcome the opportunity to share our policy documents, transition plans, and technical guidance as well as lessons learned with other Federal agencies. Although our focus is on transitioning the DoD, we recognize and welcome the increased interest at the Federal level in IPv6 transition.

Chairman TOM DAVIS. Ms. Evans, let me start with you. IPv6 raises some very broad and very serious policy issues as you addressed. Some of these issues are squarely within OMB. For example, agencies are planning for IPv6 and securing their current systems.

Other issues such as the international challenges, economic competitiveness, lack of IPv6 firewalls for classified systems go beyond the purview of OMB and the CIO Council. What is the administration doing to organize and address this challenge?

Ms. EVANS. First off, there are a couple things in there but more importantly, everything we do within the administration is coordinated within the Executive Office of the President. As we move forward and take on these issues, they are coordinated through the councils that exist within the Executive Office of the President.

We have taken on this issue, my policy and how it impacts the Federal agencies has also been looked at going forward, so I can talk about what I am doing to affect the Federal agencies overall. I would be happy to take back any other specific questions that you have and get answers for the record.

Chairman TOM DAVIS. Do we have any ballpark estimate of the cost and the labor requirements of the transition?

Ms. EVANS. Right now, based on the analysis we did, it could grow by an order of magnitude. This is the reason why we are asking for the agencies to prepare these reports and these documents so that we can get an estimate of what it is going to cost.

For the most part, and I believe my colleagues from DOD have already stressed this, a lot of the costs as far as hardware, software or the products we buy, they are already IPv6 capable and enabled and have that capability. The cost we want to make sure we have a true handle on deal with the applications that are currently in place. They may be using something very specific to IPv4. That is why I agree with everything that has been said so far. The planning efforts will be very critical to get a good handle on the cost estimates.

Chairman TOM DAVIS. Given the expenditures by the Europeans and the Asians on this, which far out-strip anything we have done are we behind the eight ball at this point? How would you describe where we stand?

Ms. EVANS. As far as the implementation of IPv6, I think everything you read in the GAO report shows that it is self explanatory. We have a huge investment obviously in version 4 and the way to move forward is the administration, at least from the Federal Government's standpoint and our investment is we are going to take a market-based approach and view how the market and the products conduct to go forward.

We are taken that first step by indicating that we want our network backbones to be IPv6 enabled by 2008. We feel that is a significant step for where we already are. When I say we are behind the eight ball, it is relative depending on what services, what activity, whether you are looking at it from the consumer or the Federal Government standpoint of the investment.

Chairman TOM DAVIS. Mr. Powner, to the extent that you are able, can you kind of describe the projects you are undertaking in IPv6?

Mr. POWNER. The projects GAO is currently undertaking?

Chairman TOM DAVIS. I am sorry, I meant to ask this of Mr. Wauer.

Mr. WAUER. Those are spread out over the whole Department of Defense. We are looking at all of the new procurements going on such as TSAT, the gig bandwidth expansion and several of the other procurements that are going on, JTERS. All of those are going to be IPv6 enabled.

Chairman TOM DAVIS. Are you in any position at this point to talk about how long it would take to complete the transition and what the cost would be?

Mr. WAUER. No, I am not.

Chairman TOM DAVIS. Ball park?

Mr. WAUER. Anything I would give you would be strictly off the top of my head. The actual implementation plans from each of the services and components are being generated. They have gone through a first cut and until we see those and are able to aggregate those, it would be very difficult to put a specific timeframe on that.

Chairman TOM DAVIS. Mr. Powner, how do we measure the success of the transition? Could GAO benchmark the United States versus other nations? Would that be an appropriate benchmark?

Mr. POWNER. One of the things that we are currently in the process of doing for you is looking at some of the early adopters of IPv6. In fact, we will touch on some of that with where some of the other countries are. Initially, some of the data out there is a bit misleading. Clearly from a leadership perspective, I agree with some of your comments earlier and where your questions were going that we are behind the eight ball from a leadership perspective clearly. From an actual transition perspective, it is a little unclear where some of the other countries are. There are councils in place and tax incentives being thrown out there for corporations and agencies.

Chairman TOM DAVIS. How much has been spent by other countries roughly on the transition at this point?

Mr. POWNER. No ballpark.

Chairman TOM DAVIS. Significantly more though than we have spent, is that fair to say?

Mr. POWNER. Likely, yes. That is a huge unknown here in the States, how much we spend, especially from the Federal perspective.

Chairman TOM DAVIS. You may actually have the incentive because they are the ones that need the addresses and everything else.

Mr. POWNER. Absolutely and we don't have the pressing need because we control more than 70 percent of those 4 billion addresses to date.

Chairman TOM DAVIS. If the world stayed at IPv4 at this point, we would not be disadvantaged competitively, it would be the other countries and that is where the impetus is?

Mr. POWNER. Correct, but I think if you look from a mission perspective and why DOD has this very detailed effort in place to transition from a mission perspective, we would like to stay on the cutting edge. There are implications for homeland security applications where we could really benefit from what the new protocol could provide.

Chairman TOM DAVIS. Would you say this is not comparable to Y2K because we are not dealing with a time certain at this point? This continues to be a work in progress as it emerges. As Ms. Evans said, market-based and we will see how quickly it gets up to snuff?

Mr. POWNER. It is clear we don't have a firm deadline like Y2K but I think it is nice we have a target the administration is now throwing out for 2008. Clearly it is similar to Y2K in the sense that it affects a lot of equipment that is out there. Our phones, our PCs, operating systems, network routers, it is widespread in terms of what will need to eventually be swapped out.

Chairman TOM DAVIS. Reading the papers today with constant reports of intrusions and security breaches, it appears the Internet is relatively insecure. With full implementation of IPv6, do you think it would provide greater security potentially?

Mr. POWNER. Clearly with the new protocol, there is a feature in it that allows for more robust authentication and confidentiality of the day. In the long term, it is believed that protocol will allow for greater security.

The issue where it is insecure as Mr. Rhodes demonstrated is there is a lack of awareness that agencies currently have, IPv6 in their networks today? If they knew that occurred, they could effectively mitigate those risks.

Chairman TOM DAVIS. Let me ask the entire panel, should the U.S. Government obtain its own block of IPv6 address space now?

Mr. RHODES. I don't think it is actually necessary for the United States to do that when you are talking about a huge volume of addresses. Locking in your own set is not the same as it was with IPv4. That is one of the great benefits of IPv6 that there is plenty for everyone. If you lock in your own, that is fine because then you have contiguous sets of IP addresses that you can work but it is not the same struggle that we had with the current set of addresses that you need to worry about in IPv6.

General MORAN. The Department of Defense is in the process of pulling together an area of how many we think we will need and we are processing forward to establish that and get it allocated to us.

Chairman TOM DAVIS. Do you think the transition to IPv6 is an economic imperative and do you think the Federal Government is losing its lead in technology by not moving more quickly? Mr. Powner, do you have any thoughts on that?

Mr. POWNER. Clearly, I think we are in a far better position if we lead than lag. Being in a position where we can take advantage of some of the applications that IPv6 could provide would put us on sound footing, especially when you look at some of the capabilities we need to secure, the Department of Homeland Security.

Mr. RHODES. Mr. Chairman, as a scientist and as an engineer, I can only say if we allow other people to adapt before us, they will be the ones who build the killer applications and we won't because they will be able to work with it everyday. The Chinese already have an IPv6 router that they are just waiting for market share on. They have an IPv6 dedicated and enabled network.

If you look at the implementations in Japan and look at the equipment being built in Japan, they are the ones working with it

on a regular basis in day-to-day operations. We would like to have a voice over IP; they are already working on it because they get the quality of service benefit from IPv6. Somebody is going to be ahead of us if they are working with it every day.

If we relegate it to being networks sitting inside universities, that is fine but that is research. As Ms. Evans points out, that is not the market driving it.

General MORAN. From the Department of Defense perspective, it is an operational imperative that we move to IPv6 because if you look at the future warfighting concepts, whether they be land, air or sea, we must have an IPv6 environment in order to move the information we are going to require to be successful in the environment. Therefore, the DOD I think has moved out so aggressively.

Chairman TOM DAVIS. Do you think IPv6 quality of service standards meet the needs of DOD and will IPv6 give DOD less quality of service than we have currently?

General MORAN. I am not a technologist but I do believe in order to get the quality of service capabilities that we require across our global information grid which is going to be our part of the network, we are going to need to have the IPv6 quality of service implementation.

We are involved through the department level to ensure that the definitions of those standards meet our requirements.

Chairman TOM DAVIS. But basically what you have is Asia and Europe moving ahead on their own. Whatever we do, we will have to adjust to these standards. Either we will be left behind or the more proactive we are, we will be able to continue a leadership role.

General MORAN. It is my personal belief that we need to be in a leadership role so that we get the standards developed in a way that from the Department's perspective, we get the capabilities we require.

Chairman TOM DAVIS. I appreciate the leadership role DOD is taking.

Mr. Gutknecht, any questions?

This is new stuff for a lot of members. A lot of us are still trying to figure out how to plug in the computers but it is critically important for us, not just for operation of government but for global competitiveness.

From the GAO perspective, I appreciate your report. This was very, very helpful to others in kind of laying this out. This is the first congressional hearing on this but it is something we will continue to try to ride herd on here. Hopefully the interest will spread to other committees as we understand the national security implications, the global competitiveness, economic ramifications of this and this is a big bite for you, Ms. Evans, as well. I hope you are getting cooperation within the Government as you continue to take your leadership role on this.

If there aren't other questions for this panel.

General MORAN. I really want to make one statement about one item you just mentioned and that was the question about Y2K. I do believe the reason the Department has been so successful is that our leadership is using the Y2K model to manage this. That is what has forced the leadership to deal with the realities of this

change that is required. Even though we don't have a day and time that we have to be on IPv6, the management strategy the Department is using is exactly what we used in Y2K. I would argue that is why we were so successful.

Mr. WAUER. If I can inject one other thing, one of the things the Department has found is this is a highly complex process. It is spread out over a myriad of different applications. It is not a trivial thing, both from a technical and management standpoint.

We actually stood up a transition office. This is not a part-time job for a group of people. This is going to require some dedicated staffing and some real emphasis being placed on it to get this thing done right.

Chairman TOM DAVIS. Is there dedicated funding for this at this point or are we kind of taking a little here and there?

Mr. WAUER. The first 2 years, there was some dedicated funding for the transition office itself. We are now in the roll. It is spread across because the way we manage true programs, it is spread out across the programs.

Chairman TOM DAVIS. Explain to me what happens if we sit back and do nothing. If we were to sit back at this point and take a very relaxed point of view and let everyone else move ahead, what are the ramifications of that? Ms. Evans.

Ms. EVANS. I would like to venture an answer that we could. As a Nation, we could sit back because we do own over 70 percent of the address in space. We could invest and make that address in space continuously work for us and gain greater efficiencies but I think as pointed out by several others here, if you want to drive innovation, you have to create an environment where people can think about what if. You saw that as we were going through the big dot com boom. Everybody was in the what if, the Internet presented so many different opportunities.

This isn't a concept, a technical concept that sometimes is a little hard to grasp but it provides the opportunity to provide an environment out there that you can ask that question again, what if. What if I want to do this for Homeland Security, what if I want to do this for the Department of Defense so that I can expand? Industry, I believe, would respond because of the way that innovation has always been here within the United States. So we could sit back and continue to invest in the current technology that we have and make it more efficient or we can invest in the possibilities of the future.

The administration acknowledges that with proper planning and proper resources, IPv6 would allow the country to be able to move forward to deal with all those issues.

Chairman TOM DAVIS. Mr. Rhodes.

Mr. RHODES. Just wanted to give you one practical homeland security application. We are very concerned about chemical, biological, radiological and nuclear unconventional devices. One of the solutions to that is to place sensors. Each one of those sensors is going to be on a network, each one of those sensors is going to require an IP address, they are going to have to send their information back somehow.

If you want to really have ground truth either from the standpoint of the soldiers, sailors, airmen and Marines or the first re-

sponders, you are going to have to have this. Yes, we could sit back but you just don't have enough Internet available to you at this moment in its own configuration.

Chairman TOM DAVIS. Thank you very much.

We will take a 2-minute break and call our next panel.

[Recess.]

Chairman TOM DAVIS. Thank you all for being here.

You heard our first panel of witnesses and some of the questions. Hopefully we can get into some other questions as we move through this.

We have on this panel: John Curran, chairman, American Registry for Internet Numbers; Jawad Khaki, corporate vice president, Microsoft Corp.; Stan Barber, vice president, Verio, Inc.; and Alex Lightman, chief executive officer, Charmed Technologies, Inc.

[Witnesses sworn.]

Chairman TOM DAVIS. Mr. Curran, we will start with you and move down the line. Try to keep it to 5 minutes but if you need time, it looks like we have a small group of members, so we will have some time if you need a couple extra minutes to make your point.

STATEMENTS OF JOHN CURRAN, CHAIRMAN, AMERICAN REGISTRY FOR INTERNET NUMBERS; JAWAD KHAKI, CORPORATE VICE PRESIDENT, MICROSOFT CORP.; STAN BARBER, VICE PRESIDENT, VERIO, INC.; AND ALEX LIGHTMAN, CHIEF EXECUTIVE OFFICER, CHARMED TECHNOLOGIES, INC.

STATEMENT OF JOHN CURRAN

Mr. CURRAN. Good afternoon.

My comments are formally a part of the record, so I am not going to read them but I will summarize them for the sake of brevity.

I am John Curran. I was one of the founders of the American Registry of Internet Numbers. I have been the chairman since its inception in 1998.

I would like to say I welcome the chance to come here and talk about U.S. leadership and the IPv6 arena. I think it is a very important topic.

I want to say for background not everyone is aware of how IP addresses are allocated. ARIN is one of the five regional Internet registries that handle address management. We handle it for North America which includes Canada, the United States, much of the Caribbean. Our counterparts are AfriNIC, APNIC, LACNIC and RIPE NCC which handles Europe. Combined, these registries form a bottoms up policy formation process that all Internet service providers worldwide participate in. This is a very important concept to keep in mind as we talk about Internet numbers and how they are allocated and the transition to IPv6.

I have background in industry as well which is relevant to this. I have been involved in three Internet companies as chief technology officer including BBN which was the builders of the IBERnet, the original IP network; XO Communications out in Virginia; and most recently a company called ServerVault.

My involvement in the Internet actually goes back quite some time. I was involved in the Internet Engineering Task Force back when it was time to form the IP Next Generation Directorate, the group that took on the problem of the IP address depletion issue. I would like to review what happened at that time because it is very important to this proceeding to give context as to why we are talking about IPv6 now.

Back in 1993, the emerging research network and commercial Internet was very successful. We had the regional networks growing by leaps and bounds, we had the very start of the commercial Internet providers. A group of people got together and figured out that we were going to have an address depletion problem. Back at that time, that problem looked like it could occur as soon as 2005, potentially as late as 2010.

As a result, the IETF formed a group called the IP Next Generation Directorate which was challenged with forming the requirements for the next generation Internet protocol. The result of that group and the follow on efforts in the IETF was the IPv6 protocol. That protocol as we all know has a much larger address space and has numerous technical enhancements. This is all covered very well in the GAO report and I won't go through it.

It was envisioned that larger address space was needed because we were going to run out of address spaces again very early in 2000. Luckily, there were some changes in address allocation policy at the same time. These changes resulted in the usage of IPv4 address space being reduced substantially, the rate at which we were using them, and as a result, we have no problem today. IPv4 address space is being used but there is plenty available for organizations worldwide to connect.

The reality is that we do forecast this a bit. The forecasts show 2018 being one of the earliest forecasts but it is a moving target. You can have a few years of increased usage that will cause that forecast to come in.

The important point here is that whether we are looking at a number of 201, 2015, there is ample time for organizations to transition to IPv6. There is not a crisis, per se. This is important to remember because the transition to IPv6 is a very challenging item. We had the prior panel discuss the planning, the business case and the security issues associated with that.

I would like to highlight the fact that we have been allocating IPv6 addresses to organizations since 1999. The Internet community is standing by ready to transition. We have the protocol done, we have the address allocation authorities done, there are test networks for IPv6. So we are ready to go. That is not a challenge.

The challenge is that you need to have a transition plan and you need to have business cases. These are very complicated for industry to form. One of the things that led in the United States to a lot more analysis of transition issues was the Department of Defense's adoption of a Statement of Migration to IPv6. That caused not only within the Department of Defense community but in the contractor community and in the vendor community, a focus on all of the issues necessary to enable this.

The reality is that is what we need, more industry involvement. This industry involvement can be achieved by involving more Fed-

eral agencies in the planning process. Per se, industry will help facilitate the transition to IPv6, but we don't need anything other than the impetus provided by more Federal planning.

As some of the largest users of IT technology, it is appropriate that Federal agencies are the ones that start the planning process as early as possible because they have large issues that are associated with their scale.

I just want to say that ARIN supports the increased involvement of more Federal agencies in this planning process. The Internet community is ready to transition to version 6. There is time to get the job done and we look forward to this committee's and the GAO's involvement in encouraging more Federal agencies to move in this direction.

That concludes my comments. Thank you and I look forward to questions.

[The prepared statement of Mr. Curran follows:]

U.S. House of Representatives
Committee on Government Reform

Testimony By:

John Curran
Chairman, Board of Trustees
American Registry for Internet Numbers ("ARIN")

Hearing on the Internet and IPv6
June 29, 2005
2:00 p.m.
Rayburn House Office Building
Room 2154

Chairman Davis, Ranking Member Waxman and Committee Members:

Good afternoon.

My name is John Curran. I am one of the founders of the American Registry for Internet Numbers (ARIN), and have served as Chairman of the Board of Trustees since ARIN's inception in 1998. I would like to thank the Committee for the opportunity to speak regarding the leadership of the United States with respect to Internet Procotol version 6 and hope that the Committee find my comments useful in their deliberations.

First, as background, ARIN is one of the five regional Internet registries ("RIRs") responsible for the management, allocation, and stewardship of number resources in the form of Internet Protocol or IP addresses. ARIN is responsible for much of the North American Region encompassing the United States, Canada, and some portions of the Caribbean. (The other four RIRs are LACNIC (South America/Mexico); APNIC (the Asia-Pacific region); AfriNIC (Africa); and RIPE (Europe). Additionally, ARIN facilitates a bottom up policy development process in which the members of the ARIN Internet community guide the formation of Internet resource allocation policies.

My involvement with the Internet and its administration actually goes back earlier to 1990; since that time I have served as the Chief Technology Officer for three Internet companies including BBN/GTE Internetworking, XO Communications, and most recently ServerVault, a secure managed infrastructure company based in Dulles, Virginia. I also served as an Area Director of the Internet Engineering Task Force (IETF) Operations and Network Management area. As a result of this background, I was selected in 1993 to serve as a member of the Next Generation Directorate of the IETF which led to formation of Internet Protocol version 6. I'd like to briefly review for the Committee the circumstances surrounding the formation of IPv6 as it is relevant to our discussions today.

In 1993, the Internet was experiencing remarkable growth due to the success of the earliest research Internet Protocol (IP) networks and the emergence of the commercial Internet marketplace. One consequence of the success was the concern that the pool of available IP version 4 addresses could be exhausted in the late 2005-2010 timeframe if the growth continued as forecasted.

As a result of this concern, the IETF formed the "IP Next Generation" (IPng) Directorate and charged it with considering requirements for the next version of the Internet Protocol. This directorate and the work of subsequent groups in the IETF led to development of the Internet Protocol version 6 (IPv6), which has larger address size and incorporates technical enhancements for security, performance, and administration. I would direct Members of the Committee to

the recent excellent GAO report (GAO-05-471) on IPv 6 for further background on the topic.

Fortunately, changes in the allocation policies for IPv4 addresses used by the regional Internet registries and the introduction of recovery efforts have further extended the availability of the IPv4 address space. At this time, the earliest estimate of the depletion of the IPv4 address space is 2018, and most estimates are further out in the 2025 timeframe. As a result, there is more than adequate time for most organizations to plan their migration from IPv4 to IPv6, and such a migration is inevitable as the IPv4 address space is finite.

The Internet community has done a remarkable job completing the tasks necessary to enable the deployment of IPv6 throughout the world including the ARIN region. The Internet Engineering Task Force (IETF) established the technical standards several years ago specifying IPv6. The Internet community has been active through research and test IPv6 networks as well as a number of information sharing forums facilitating the migration from IPv4 to IPv6. The regional Internet registries stand ready to allocate IPv6 address space to qualifying organizations and having been doing so for several years. (Please refer to attachment for details.) IPv6 allocations began in 1999 with steady growth through 2002 followed by significant growth in 2003 and 2004, particularly in the RIPE and APNIC regions. Within the ARIN region, there was a slight decline in 2004, however, during the first quarter of 2005 there appears to be a

resurgence of IPv6 allocations. In order to further promote IPv6 deployment, the ARIN Board of Trustees first waived IPv6 fees in 2001 and has continued to extend IPv6 waivers through for qualifying organizations.

While these numbers are very modest compared to the scope of today's Internet, it should be recognized that the transition from IPv4 to IPv6 is for most organizations predicated upon both a comprehensive migration plan as well as successful business case. The formation of these plans will become easier with time and with increased industry adoption of IPv6.

The promotion of IPv6 deployment in the United States would be further enhanced by leadership among federal agencies in preparing for this transition. We have already seen increased IPv6 private sector activity as a result of the United States Department of Defense which has articulated and committed to a IPv4 to IPv6 migration strategy. Having additional federal agencies begin the planning process as recommended in the GAO report would further increase industry activities in the United States, and improve the readiness of the government for this important transition. Government contractors are likely to follow this leadership.

Mr. Chairman, I would like thank you for the opportunity to speak today, and look forward to answering your questions.

NRO
IPv6 Allocations:
Regional Internet Registries to Local Internet Registries and Internet Service Providers
Yearly Comparison
AFRINIC
APNIC
ARIN
LACNIC
RIPE NCC
160
140
120
100
80
60
40
20
0
1999
2000
2001
2002
2003
2004
2005
* new and additional allocations
March 2005
Internet Number Resource Report
Number Resource Organization

Chairman TOM DAVIS. Thank you very much.
Mr. Khaki, thank you very much for being with us.

STATEMENT OF JAWAD KHAKI

Mr. KHAKI. My name is Jawad Khaki. I am the corporate vice president for Windows Networking and Device Technologies where I have worked for 16 years.

I consider it a great honor to be with the committee today. Beginning in July, I will serve on the Federal Communications Commission's Technical Advisory Council which was designed to provide the FCC with technical advice on emerging technologies.

In both this hearing today and as part of the FCC Council, my goal is to help America maintain its tradition of technological excellence and role as the global leader in information technology.

The success of the Internet today is due in large part to the efforts of the U.S. Government providing initial financial incentives including supporting academic research and Microsoft and other key industry partners providing Internet capable devices and applications.

Broadband Internet access is now commonly available worldwide and combined with the latest IP devices and services such as mobile telephones, multi-player games, voice-over Internet protocol, video conferencing, IP-based TVs are placing increasing requirements on the Internet's infrastructure. IPv6 brings relief to this strained infrastructure.

International IPv6 efforts continue to pick up momentum, as you noted most notably in Asia, specifically in Japan and China. In September 2000, the Japanese Prime Minister, Mori Yoshiro made IPv6 a Japanese national priority akin to the U.S. Government's approach to the Internet 30 years ago.

We anticipate that Japan will roll out robust, commercial IPv6 networks capable of supporting tens of millions of broadband subscribers over the next few years. Chinese and Japanese efforts are designed not only to deploy IPv6 Internet technologies but also to promote domestic industry. Domestic companies in China receive substantial government funding for their efforts. We also see similar efforts in India, Europe and other parts of the world. IPv6 adoption has proceeded slowly in the United States but is likely to accelerate as IPv6 network solutions and applications become more available, robust and affordable.

The conversion from IPv4 to IPv6 is a large task that will affect network architectures, applications, systems and operational procedures but we believe the benefits would outweigh the costs. It appears private industry efforts are working well at this stage of IPv6 planning and deployment. Companies continue to support IPv4, increasing providing IPv6 compatibility and many are preparing for an eventual transition to an IPv6 network.

It is difficult to codify an exact cost amount of either an organizational or national level IPv6 transition since the costs will depend heavily on the way entities deploy IPv6. Transition technologies provided as an inherent part of the IPv6 protocol support are in the short term the most cost effective, fastest and least disruptive way to introduce IPv6 connectivity into an existing IPv4 environment.

In the long term a full native IPv6 deployment can be achieved gradually by adding IPv6 into the network through a regular technology refreshed cycle. Microsoft understands the importance of IPv6. Our research and development teams participate in the IETF IPv6 Open Standard Activities and the next version of the Windows operating system, code-named Longhorn, will be fully IPv6 capable.

While we are working toward developing a comprehensive set of IPv6 capable applications and services, we remain acutely aware that any IPv6 deployment should be a phased transition that results in minimal infrastructure upheaval. Ultimately, Microsoft believes that marketplace dynamics with the Government being an engaged customer, will gradually lead to widespread use of IPv6 in the United States and around the world.

As we look at the Government's role, we would not recommend mandates or regulations to artificially force IPv6 deployment but rather, active political support and efforts to strengthen the domestic economy and stimulate commercial innovation.

On the academic front, U.S. Government funding of research grants and programs that provide a guiding light on evolution of the Internet should be continued. As Bill Gates stated at the Library of Congress in May, "Our universities and laboratories must be invigorated with first class research programs and thinkers to continue to blaze the technology trail."

We suggest that international efforts to stimulate adoption of IPv6 be evaluated and that the U.S. Government learn from and if appropriate, adopt some of these emerging practices. Providing economic incentive programs typically show faster results than policy recommendations alone.

U.S. Government procurement actions have a profound impact on commercial product strategy and delivery plans. Strong IPv6 support from the U.S. Government such as current efforts by DOD will only strengthen the perception that IPv6 is an important technology for American business and the public sector.

In conclusion, Microsoft is excited about the IPv6 potential to enable pervasive collaborative computing. The U.S. Government has a great opportunity to foster an environment in which we have industry and academic IPv6 thought leadership. We are eager to work with you to achieve this environment.

Thank you once again for the opportunity to speak before the committee. I look forward to answering your questions.

[The prepared statement of Mr. Khaki follows:]

Statement of Jawad Khaki

Corporate Vice President,
Windows Networking and Device Technologies
Microsoft Corporation

Testimony Before the
Committee on Government Reform
U.S. House of Representatives

June 29, 2005

Hearing on "To Lead or Follow:
The Next Generation Internet and the Transition to IPv6"

COMMENTS OF MICROSOFT CORPORATION

Introduction

Chairman Davis, Ranking Member Waxman and Members of the Committee: My name is Jawad Khaki, and I am the Corporate Vice President for Windows Networking and Device Technologies at Microsoft, responsible for the core Windows network team. I consider it a great honor to be with the Committee today, and look forward to working with the Committee to help ensure that America remains at the forefront of innovation and opportunity. Over the last decade Microsoft has worked closely with the government and our partners to help promote the growth of new, innovative Internet technologies and strengthen our domestic IT industry.

I have been at Microsoft for over 16 years, and have focused on network, software, and hardware design for the last 25 years. Beginning in July, I will also serve on the Federal Communications Commissions' Technical Advisory Council, which is designed to provide the FCC with technical advice on emerging technologies. In both this hearing today and as part of that Forum, my goal is to help America maintain its tradition of technological excellence and role as the global leader in information technology.

The current Internet Protocol, version 4 ("IPv4"), has fostered amazing growth of the Internet. Yet with the rapid growth of broadband technologies, the advent of new Internet-connected devices, and increasing concerns about the functionality and flexibility of the IPv4-based Internet, more advanced networking technologies are desirable.

A gradual, market-based conversion to IPv6 is the most technologically feasible and least disruptive way of addressing these concerns and realizing the full promise of the Internet. A strong partnership between government and industry is also critically important, as is a proactive national policy to promote IPv6.

This testimony first provides a brief historical overview of IPv4 and the significant role the government played in its creation and subsequent growth. It then highlights the successes other countries have had in promoting IPv6 development through government incentives and industry cooperation. Next, the testimony highlights why IPv6 is so important to the continued growth of our IT industry and how Microsoft is working hard to promote IPv6. The testimony concludes with a call to action for both industry and government.

A Brief Historical Perspective on IPv4 Deployment

The US government was instrumental in fostering the development and deployment of IPv4 which in turn helped propel the Internet to its current position as the main artery of communication and information sharing. Beginning in the late 1960's, the Advanced Research Projects Agency provided the funding to design and deploy the ARPANET, the predecessor to the Internet, and helped foster the development of IPv4. The National Science Foundation's support for NSFNet, a cross-country Internet backbone designed to help support government agencies, research, and educational activities, in the 1980's prompted rapid industry innovation in IPv4 networking technologies and devices.

By the early 1990's, independent commercial networks began to develop, using many of the same devices and applications produced for the NSFNet. When NSFNet sponsorship ended in the mid-1990's, the Internet's backbone and periphery networks moved into the private sector. Shortly thereafter, consumers and businesses moved quickly to the Internet, propelled by new technologies such as Microsoft's Windows 95, which supported the IPv4 protocol.

In summary, the success of the Internet today is due, in large part, to the efforts of the US government providing initial financial incentives, and Microsoft and other key industry partners

providing Internet-capable devices and applications. Throughout this period, the United States maintained a strong leadership role in the technical development of the Internet's architecture, in developing IPv4 devices and applications, and in supporting private industry growth. We firmly believe that the United States must continue this tradition of proactive leadership as we move forward in our transition from IPv4 to IPv6.

Why IPv6 is Important

The United States has benefited greatly from an IPv4-driven Internet; it has propelled our academic research, made government more efficient and responsive, and enabled both US and international companies to grow the world economy. While other countries have also benefited from the growth of the Internet, it is only recently that countries besides the United States have begun focusing on next-generation networking technologies, most notably IPv6.

The reasons for this focus on IPv6 are understandable. Over 450 million people now have access to the Internet, and close to 300 million users actively use the Internet from a personal computer at home. Broadband Internet access is now commonly available worldwide, and the latest IP-based devices and services such as mobile telephones, multiplayer games, Voice over Internet Protocol (VoIP), videoconferencing and IP-based TVs are placing increasing demands on the Internet's performance. Indeed, many of the most innovative uses of the Internet now require a combination of high-speed network connectivity, sophisticated software, and advanced networking devices. This combination is most effectively realized through an IPv6-capable Internet. Appendix A describes some of the design limitations of the IPv4 protocol and highlights how IPv6 not only mitigates these limitations, but also provides other technical

advantages, such as many orders of magnitude increase in the number of addresses available for network-connected users and devices.

International IPv6 Efforts

The most noteworthy and sophisticated IPv6 efforts outside of the United States are in Asia. Several factors have played a large role in the Asian push to move to a next-generation Internet architecture: 1) Asia has a smaller allocation of IPv4 address space than either North America or Europe, 2) Several Asian countries have deployed high-speed broadband Internet infrastructure which reaches a high percentage of their population, and 3) Advanced mobile devices and applications requiring Internet access are hugely popular among many Asian populations.

Japan is a particularly good example of active government involvement in IPv6 deployment. In September 2000, Prime Minister Mori Yoshiro made IPv6 a national priority, and by early 2001 Japan had initiated an "e-Japan" strategy that specifically called out the need for government support of IPv6 networks. Since that time, Japan has used cooperation with other Asian nations, economic incentives, policies supporting network security and consumer privacy, deregulation, and the digitization of government to help promote its IPv6 efforts to great effect. This strong push has prompted Japan's commercial sector to respond with rapid advances in network technologies and devices. We anticipate that Japan will roll out robust, commercial IPv6 networks capable of supporting tens of millions of broadband subscribers over the next few years. This Japanese effort is in many ways akin to the US government and industry partnership seen most prominently during the early development of the Internet.

In other parts of Asia, national governments are highly focused on growing their domestic IPv6 industries. For example, India's IT Ministry listed IPv6 as one of its ten IT next-generation communication and computing framework initiatives. The Chinese government created the China Next Generation Internet (CNGI) project fund to support the development of IPv6 Internet networks and support telecom operators developing IPv6 technologies. China's CERNET2 IPv6 project is designed to not only deploy IPv6 Internet technologies, but also to promote domestic industry; key suppliers of technology for this project are Chinese companies.

In addition to the ongoing Asian efforts, the European Community has supported IPv6 for several years through research and experimental network trials both regionally and with Asian countries, such as South Korea. We are increasingly seeing activity and interest from Europe's public and privacy sector, particularly with respect to military organizations.

Marketplace Forces in the US Are Working to Deploy IPv6 at an Appropriate Pace

IPv6 adoption has proceeded slowly in the United States, but is likely to accelerate as IPv6 network solutions and applications become more available, robust, and affordable. Due to the flexible nature of IPv6 from a deployment perspective, we see early IPv6 conversion activity taking place at the edge of the network such as in home computers, and gradually moving to encompass to rest of the global Internet infrastructure. Over the past 6 months, we have seen several US carriers and service providers making solid plans toward piloting and deploying IPv6 services.

While deploying IPv6 technologies offers significant promise, the conversion from IPv4 to IPv6 is a large task that ultimately will affect nearly all current IP-based network architectures, applications, systems, and operational procedures. Given the magnitude of the project and the

lack of specific deadlines, hardware and software designers, network providers, and users are generally approaching the conversion from IPv4 to IPv6 judiciously to avoid costly missteps. From our perspective, it appears that private industry efforts are working well at this early stage of IPv6 planning and deployment; companies continue to support IPv4, increasingly provide IPv6 compatibility, and many are preparing for an eventual transition to an IPv6 network.

Cost For Migrating From IPv4 to IPv6

There will be significant costs associated with migrating from IPv4 to IPv6, but we anticipate that the net benefits of the migration will outweigh these costs. These benefits are detailed in Appendix A.

However, it is difficult to quantify an exact cost amount of either an individual or national-level IPv6 transition, since the costs will depend heavily on the way entities deploy IPv6. For example, support for IPv6 transitional technologies are provided as an inherent part of the protocol, and we believe these transitional technologies are the most cost-effective, fastest, and least disruptive way to introduce IPv6 connectivity into an existing IPv4 environment. Commercial products are available today to deploy these transitional technologies.

As a second example, a full native IPv6 deployment—one that does not use transitional technologies or a hybrid IPv4-IPv6 architecture—can be achieved through gradually adding IPv6 into the network through an entity's regular technology refresh cycle. This gradual process minimizes the cost associated with rapid hardware and software upgrades. Regardless of method of deployment, there will be "soft" costs such as employee training, documentation, and other non-technology costs as part of a transition to an IPv6 architecture.

Some of Microsoft's partners have already begun building IPv6-capable networks or have made progress toward understanding what is needed to support the new protocol. This includes both international partners, as well as US agencies such as the Department of Defense.

Microsoft's Efforts to Promote IPv6-Enabled Software

We are most familiar with our own efforts to promote IPv6 and help the global Internet community move from an IPv4-based Internet to an IPv6 environment. Microsoft is not a newcomer to IPv6; we have long understood its importance and have made a strong commitment to promote its adoption. Moving forward, we are committed to supporting our customers' needs and rollout schedules for IPv6 and ensuring that our product lines support IPv6. We remain acutely aware, however, that any IPv6 deployment should be a phased transition that results in minimal infrastructure upheaval for our partners and customers.

Microsoft's research and development efforts have participated and contributed to the Internet Engineering Task Force's IPv6 standard-setting activities since 1996, when the specifications for IPv6 were still in draft form. In early 1998, Microsoft made an early version of an IPv6 protocol available to the IPv6 standards development community in the hopes of building industry consensus.

We have been incorporating IPv6 technology into our existing software for the last five years:

- In March 2000, we released a technology preview for the Windows 2000 operating system. This preview allowed software developers to familiarize themselves with the capabilities of IPv6 and to enable applications to use IPv6.

- In October 2001, we released the Windows XP operating system with a developer preview of the IPv6 protocol. We enabled key components for IPv6 so that software developers could begin enabling applications to work with IPv6 only or both IPv4 and IPv6 together.
- In March 2003, we released Windows Server 2003 with the first edition of Microsoft's IPv6 production stack and IPv6-enabled components.
- In July 2003, we released the Advanced Networking Pack for Windows XP. This release contained IP-based tunneling technology that provided the ability to provide IPv6 addresses over IPv4-based NATs.
- In August 2004, Windows XP Service Pack 2 (SP2) was released. This service pack upgraded the XP IPv6 support to be full production quality, and also included integrated IPv6 traffic support with the new Windows Firewall.
- We are currently working on delivering the next-generation Windows operating system, code-named Longhorn. Longhorn will be fully IPv6-capable. We are also working toward developing a full set of IPv6-capable applications and services during the next major product release cycle.
- In our effort to deliver Longhorn and the Longhorn-wave of IPv6-capable products, Microsoft's IT organization has taken an aggressive approach toward piloting, deploying and testing IPv6 on our corporate network. This deployment includes deploying IPv6-aware applications and hardware and IPv6 transitional technologies. These internal deployments help us gain operational experience in deploying and simultaneously running IPv4 and IPv6 technologies on our corporate network. It also allows us to extensively test our products and services prior to release to the public.

Microsoft's Commitment to IPv6 Security

Our IPv6 strategy includes a strong commitment to security. For example, we believe that every computer must be able to protect itself against attacks, even if the computer is behind a firewall in an internal network. Our belief is based on the fact that many attacks today come from inside the organization or home, whether it's from a laptop or digital media device unknowingly carrying a virus, or due to a malicious internal user. Just like we all lock the front doors to our homes even though our national borders are protected, each computer must likewise protect itself from attacks within the network. For this reason, Windows XP SP2 includes a firewall for both IPv4 and IPv6 in every computer.

As a second example, the Microsoft IPv6 implementation includes IP layer security known as Internet Protocol Security (IPSec). IPSec is an industry standard security technology that provides for data authenticity and integrity as well as data confidentiality across the array of protocols used by devices and applications.

Thirdly, we are working with our industry partners to help ensure that IPv6 security is incorporated into current and next-generation security products and services such as intrusion detection systems and firewalls.

Lastly, our existing security technologies will continue to operate in hybrid environments where both IPv4 and IPv6 are used. In order for a network environment to be fully IPv6 enabled, both the operating system and application or service must be IPv6-enabled. But in a hybrid IPv4-IPv6 environment, this will not be the case. For example, in Windows XP and Windows Server 2003, even when IPv6 is enabled on the network many applications and services will only

respond via IPv4. Under this situation, existing IPv4-based security mechanisms continue to protect the network traffic over IPv4.

The US Government's Role with Respect to IPv6 Deployment

Microsoft believes that software and hardware manufacturers will increasingly provide affordable IPv6 offerings that are attractive to the public and private sectors because of IPv6's technical merits. Thus, the ordinary operation of the commercial marketplace, which includes the government being an engaged customer, should gradually lead to widespread use of IPv6 in the United States and around the world.

In keeping with this government's role in the development and incubation of the ARPANET, NSFNet, and IPv4, we support an active and engaged government policy geared towards promoting IPv6 as the next generation networking protocol. We would not suggest mandates or regulations that favor one implementation of IPv6 over another, but we welcome efforts to strengthen our information technology economy and stimulate commercial innovation.

On the academic front, as Bill Gates stated at the Library of Congress in May, we support government funded basic research programs, including those that consider what the Internet will look like in the future. Our universities and laboratories must be invigorated with first-class research programs and thinkers to continue to blaze the technology trail. One practical way of doing this is promoting the inclusion of IPv6 in undergraduate and graduate coursework.

As noted earlier, several Asian governments and the EU are working with their commercial partners to stimulate faster adoption of IPv6. We suggest that these efforts be evaluated for consideration, particularly tax incentives and government-matched funding.

Another role that the US government can play is as a major purchaser of information technology software and hardware. US government procurement standards and requirements

have a profound impact on commercial product strategy and delivery plans. State and local governments, and even commercial entities, often base their IT purchases on the federal government. Thus strong IPv6 support from the US government, such as current efforts by the Department of Defense, will only strengthen the perception that IPv6 is a trusted, legitimate technology that should be in the future plans of American business and the public sector.

Conclusion

I sincerely hope the Committee has found these comments helpful as it evaluates the US transition from IPv4 to IPv6. Assuming continued exponential growth in both the number of devices connected to the Internet and the overall level of network traffic, IPv6 conversion is a necessary step to sustain the health and realize the full promise of the Internet. Microsoft is excited about IPv6's potential to enhance the computing and communication experiences of users around the world and hope that the US government will continue its long tradition of promoting innovation in the IT industry by supporting the development and implementation of IPv6 technologies. We look forward to working with this Committee and our partners to ensure that the US continues to be drive innovation and growth in IPv6 specifically and in our industry generally. If you need further information, I would be happy to speak before the committee at a later date or work with your staff to answer more specific questions about IPv6.

Appendix A: Overview of IPv4 and IPv6

Overview of Internet Protocol Version 4 (IPv4) and Its Weaknesses

The Internet Protocol ("IP") is the international standard protocol that defines how data is sent from one computer or device to another over the Internet. While that function sounds simple, the technical details of using and deploying IP are quite complex. In addition, because IP is fundamental to Internet connectivity, and is implemented in so many kinds of software and hardware, a change in IP is no simple task.

IPv4 was developed over 30 years ago, and has now been in use for over 20 years. During that time, the Internet has grown from a small network for a relatively few researchers and government contractors to an indispensable and nearly ubiquitous avenue of communication, commerce and entertainment for governments, educational institutions, corporations, and individuals.

This boom in Internet usage and the accompanying new demands on Internet service have underscored design weaknesses in IPv4 that are already beginning to affect the quality of service Internet users enjoy. These weaknesses include:

- *A lack of adequate address space to meet fast-growing demand.* IPv4 provides recognition of up to four billion addresses. While that number seems virtually unlimited, IP addresses have been rationed using short-term organization-specific solutions since the early 1990's. These solutions have been quite successful and have removed the appearance of IP scarcity for the average user. However, these solutions were not intended to be permanent, and the supply of addresses will face increasing pressure over time.

- *Address-conservation techniques that limit end-to-end connectivity between computers and other devices.* To make the most out of limited address space, some users have adopted workaround technologies such as Network Address Translators ("NATs"), which map a single IP address to several private addresses. However, these technologies interfere with many of today's applications, making the Internet difficult to use for many users, and also interfere with efforts to provide end-to-end security.
- *Growing numbers of addresses that burden the means of routing communications.* The Internet's routing tables and other means of routing network communications are becoming increasingly burdened and inefficient due to the sheer number of Internet addresses and the related practices for allocating these addresses. The resulting costs and delays may prove to be a larger problem than IPv4's constraints on the absolute number of available addresses.
- *The need to support new network services that did not exist when IPv4 was developed.* Technology advances and the evolution of the Internet over the last 20 years have led to new requirements in areas such as security, mobility and quality of service that IPv4's design did not take into account. While it is possible to substantially address these requirements in IPv4, such work-around solutions can be complex, costly, and inefficient.
- *A lack of integrated security.* Since IPSec was created after IPv4's standardization, many current IPv4 devices do not support IP-layer security. In addition, some elements of the IPv4 protocol such as ARP cannot be evolved to meet the security challenges posed by modern-day technologies such as wireless LANs.

Internet Protocol Version 6 (IPv6) and Its Advantages

IPv6 was designed to overcome the weaknesses of IPv4 described above, to enable new computing and communications paradigms, and to provide a flexible and operationally robust platform for future Internet growth. IPv6's advantages over IPv4 include:

- *IPv6 positions the Internet for future growth*. IPv6 increases the size of each address from 32 to 128 bits, vastly increasing the number of available addresses and virtually eliminating the need for NATs and other address-conservation techniques with their attendant disadvantages.
- *IPv6 supports end-to-end connectivity*. Because every individual device connected to the Internet will be able to have its own IP address, IPv6 promotes speed and quality of service and facilitates applications such as IP telephony and video teleconferencing. IPv6 also restores the original objective of Internet architecture to enable end-to-end communications by permitting routing of communications around failures in the network.
- *IPv6 provides a framework for end-to-end trustworthy networking*. Through built-in security and support for authentication and privacy capabilities, IPv6 promotes end-to-end trustworthy networking, and thus provides better resistance to attacks.
- *IPv6 will enable more efficient routing of network communications*. IPv6's large address space can be allocated in a hierarchical manner that reflects the current topology of the Internet. This hierarchical allocation and its better route aggregation framework should permit greater efficiency in the routing of network communications.

- *IPv6 better handles mobile applications and services.* IPv6 provides native redirection features and capabilities for facilitating device and user movement. These features better enable mobility of networked wireless services and simplify the design and construction of wireless networks. This same technology can also help the industry to develop application and services through innovative use of IP addresses.
- *IPv6 permits easier networking.* IPv6 offers a stateless autoconfiguration feature that will allow "plug and play" use of devices.
- *IPv6 enables exciting new products and services.* These features will allow developers to offer exciting IP-based applications that fundamentally change users' Internet experience.

Chairman TOM DAVIS. Thank you very much.
Mr. Barber.

STATEMENT OF STAN BARBER

Mr. BARBER. It is a distinct honor to speak to you today about the next generation Internet and the transition to Internet protocol version 6.

My name is Stan Barber, the vice president of engineering operations at Verio, Inc. Verio is one of the world's leading Internet service providers and one of several so-called Tier 1 Internet backbone providers, the networks with sufficient reach, scale and traffic to afford their customers and customers of other interconnecting networks, including U.S. Government users, global connectivity. Verio is based in Englewood, CO, and is a subsidiary of NTT Communications Corp. and an affiliate of NTT America, Inc.

The committee is to be congratulated for its focus on the next generation of Internet services. We all recognize that the Internet has become in a few short years a fundamental aspect of our economy and essential to the productivity of business and delivery of government services. To some, the term "next generation" suggests speculation about future technological developments, and wide expanses of time and opportunities to identify and address issues. However, we live on Internet time, and, "next generation" in that context means "now."

Indeed, the next generation of the Internet, IPv6, was defined as an open source, non-proprietary protocol in the 1990's and has already found its place extensively in major computer operating systems such as Windows XP and Linux and in many public and private networks around the world. I believe that my company, Verio, is the world's most experienced commercial IPv6 service provider and operates the most extensive commercial IPv6 network.

Most networks today still operate in the older IP version 4 protocol, but the transition to the later technology is essential and inevitable because of the inherent advantages built into IPv6. IPv4 does not today provide for sufficient addresses to accommodate efficiently connectivity to all potential users worldwide. IPv6, on the other hand, increases the number of directly addressable nodes exponentially. While security for IPv4 is provided where practical as a "patch," using overlay systems, IPv6 builds in high level security protections, such as secure remote node authentication and encryption, directly into the network layer, assuring more reliable and ubiquitous protection.

IPv6 generally increases flexibility and functionality with additional benefits, such as more efficient routing of traffic and more effective usage with wireless devices. The result is lower costs and improved services, like end-to-end communications and communications with devices other than PCS, something we call m2m-x communications. That is why Internet equipment manufacturers and the leading software providers, service providers and private network operators have started to transition from v4 to v6, and those that have not as yet, will inevitably find that flexibility, efficiency and security requires the conversion.

Other countries are ahead of the United States in this transition. This does not reflect any genuine technological advantage over the

United States. Indeed, it may be said that the United States continues to lead the rest of the world in Internet and related technology. Other countries have advanced to IPv6 primarily because of an initial lag in Internet development. Consequently, they have been more keenly focused on the need to address the shortage of Internet addresses and less extensive legacy networks in need of transition.

For example, the European Commission created a task force to design a plan of action for development, testing and deployment of IPv6 in 2001. The task force is coordinating efforts in individual member counties and regions and seeking cooperation with other countries.

The Chinese government has established an IPv6 network linking major universities. The government is also funding a plan to develop a more extensive IPv6 infrastructure.

Taiwan is also developing a national information infrastructure built on IPv6.

India has established the IPv6 Forum to coordinate development and implementation of IPv6.

In Japan, the home of our parent company, the government's e-Japan Strategy has been promoting the transition to IPv6 Internet. In addition, an e-Government Creation Plan facilitates the procurement of IPv6-capable devices. In the commercial sector, the IPv6 Promotion Council helps address issues related to the transition.

I have described these initiatives in other countries not to advocate any U.S. Government mandate or funding of transition to IPv6 in the private sector, but to note the clear recognition by policymakers abroad of the potential of IPv6. This committee is showing its characteristic leadership in bringing to the attention of the public the need for an effective transition from legacy Internet technologies in government and more generally.

The report of the Government Accountability Office requested by this committee demonstrates a deep understanding of the issues raised by this technological transition. The GAO offers solid recommendations to save government money and to protect against security threats.

In addition to GAO's comments, it is also useful to recognize that the transition to IPv6 need not be disruptive or costly. Verio and NTF Communications employ the so-called "dual stack" transition strategy globally in which we run simultaneous IPv4 and IPv6 systems. Use of the IPv6 system is selected where a peer has that capability; the legacy protocol is employed where the peer cannot be reached in IPv6. Thus, the transition is transparent to users and existing software and equipment.

Software and equipment that does not accommodate IPv6 can be updated in conjunction with normal upgrades or as specially designated by management. The key point is that, as recognized by the GAO report, government and private sector management should at least be surveying their essential IT operations to accommodate the inevitable transition. In this regard, the GAO and this committee are also to be congratulated for highlighting an extremely important issue of security related to on-going employment of legacy IPv4 networks in the transition to IPv6.

As I have indicated, some operating systems, including such ubiquitous systems as Windows XP, Apple's OS X, Linux and Unix-based systems, already accommodate IPv6, although they are used primarily in this country in conjunction with the legacy network protocol.

Similarly, many software applications today accommodate IPv6. Not all IT managers are aware of the potential of a grave security threat to their systems by allowing unauthorized parties access to software using "ghost" IPv6 addresses unrecognized by their systems because they are buried within IPv4 addressed packets. Or, if they are aware of the threat, they do not have the budgets and other resources to address the problem.

Even as government agencies and the private sector transition, as they must, from the legacy platform to IPv6, they must be vigilant in adapting firewalls and other equipment and software to prevent unauthorized parties from using IPv6 capabilities accessed covertly over existing IPv4 networks.

Mr. Chairman, I thank you again for the opportunity to address this committee about these critical issues of technological development and implementation, and for your leadership in identifying and making the public aware of these important matters. Verio stands ready to continue to assist the committee further in any way we can.

[The prepared statement of Mr. Barber follows:]

Statement
of
Stan O. Barber
Vice President of Engineering Operations,
Verio, Inc.

Before the
Committee on Government Reform
U.S. House of Representatives

June 29, 2005

Mr. Chairman and Members of the Committee, it is a distinct honor to speak to you today about the Next Generation Internet and the Transition to Internet Protocol version 6. My name is Stan Barber and I am the Vice President of Engineering Operations of Verio, Inc. Verio is one of the world's leading Internet service providers and one of several so-called Tier 1 Internet backbone providers, the networks with sufficient reach, scale and traffic to afford their customers and customers of other, interconnecting networks, including US government users, global connectivity. Verio is based in Englewood, Colorado and is a subsidiary of NTT Communications Corporation and an affiliate of NTT America, Inc. The Committee is to be congratulated for its focus on the next generation of Internet services. We all recognize that the Internet has become in a few short years a fundamental aspect of our economy and essential to the productivity of business and delivery of government services.

To some, the term "next generation" suggests speculation about future technological developments, and wide expanses of time and opportunities to identify and address issues. However, we live on Internet time, and, "next generation" in that context means "Now."

Indeed, the next generation of the Internet-- IPv6-- was defined as an open source, non-proprietary protocol in the 1990s and has already found its place extensively in major computer operating systems such as Windows XP and Linux and in many public and private networks around the world. I believe that my company, Verio, is the world's most experienced commercial IPv6 service provider and operates the most extensive commercial IPv6 network. Most networks today still operate in the older IP version 4 protocol, but the transition to the later technology is essential and inevitable because of the inherent advantages built into IPv6.

IPv4 does not today provide for sufficient addresses to accommodate efficiently connectivity to all potential users worldwide. IPv6, on the other hand, increases the number of directly addressable nodes exponentially. While security for IPv4 is provided where practical as a "patch", using overlay systems, IPv6 builds in high level security protections, such as secure remote node authentication and encryption, directly into the network layer, assuring more reliable and ubiquitous protection. IPv6 generally increases flexibility and functionality with additional benefits, such as more efficient routing of traffic and more effective usage with wireless devices. The result is lower costs and improved services, like end-to-end communications and communications with devices other than PCs, something we call m2m-x communications. That is why Internet equipment manufacturers and the leading software providers, service providers and private network operators have started to transition from v4 to v6, and those that have not as yet, will inevitably find that flexibility, efficiency and security requires the conversion.

Other countries are ahead of the United States in this transition. This does not reflect any genuine technological advantage over the US. Indeed, it may be said that the US continues to lead the rest of the world in Internet and related technology. Other countries have advanced to IPv6 primarily because of an initial lag in Internet development. Consequently, they have been more keenly focused on the need to address the shortage of Internet addresses and less extensive legacy networks in need of transition. For example:

- The European Commission created a task force to design a plan of action for development, testing and deployment of IPv6 in 2001. The task force is coordinating efforts in individual member counties and regions and seeking cooperation with other countries.
- The Chinese government has established an IPv6 network linking major universities. The government is also funding a plan to develop a more extensive IPv6 infrastructure.
- Taiwan is also developing a national information infrastructure built on IPv6.
- India has established the IPv6 Forum to coordinate development and implementation of IPv6.
- In Japan, the home of our parent company, the government's e-Japan Strategy has been promoting the transition to IPv6 Internet. In addition, an e-Government Creation Plan facilitates the procurement of IPv6-capable devices. In the commercial sector, the IPv6 Promotion Council helps address issues related to the transition.

I have described these initiatives in other countries not to advocate any US government mandate or funding of transition to IPv6 in the private sector, but to note the clear recognition by policymakers abroad of the potential of IPv6. This Committee is showing its characteristic leadership in bringing to the attention of the public the need for an effective transition from legacy Internet technologies in government and more generally. The report of the Government Accountability Office requested by this Committee demonstrates a deep understanding of the issues raised by this technological transition. The GAO offers solid recommendations to save government money and to protect against security threats.

In addition to GAO's comments, it is also useful to recognize that the transition to IPv6 need not be disruptive or costly. Verio and NTT Communications employ the so-called "dual stack" transition strategy globally in which we run simultaneous IPv4 and IPv6 systems. Use of the IPv6 system is selected where a peer has that capability; the legacy protocol is employed where the peer cannot be reached in IPv6. Thus, the transition is transparent to users and existing software and equipment. Software and equipment that does not accommodate IPv6 can be updated in conjunction with normal upgrades or as specially designated by management. The key point is that, as recognized by the GAO report, government and private sector management should at least be surveying their essential IT operations to accommodate the inevitable transition.

In this regard, the GAO and this Committee are also to be congratulated for highlighting an extremely important issue of security related to on-going employment of legacy IPv4

networks in the transition to IPv6. As I have indicated, some operating systems, including such ubiquitous systems as Windows XP, Apple's OS X, Linux and Unix-based systems, already accommodate IPv6, although they are used primarily in this country in conjunction with the legacy network protocol. Similarly, many software applications today accommodate IPv6. Not all IT managers are aware of the potential of a grave security threat to their systems by allowing unauthorized parties access to software using "ghost" IPv6 addresses unrecognized by their systems because they are buried within IPv4 addressed packets. Or, if they are aware of the threat, they do not have the budgets and other resources to address the problem. Even as government agencies and the private sector transition, as they must, from the legacy platform to IPv6, they must be vigilant in adapting firewalls and other equipment and software to prevent unauthorized parties from using IPv6 capabilities accessed covertly over existing IPv4 networks.

Mr. Chairman, I thank you again for the opportunity to address this Committee about these critical issues of technological development and implementation, and for your leadership in identifying and making the public aware of these important matters. Verio stands ready to continue to assist further the Committee in any way we can.

Chairman TOM DAVIS. Thank you very much.
Mr. Lightman.

STATEMENT OF ALEX LIGHTMAN

Mr. LIGHTMAN. Thank you for allowing me to share my observations on the possibilities, opportunities and challenges presented to the U.S. Federal Government by the looming and inevitable transition to Internet protocol version 6.

As the name of this hearing, "To Lead or Follow," implies, this is an urgent time for Internet leadership. The Federal Government invested the first $50 million in the first Internet, and as a result, the United States led the world in that technology.

The United States has 50 percent of the Internet service business, and the Internet has impacted thousands of industries, creating an estimated $500 billion a year in extra Federal revenues, and adding over $1 trillion in wealth via companies like Google, Yahoo!, Amazon, eBay, and hundreds of other public companies.

Similarly, the new Internet has the potential to create 10 million new American jobs and trillions of dollars in revenue for the United States, but leadership is slipping away to other countries, and it will soon be difficult, if not impossible, to recover. One company, Japan's NTT, has more IPv6 customers than all American companies combined. In fact, over 99 percent of IPv6 traffic is occurring outside of the United States. In the first Internet, we had 99 percent of all Internet traffic in the early stages. To answer your question from earlier, we are way, way, way behind the eight ball.

Japan, China, Korea, and Europe have invested over $800 million in the new Internet compared to about $8 million for the U.S. Federal Government, and are now changing the new Internet to reflect their political priorities, which are very, very different from America's political priorities, and even American laws.

I got a 300 page document from a friend of mine in Spain where they are basically trying to make IPv6 anonymous so that you can't see who is using it and doing what. In China, they have 70,000 people, 50,000 now and 20,000 about to be hired whose whole job is to scour the Internet finding people doing things they don't like and then grabbing them. These are two opposite extremes from the way America would like to do it. We would like to have peaceful, non-terrorist uses of the Internet be private but we want to be able to reach out and protect the country when we have to.

With Federal leadership in the new Internet, the U.S. Federal Government will create a service export boom, with millions of innovative new jobs, increased competitiveness for hundreds of industries, and thousands of new startups, potentially creating a booming economy. American leadership in the new Internet will also add thousands of new products vital to our military and homeland defense, better security, and underpin sustainable technological leadership for the United States.

The promise of the products and services enabled by the new Internet is huge, an affordable way to show high quality television over the Internet, a possible way to deal with spam and attacks on networks, and hundreds of applications to make American lives easier and safer.

Over $9 trillion of America's nearly $13 trillion economy relates to services, subscriptions, and transactions, and we kind of take it for granted people can't come in and grab those away from us. IPv6 will help keep the trust and keep hundreds of millions of customers loyal to American companies. If we don't show leadership in the new Internet, we get a loss of millions of jobs and market shares across thousands of companies.

This is my big concern. A loss of public trust and reputations in transactions over U.S. networks using the existing, highly vulnerable IPv4 protocol, coupled with an increase in trust of IPv6 networks in Japan, Korea, China, and the 25 nations of the European Union, could have a devastating impact on America's service economy. Internet Service Providers, telecommunications giants, banks, brokers and even our defense contractors will lose business.

Where the U.S. Government showed leadership, as we did with the post office, the interstate highway system, airplanes, lasers, radar, computer chips, and satellites, none of which would have happened if we had left it to the market, we are world leaders even decades later.

Where our Government did not show leadership, where there wasn't a Congressman Davis to hold hearings and get involved with it, including color televisions, big screens and high definition television, digital cameras, and DVDs, America plays almost no role in these and related areas, except as a consumer and our trade deficits reflect that, almost $700 billion this year, importers of food, importers of goods. God help us if we become importers of services, subscriptions and transactions. We are a follower, not a leader, in these fields. If we do not show leadership in the new Internet, this same thing will happen to us, but on a much broader basis, it will be in everything the new Internet touches, which is almost everything.

Mr. Chairman, the opportunity exists for the American Government to show leadership in the new Internet, to make a real difference for our national security and our industries and workers. By supporting the transition of the Government agencies to the new Internet standard, as the Defense Department has already started to do, we will not only support a more efficient and effective government, that is, help facilitate fundamental government reform, but will send a signal to the world that America is still a technology leader in the 21st century. And for anything as important as a new Internet standard, it will not be left behind, but will march in front, and our Coalition Partner governments will join with us and rally to our standards banner. I confirmed this at the Coalition Summit which you honored us by being the opening keynote speaker.

Mr. Chairman, there are many specific actions that your committee could take to support the promotion of the new Internet in our Government, and to support the government reform that will be possible when all of government talks with the same technical language, so to speak, with this new standard. Here are three: one, mandate IPv6 for the entire Federal Government by 2010; two, choose a leader who has the authority, responsibility, and accountability as well as the creativity, passion, and integrity, to galvanize

thousands of other leaders to get excited and committed to making the transition to IPv6 on schedule.

I point to the case of the Coalition Summit where 30 different Coalition partners, people who fight and die beside us in Iraq, said who is your IPv6 leader. We have our person in Sweden, the same person who managed the transition for the government from IPv4. Japan has their leader who reports directly to the Prime Minister in monthly meetings about this. China has its leader, Korea has its leader. Everyone has a leader but us.

Finally, enable this leader to create a Federal IPv6 Transition Office to serve as the central engine for the Federal IPv6 transition, overseeing a budget which I put this number out there 6 months ago and nobody has even taken a shot at it, of $10 billion, with the budget of FITO itself of about $50 million a year.

This office will assist in managing the complexity of an Internet transition, something we did before, in the early eighties when the Internet was only one-millionth as large as it is today. It is worth pointing out there was a protocol before IPv4 called NCP. Ten years after TCIP was introduced, the Federal Government said, we are going to get rid of this less useful protocol and we shut it off for 1 day. People howled and we shut it off for 2 days. Then we shut it off entirely.

Because of this hearing and what is set in motion, there will come a point at which we realize there is no sense having IPv4 and we will shut it off like we shut off NCP. Let us have America be the ones to determine when that shut off is rather than other countries that might stop routing our packets.

If I had to summarize what the Federal Government should know about IPv6 it would be: the transition to IPv6 has costs and benefits. The benefits far outweigh the costs. Failure to transition to IPv6 for the whole economy by 2012 will cause a loss of Federal revenues that is roughly comparable to a tax cut, with these funds flowing to Europe and Asia rather than to American taxpayers.

Thank you, Mr. Chairman and members of this committee, for your time and attention, and for the proud leadership role in technology and innovation for America that you represent.

[The prepared statement of Mr. Lightman follows:]

Testimony submitted to the Committee on Government Reform Hearing, June 28, 2005

"To Lead or Follow: The Next Generation Internet and The Transition to IPv6"

By Alex Lightman, CEO, Charmed Technology and IPv6 Summit, Inc.
1431 Ocean Avenue, Suite 600, Santa Monica, CA 90401

Mr. Chairman, honored members of this committee:

Thank you for allowing me to share my observations on the possibilities, opportunities and challenges presented to the US federal government by the looming and inevitable transition to Internet Protocol version 6, IPv6, which is also referred to as The New Internet.

As the name of this hearing, "To Lead or Follow," implies, this is an urgent time for LEADERSHIP. The federal government invested the first $50 million in the first Internet, and as a result the U.S. led the world in that technology. The U.S. has 50% of the Internet service business, and the Internet has impacted thousands of industries, creating an estimated $500 billion a year in extra federal revenues, and adding over $1 trillion in wealth via companies like Google, Yahoo!, Amazon, eBay, and hundreds of others.

Similarly, the New Internet has the potential to create 10 million new American jobs and trillions of dollars in revenue for the U.S., but leadership is slipping away to other countries, and it will soon be difficult, if not impossible, to recover. One company, Japan's NTT, has more IPv6 customers than all American companies combined.

Japan, China, Korea, and Europe have invested over $800 million in the New Internet, and are now changing the New Internet to reflect their political priorities, which are very, very different from America's political priorities, and even American laws.

With federal leadership in the New Internet, the U.S. federal government will create a service export boom, with millions of innovative new jobs, increased competitiveness for hundreds of industries, and thousands of new startups, potentially creating a booming economy.

American leadership in the New Internet will also add thousands of new products vital to our military and homeland defense, better security, and underpin sustainable technological leadership for the United States. The promise of the products and services enabled by the New Internet is huge -- an affordable way to show high quality television over the Internet, a possible way to deal with spam and attacks on networks, and hundreds of applications to make American lives easier and safer.

Over $9 trillion of America's nearly $13 trillion economy relates to services, subscriptions, and transactions, and IPv6 will help keep the trust and keep hundreds of millions of customers loyal to American companies.

If we **don't** show leadership in the New Internet, we get a loss of millions of jobs and market share across thousands of companies.

A loss of public trust and reputations in transactions over U.S. networks using the existing, highly vulnerable IPv4 protocol, coupled with an increase in trust of IPv6 networks in Japan, Korea, China, and the 25 nations of Europe, could have a devastating impact on America's service economy. Internet Service Providers, telecommunications giants, and banks, brokers and even our defense contractors will lose business.

© Alex Lightman 2005

Where the U.S. government showed leadership, as we did with the post office, the interstate highway system, airplanes, lasers, radar, computer chips, and satellites, we are world leaders even decades later.

Where our government did **not** show leadership, including color televisions, big screens and high definition television, digital cameras, and DVDs, America plays almost no role in these and related areas, except as a consumer. We are a follower, not a leader, in these fields. If we do not show leadership in the New Internet, this same thing will happen to us, but on a much broader basis -- it will be in everything the New Internet touches, which is almost everything.

Mr. Chairman, the opportunity exists for the American government to show leadership in the New Internet, to make a real difference for our national security and our industries and workers. By supporting the transition of the government agencies to the New Internet standard, as the Defense Department has already started to do, we will not only support a more efficient and effective government -- that is, help facilitate fundamental government reform -- but will send a signal to the world that America is still a technology leader in the 21st century, and for anything as important as a New Internet standard, it will not be left behind, but will march in front, and our Coalition Partner governments will join with us and rally to our standards banner.

Mr. Chairman, there are many specific actions that your Committee could take to support the promotion of the New Internet in our government, and to support the government reform that will be possible when all of government talks with the same technical language, so to speak, with this new standard. Here are three.

1. Mandate IPv6 for the entire federal government by 2010.

2. Choose a leader who has the authority, responsibility, and accountability as well as the creativity, passion, and integrity, to galvanize thousands of other leaders to get excited and committed to making the transition to IPv6 on schedule.

3. Enable this leader to create a Federal IPv6 Transition Office (FITO) to serve as the central engine for the federal IPv6 transition, overseeing a budget to be determined, and with a budget for FITO itself of perhaps $50 million. This office will assist in managing the complexity of an Internet transition, something we did before, in the early eighties when the Internet was only one-millionth as large as it is today.

If I had to summarize what the federal government should know about IPv6 it would be: The transition to IPv6 has costs and benefits. The benefits far outweigh the costs. Failure to transition to IPv6 by 2012 will cause a loss of federal revenues that is roughly comparable to a tax cut, with these funds flowing to Europe and Asia rather than to American taxpayers.

Thank you, Mr. Chairman and members of this Committee, for your time and attention, and for the proud leadership role in technology and innovation for America that you represent.

© Alex Lightman 2005

APPENDIX

I think there are ten points that could serve to justify this Committee's interest in and support of federal leadership in IPv6.

1. IPv6 has advantages for security, including authentication, mandatory IPSec (Internet Protocol Security), and Quality of Service that can, combined with intelligent policy choices, reduce a number of low-level outside attacks and may potentially help to fight spam and other parasitic uses of the Internet. IPv6 also has advantages for mobility and ad hoc networking, larger packet sizes, and a vastly larger number of addresses. Autoconfiguration also makes IPv6 easier to get started using and faster by making human configuration unnecessary. It's useful to remember that these advantages can touch the lives of 295 million Americans and their 13 million companies and 100 million homes, creating massive potential multiplier effects of these benefits.

2. The transition to IPv6 globally is inevitable, but American participation in the benefits is not. In the foreseeable future, more products will be shipped with IPv6 connections (TVs, cars, radios, PCs with MS Longhorn OS, mobile phones, toys, home appliances, cash registers, etc.) than is the case for the one billion IPv4 users today. IPv4 was made to connect mainframes and minicomputers. IPv6 was made to connect almost everything electronic, a category millions of times larger. In 1965 there were 10,000 people for every computer. By 2015 there may be 10,000 connected IT devices for every person.

3. As many as 250 different objects or systems in the average home could potentially be connected to the Internet. It's possible that Americans will be swimming in IPv6 addresses that come with their consumer electronics, white goods, electrical outlets, tools, thermostats, etc. The federal government will need to be involved at multiple levels to insure safety, interoperability between different industries, and more.

4. The federal government will need to keep tabs on the automated economy further enabled by IPv6, which could have tax, labor, legal, intelligence, and other ramifications. Machine-to-Machine Internet communications will grow at least ten times as fast as human-to-human Internet communications in the future. There is an "Internet Iceberg Effect," in that over 90% of the growth of Internet communications will not be directly observed by humans

5. IPv6 is essential to the continued expansion of wireline broadband, wireless telephony, wireless broadband, RFID, supply chain management, commercial nanotechnology, medical monitoring, digital intellectual property rights management, information sharing, and synchronization, and trade, in digital services, subscriptions and transactions

6. The rewards to early adopters of a new Internet protocol are disproportionately greater than to the later adopters. The American federal government spent $50 million on the early Internet, and receives over $500 billion in extra federal revenue as a consequence, a million-fold return every year. The U.S. federal government outspent all other federal governments combined -- by 100 to 1 -- during the early IPv4 Internet. As a consequence, the U.S. has half of the ISPs and half of the IPv4 traffic. Other governments, primarily Japan, Korea, China, and the European Union, have outspent the U.S. federal government 100 to 1 ($800 million to $8 million) in this decade. As a consequence, foreign countries currently have over 80% of IPv6 traffic -- and could potentially have 99% of IPv6 traffic by 2008 -- if they enforce their mandates and build v6 networks as planned.

© Alex Lightman 2005

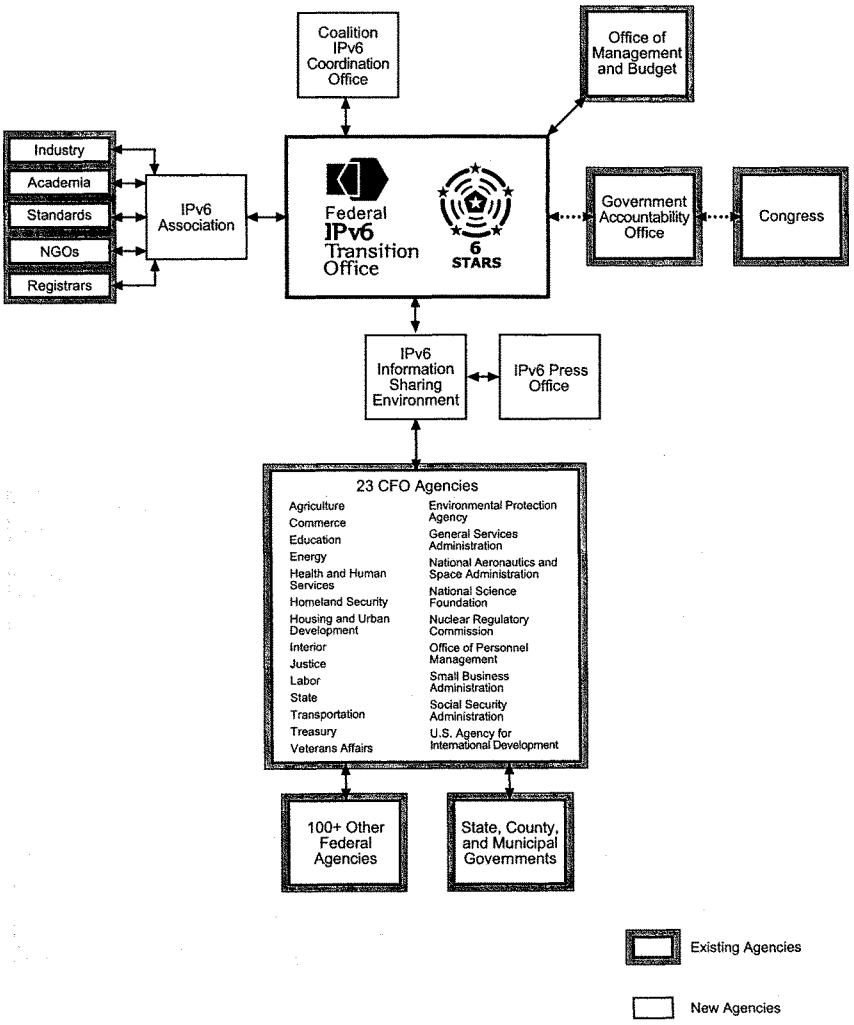
7. To lead or follow? The difference between U.S. leadership in IPv6 versus U.S. lack of leadership could be an extra $1 trillion in annual GDP and 10 million jobs in fast growing sectors, including home-based health care, security monitoring, transaction processing for banks, brokers, and insurance companies. The U.S. is a net importer in the amount of $600 to $700 billion annually of goods, as well food, capital, people, and labor. The U.S. is a net exporter, based on leadership in IT, of media, services, data, and transactions. Loss of Internet leadership could lead to being a net importer in every category.

8. The transition to IPv6 has five phases, and we are in the middle of Phase 2, acceptance. The first four phases have to do with IPv6 existence, acceptance, equivalence, and dominance. The fifth phase is IPv4 extinction, as trusted networks cease to route IPv4 packets unless they are encapsulated in IPv6 packets between trusted senders. The last time we had a similar transition co-existence, the U.S. federal government terminated all use of the old Internet Protocol (NCP) ten years after the introduction of the new Internet protocol. We are seven years into the new Internet protocol this time. The federal government needs to estimate the optimal date to make a complete switch to IPv6 and to turn off IPv4 packets as it did with NCP. The benefits of running dual protocols when IPv6 is widespread will not outweigh the costs.

9. The Chinese government deserves more attention and respect than it has received for its spectacular achievements related to information technology. China is #1 in total wireless users and #2 in broadband (after the US), and is likely to pass Japan as #1 in IPv6 users within two years, and never look back. China is engaging in Internet diplomacy by agreeing to face to face meetings with ministers of communications from Korea and Japan every six months. China could gain support from dozens of nations if it used its full diplomatic and commercial power to gather support for its own version of IPv6, starting with its own version of IPSec, since the U.S. prohibits exports of IPSec software not only from the US but also its Coalition Partners.

10. The European Union has a number of laws that require anonymity, and it is possible that, in the absence of consistent, firm, and serious U.S. leadership, Europe will make another version of IPv6, one that will reduce security by making each user virtually untraceable. The U.S. cannot assume that Europe, or any other country or group of countries, will use their leadership and investment in IPv6 the way the U.S. would.

© Alex Lightman 2005


Coalition IPv6 Coordination Office
Office of Management and Budget
Industry
Academia
Standards
NGOs
Registrars
IPv6 Association
Federal IPv6 Transition Office
6 STARS
Government Accountability Office
Congress
IPv6 Information Sharing Environment
IPv6 Press Office
23 CFO Agencies
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
100+ Other Federal Agencies
State, County, and Municipal Governments
Existing Agencies
New Agencies

Chairman TOM DAVIS. Thank you very much.

I want to thank all of you. Internet and related areas is one of the few areas where we are generating a trade surplus.

From almost unanimous testimony, it appears if nothing else, the transition to IPv6 is going to give more innovation, that is where the innovation is coming from. What are they rolling out in Japan right now in products from using IPv6 that we don't see over here? Does anybody have an answer to that?

Mr. LIGHTMAN. What they found is that first of all with building controls, they have loan way and other companies which they found they can save 29 percent of building operating costs, enough to pay for an entire building within 20 years by having each room have up to 250 controls all managed automatically by IPv6.

They installed voice over IPv6 in college dorm rooms and were giving students free calls all over the country. They have had over 800 taxicabs in Goya, Japan using IPv6 to decide where taxis should go to more efficiently pick up people. So it is involved in services, it is in cars, it is in elevators, it is in trains and there are 370 companies doing projects on IPv6. All I am talking about is the academic projects of two universities.

Chairman TOM DAVIS. Does anyone else want to add to that?

Mr. KHAKI. I would characterize the Japanese deployment to be in its early stages and the examples that Mr. Lightman gave are accurate. I think what is impressive is the investments they are making for the long term infrastructure for their country in partnership with telecommunications operators.

As I commented earlier, they are building the next generation communications infrastructure. They will deliver security services for IT as well as content services for the home. It is a longer term investment that I think is more impressive than what we are seeing in terms of early adoptions. Almost every company in Japan that creates consumer electronics devices or network infrastructure has a strong IPv6 plan and those products may position Japanese industry in much more competitive position than they would have been with IPv4.

Chairman TOM DAVIS. Mr. Barber.

Mr. BARBER. There are also a number of groups that are formed in Japan to foster the use of IPv6 in non-traditional devices as I mentioned in my testimony, non-PC communications. Those range not only from things like cell phones which already have Internet today in many parts of the United States, but to more atypical devices like you mentioned in your opening comments, refrigerators, security systems in the home.

There was a discussion about taxicabs that was mentioned earlier but they are also using it to provide real time information in the car so when you are driving from point to point, you can pick up information on the current traffic patterns or perhaps weather in the area you are about to enter, things like that. The capabilities they are exploring in Japan are extensive and they are possible because of IPv6.

Chairman TOM DAVIS. Mr. Lightman talked about the United States would be wise to mandate any transition by a certain date, 2010, and if we didn't do it by 2012, you talked about perhaps some

fairly serious economic ramifications. How do the rest of you feel about that?

Mr. Curran.

Mr. CURRAN. I think it is important to have a transition plan for every Federal agency. This is something that is necessary, a transition is inevitable and the activity of going through and building the plan to do transition on an agency by agency basis is necessary. Just going through and having that plan as we have seen the activity that has followed the DOD commitment to a migration plan and a commitment to move to IPv6 will cause industry activity within the United States.

I believe a specific date may not be required but the fact of having a plan which calls for transition and having that plan submitted by a date is a very wise idea.

Chairman TOM DAVIS. Do you think we are behind the eight ball at this point or do you think we are OK?

Mr. CURRAN. You have to recognize that my view on this is somewhat skewed because of my experience with the Internet over the last 15 years in the addressing field. I believe that it is not a question of whether or not we have to move quickly to catch up. Earlier you asked the members from Government whether or not it was important for the Government, for example, to go get its own block of IPv6 address space. That is not necessary. The address space will be there. IPv6 provides an ample address space so it will be there when agencies go to get it.

I think the more important question is that it is important to raise the awareness of IPv6 within the United States, it is important to get all of the people involved in technology, manufacture, the vendors to produce IPv6 capable products and not just know it is a switch they have to turn on but someone is going to actually turn that switch and use it.

The act of the DOD committing to version 6 caused to work out interoperability problems that would not have otherwise been found. The commitment of agencies to do the same will cause the U.S. industry to catch up on version 6.

Chairman TOM DAVIS. Does everyone who requests a block of addresses receive it?

Mr. CURRAN. The regional registries all have allocation policies that they follow for issuing those address blocks. These are set on a region by region basis. The challenge is if you meet the guidelines, you get your address space. There are applications in every region of the globe that don't meet that region's addressing policy and get turned down.

Chairman TOM DAVIS. Is that a business case you have to make to get that address?

Mr. CURRAN. It is simply showing that you have valid uses for the address space. One of the challenges we face as the stewards of the address space is ensuring that people indeed have equipment to use the addresses on. We don't want a hoarding situation.

Chairman TOM DAVIS. That is the next question. If I'm a large consumer products manufacturer and I would put IPv4 in every product I make, say $20–40 million, can I get that block?

Mr. CURRAN. That question actually came up a number of times 2 and 3 years ago. We were approached, for example, by the cel-

lular industry. The cellular industry was directed that wide scale deployment of devices with embedded addresses should look in the direction of version 6.

We are trying to make sure that the future is looking to version 6 particularly for these embedded applications.

Chairman TOM DAVIS. Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman, for your leadership on this very important issue.

The United States represents about 5 percent of the world's population and about 50 percent of its economic strength, and about 40 percent of its technological output. The U.S. leadership position is eroding as evidenced by the pervasive and growing trade deficit which is about $600 billion today, meaning that Americans who used to make things and sell them to the rest of the world are now a consumer nation. We consume about 6 percent more than we produce. This indicates there are economic troubles currently and on the horizon. It is a much different world than we dealt with ever before.

Tom Friedman, the New York Times columnist and author just wrote a book called, "The World is Flat" and in it he argues that the old vertical model, the old economic model of knowing who is on top and knowing who is on the bottom is gone, the world is flat, it is horizontal. Knowing who is up, who is down and who is emerging is much more difficult.

He argues that this is a consequence of the convergence of information technology which now makes the tools of innovation and collaboration available to all. Depending on the motivation that you bring to these tools, positive or negative outcomes are determined.

The one interesting parallel he outlines in his book in the final chapter in particular is, he says in February 1999 two airlines were started. One was started by a bright American entrepreneur by the name of David Kneitelman of Salt Lake City, UT. He financed through American banks the purchase of a whole new fleet of jets. He outsourced the pilot training to a flight school throughout the United States and he outsourced the reservation system to retirees and housewives in Salt Lake City. When you call Jet Blue, which is his airline, and make your reservation, you are talking to someone who is in their living room in Salt Lake City. He built in Jet Blue one of the most successful and financially strong airlines in the entire world.

The other airline was started in Afghanistan by Osama Bin Laden. He financed a purchase of jets through various financiers in the Middle East; he outsourced the pilot training to a flight school in Miami; and outsourced the training or planning to Ali Sheik Muhammed.

Both airlines were designed to fly into New York City, Jet Blue into LaGuardia and JFK and of course Al Queda into lower Manhattan.

The thesis of his book is a very urgent reminder of what Americans have to do in order to not only regain their economic superiority but to also stay competitive in the world so as to ensure that our national security is strong and secure as well. I don't know if you have read the book or read his column, I am curious as to what the panelists think about the thesis that Friedman outlines.

Mr. LIGHTMAN. I read the book and I think he missed trust in a big way. Recently there was a story publicized all across England. I spent the last 2 weeks in England raising money for an IPv6 fund. People said, oh, the Indians let out the bank data; well, I am never going to outsource anything to them again. So with all the stories of all the people doing things, if people can't trust your networks, and all it takes is one release of critical data, then it can cause devastation. Millions of Indians will lose their jobs or will not gain them because of the loss of trust.

As far as outsourcing, if China succeeds in putting in its own IP Sec and its own complete transparency and can track every person and everything they are doing, and you are a government that is a dictatorship, say you are one of the 100 countries in the world that doesn't have a democratically elected government, whose Internet are you going to buy? Are you going to buy it from China which has said look, we have proven we can take care of our dissidents or are you going to buy the American one which is designed that way? There are a thousand political decisions to be made and the problem for IPv6 that there has been no elected official, somebody who basically has the legitimacy as an elected official to do this.

What makes the transitions in Korea and Japan so powerful is that the people in charge of them are elected officials and they are unique in the world. That is why these hearings are so important. Outsourcing will ground to a halt if people can't believe they will be treated as honestly in India or China or anywhere else as they would be treated at home. If we lose that trust, it is worth trillions of dollars a year in our GDP.

I want to mention one other thing. We have been a Net high tech importer for the last 2 years according to Business Week, so we are not an exporter, we are an importer of high technology. This year we have become an importer of food. What is left is services, subscriptions, transactions and media. That is it. IPv6 touches all of them right at the very guts.

Chairman TOM DAVIS. We talked about mandating a transition by a certain date. Mr. Curran, you answered. I didn't to Mr. Khaki and Mr. Barber. I would also ask should the United States fund those transition efforts like other nations have done?

Mr. KHAKI. Our viewpoint is that the natural market forces would be the right kind of forces to work out the transition issues. There has to be careful thinking of the business case and the scenario planning along with all the transitional issues. So we strongly believe that the market forces will eventually lead the transition of things.

There is a role the Government has to play in terms of encouragement which I alluded to earlier in my testimony with regards to supporting the research and education sectors through procurement policies of the Government. I think those can be a good catalyst. So we believe the transition will take place left to the market forces.

Chairman TOM DAVIS. Mr. Lightman has argued for elected officials in government to take a lead.

Mr. LIGHTMAN. I explained it in an article I wrote recently which I will send you a copy, which says "Twenty Myths and Truths

about the IPv6 transition." I leave two points to let the market decide. The Department of Commerce went out and got requests for comment which said let the market handle it and they are so embarrassed about it that they won't release the report because the position is insupportable.

I will give you three examples. One, there is one man who is the primary examiner in the U.S. Patent and Trademark Office who has 150,000 patent applications as of a month ago. It is probably 160,000 today where people and companies like Microsoft, like AT&T, like many people are trying to say, I have a patent, I want exclusive use on that so no one else can use it without my permission for 20 years.

The reason the Internet works at all is because the Federal Government paid for it, didn't try to get a patent and gave it to the world. How well do we think it is going to work if we leave it to the market but leave it to 10,000 different patents, say you use this security protocol for this kind of packet, so therefore you are infringing on my patent. It is not going to work.

Chairman TOM DAVIS. I didn't want to start an argument, but I hear you.

Mr. BARBER. I believe that the transition needs to have two components to it in the United States. The Government needs to transition its own operations to support its own mission. So if the Department of Defense believes they need IPv6 by such and such a date, they should absolutely do that by whatever date that is that meets their mission objectives.

The fact there are many agencies that don't have their planning far enough along to even project dates is of concern. So it is my belief that they should all establish some very firm transition plans that include some sort of a date by which they will at least have their transition far enough along to have IPv6 operational in their networks.

Notice I didn't talk about turn off IPv4, I only talked about turning on IPv6. When you turn off IPv4, I think is a different question and has a different set of characteristics associated with that and that will be driven by really attrition, in my opinion. When do you turn IPv4 off should be an attrition driven question, not one driven by some sort of deadline.

From a market perspective, I agree there should also be market forces at work that encourage industry to deploy IPv6 as it is to their advantage. Certainly the Government will influence that by having each agency have a mission specific transition plan but I don't think we need to have some big date out there in the future where everyone has to be on version 6 everywhere in every office in the United States.

Chairman TOM DAVIS. Mr. Khaki, how are you using IPv6 in your products and services?

Mr. KHAKI. We are a Windows operating system platform provider. It was very important for us to provide platforms that would enable software innovation for scenarios that are yet to be imagined. We have had a strong commitment in IPv6. We include IPv6 support in the Windows XP operating system. Our primary focus was to enable developers to develop new kinds of scenarios and those operating systems are being used worldwide today.

For your information, we have a global IPv6 network that integrates all our development centers spread across the world. We are using the transition technologies that I mentioned earlier in achieving this connectivity. The biggest applications we see are the ones that require pervasive collaborative communications because today's limitations of added space prevent data being transmitted and created undue burden on the network.

I would like to respond to a point made earlier on intellectual property. The 30 years of leadership the U.S. Government has shown in IPv4 was important to the academic work that was done. There is a similar role the Government has to play to make sure that academic research continues so that we have good prior art, that we remain competitive, that we do encourage industry to innovate. There are incentives, commercial incentives, tax incentives, government matched funding to enable these commercial forces to work.

I think the biggest thing we will see is the Government procurement itself be a key driver. As I have been active in the IPv6 efforts since 2001 visiting Japan and China and other places, clearly the announcement by the Department of Defense in 2003 was a major event that actually made a lot of companies in the United States more aware and brought more urgency to the issue.

Chairman TOM DAVIS. What fields do you think will most directly benefit from the exploitation of IPv6?

Mr. KHAKI. If I can give you an example, you can think of the IPv4 address limitation today in some ways similar to the memory limitations in the early days of the PC. In the early days of the PC, there was a 640K memory limit. A lot of developer creativity, a lot of IT creativity enabling new capability was being used to overcome the limitation that was there using things like LEM M, EMM and High MEM. The IPv4 address space limitation is similar to that limitation that was there.

A lot of energy is being spent in drawing on new capability, IT departments and developers are working around limitations, so we are not really moving ahead, we are kind of making what we have work slowly. That would be a key benefit. Another important one is security. IP SEC is an important addition to the IPv6 protocol, it is better integrated. Those capabilities will help us build a much more secure communications infrastructure.

Besides IP SEC there is also other lower layer technologies that are in IPv6 that help IPv6 networks to be more secure than IPv4. It is important that we look at that. Things like wireless networks, LANS were not really around when the original IPv4 was invented. So there are limitations on those protocols and IPv6 addresses that.

Chairman TOM DAVIS. Let me ask this to each of you. Mr. Curran made his comment. Do you think there is no short term shortage of IP addresses in the United States?

Mr. LIGHTMAN. As Mr. Curran admitted, they don't give them to you if they don't feel they like your business plan, so it is not a market based decision. For instance, if I wanted to have 50 million addresses, say I work for General Motors, I am consultant and I want to get a block of addresses, they can say, well, we don't really like the idea of IPv4 addresses in cars, so here is the basic point.

If you don't give away the addresses, you never have a problem with them.

In any case, you can always come back and blame the United States for hoarding them because the U.S. DOD has a very large block and we could give it back, then there would be no shortage. It is not a commercial thing, it is not a market based solution. On the one hand, people say, leave it to the market but on the other hand, the market is not working in the way addresses are allocated today.

Chairman TOM DAVIS. Anyone else?

Mr. BARBER. I think for the future of the Internet application, for ubiquitous connectivity to everything, we will run into a limitation at some point. If we make the investment in trying to make this work for IPv4, we are investing in a lot of patchwork to get the same kind of innovation that we would have with IPv6 because of its native architectural features. I believe the innovation future as someone in the previous panel said from OMB, the innovation future is with IPv6, not with IPv4, regardless of the number of addresses available.

Mr. KHAKI. The way I feel about the current situation is we are making do with the limitations we have and in the process, we are slowing things down. The IPv6 address space will relieve concerns that are there and the way I think about this is restoring the hygiene, the end to end computing model on which the Internet was founded. Today the hygiene of the network is not there because you end up with these devices that prevent communications taking place end to end and a lot of breakage is an extra cost.

Chairman TOM DAVIS. Do you think the United States has the necessary infrastructure, wireless and broadband, to exploit any of the key features of IPv6 on a national level today?

Mr. KHAKI. I believe we have a good infrastructure in this country and more is being done each day. I think the work the Government did with regards to unregulated wireless spectrum was excellent. It actually has helped us deploy new capabilities with YFI. I think those are great things. There is a lot of movement in the industry around wireless technologies. That is healthy. Broadband deployment is increasing by the day. So those are good things.

I do believe that the existing version 4 Internet infrastructure is suitable also for migrating us to version 6. The way we think about this is to separate out the infrastructure migration and the application migration because oftentimes they can be thought of as a chicken and egg. Is it the chicken or the egg? By using appropriate transition technologies and using appropriate conversion tools, you can migrate either the infrastructure or the application.

Chairman TOM DAVIS. Anyone else?

Mr. CURRAN. I would like to respond to something said earlier.

To the extent an organization doesn't get an IP address space, it is because the ISPs in that region have formed policies and those policies for that region simply state these are the valid purposes for assigning them. There is no question or judgment of business plan. If a business in the Far East got turned down for address space, it is because the ISPs that make up that region came up with allocation policies to balance availability and stewardship. So there

isn't per se a shortage, we are simply enforcing the policies that the Internet providers worldwide have adopted.

Chairman TOM DAVIS. But you would agree that there comes a time when you do end up with a shortage?

Mr. CURRAN. Absolutely. In fact, as we go forward, it only makes sense to make sure the policies for allocation of address space get increasingly frugal to ensure that people know yes, you need to balance the business case between transition versus going forward on version 4.

Chairman TOM DAVIS. I get it.

Mr. LIGHTMAN. I would like to make one comment on infrastructure. The Soviet Union is still alive and well, living in American networks. There was a Russian invention which was made for people living in apartment buildings where they had one phone number for the apartment building and a phone on all ten of the floors where it would ring on every floor. The person living with that system made up something called NAT, Network Address Translation, so people say, you have Network Address Translation, good Russian technology and it enables you to take one IP address and have 100 different people use it or even go to 100 NATs and go on and on and on. So you can have a NAT behind a NAT.

Basically if you buy into that flawed argument, you don't need any IP addresses but the refutation to that is the telephone that you have. You have a number and you can see what it is. That is end to end. It is not going to an operator. The whole invention of the switch was because the guy who had a funeral home thought he was missing calls from the operator who was switching his calls.

Why are we stuck with this Soviet technology in America's networks instead of having end to end and having everyone be identified? I would love to know that everybody who went into the Internet was part of what Microsoft brilliantly calls a trusted bubble. I want for the U.S. Federal Government and all of its commercial providers of services to be inside the trusted bubble and leave the people who don't watch their hackers and want anonymity to be in the untrusted bubble.

Chairman TOM DAVIS. Plus, the rest of the world is innovating off an IPv6 model. They are getting new products off that and we are still sitting here with the Russian telephone. Is that your point?

Mr. LIGHTMAN. Yes. Also, it is important to say IPv6 is only about 20 percent finished. There are hundreds of what are called RFCs which still have to be decided on and the U.S. Government has made no more than five comments in the last decade of what it wants and doesn't want. We have checked out and gone brain dead about participating in those standards efforts.

There was one in particular the gentleman before mentioned which is the sensor nets for doing nuclear hazardous materials. That is what they are discussing right now, how do you do ultra low power, ultra low bandwidth sensors because you don't want to put a lot of power into billions of sensors. There is no government participation. There is not even any government contractor. We have just abandoned this which leaves it other governments to go and monkey with it.

Chairman TOM DAVIS. Thank you all very much. This has been a great hearing. I think other committees will be looking at this as well but we have the responsibility for intragovernment, within the Government itself as we move forward. This has been very, very helpful.

Thank you very much and the hearing is adjourned.

[Whereupon, at 12:40 p.m., the committee was adjourned.]

[The prepared statements of Hon. Jon C. Porter and Elijah E. Cummings and additional information submitted for the hearing record follow:]

CONGRESSMAN JON C. PORTER (R-NV-3)
COMMITTEE ON GOVERNMENT REFORM
"The Next Flu Pandemic: Evaluating U.S. Readiness"
June 29, 2005

Mr. Chairman, thank you for holding this hearing today. I would also like to thank the witnesses for being here today.

As stated in the Government Reform Committee's background memorandum for this hearing, history indicates that flu pandemics can be expected to occur three to four times each century. Pandemics can be devastating, as seen in the Spanish flu pandemic where 40-50 million died circa 1918, and the next pandemic could occur within the next five years. The scary fact is that, with the advent of aircraft and the vast improvement of various modes of transportation, the next flu pandemic has the potential of being even more devastating if we are not properly prepared.

With the increase in technology we have seen in recent years has come an increase in medical innovation. Flu shots have been able to keep many millions of people from falling ill; however, vaccines alone cannot stop the flu from spreading. Furthermore, last year, Americans witnessed a vaccine shortage where thousands of individuals were unable to get a flu shot. As the flu vaccine shortage showed, our government needs to be prepared on multiple levels with respect to having enough vaccines or anti-virals to sustain the American people should a flu, or other type of pandemic, occur.

Mr. Chairman, I am glad that we are holding this hearing before this year's flu season starts. I believe that last year's vaccine shortage was truly an exercise in our nation's ability to effectively produce and distribute flu vaccines. We should learn from these mistakes and ensure that our country is not left in a vulnerable position when the next flu pandemic hits.

Again, thank you for holding this hearing today, and I look forward to hearing the testimony from the witnesses.

***

Opening Statement

Representative Elijah E. Cummings, D-Maryland

Full Committee Hearing:
"To Lead or To Follow: The Next Generation Internet and the Transition to IPv6."

Committee on Government Reform
U.S. House of Representatives
109th Congress

June 29, 2005 at 2 p.m. in 2154 Rayburn

Mr. Chairman,

Thank you for calling today's important hearing examining the federal government's transition from the existing Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6 or Next Generation Internet).

In the 21st Century, the internet is central to the day-to-day operations of the federal government. Communications can now travel as fast and as far as the internet can take us. The electronic processing of information and the sharing of information can allow the delivery of services to function with unprecedented ease and effectiveness. Given the potential advantages that accompany the federal government's information technology capabilities, we must remain

committed to utilizing advancements in the internet.

Internet Protocol (IP) governs the flow of information from one user to another over the internet. IP addresses identify network devices connected to the internet and routes information from a source to a destination. The version of Internet Protocol common today is IPv4. Early internet developers created IPv4 over 3 decades ago to function with a less extensive internet in mind than the internet we have come to enjoy and expect in the 21st Century.

IPv6 was created to enhance the performance of the Internet by addressing the limitations of IPv4. IPv6 would create a tremendous increase in the number of unique IP addresses, contribute to the elimination of network address translation, improve the transmission of data such as video, and provide long-term security benefits.

Mr. Chairman, given the promise of the IPv6 I am troubled that the GAO reported that only 4 of 22 agencies have a date or goal for moving to the Next Generation Internet. We must do more to address the federal government's slow transition to

IPv6, for in doing so we take a significant step forward in increasing our effectiveness and efficiency. The American people expect that we lead in the world and not follow.

I yield back the balance of my time and look forward to the testimony of today's witnesses.

Question for the Record
for the Honorable Karen Evans
Administrator for Electronic Government And Information Technology
Office Of Management And Budget
from the Hearing Before the Committee on Government Reform
U.S. House of Representatives
On "The Next Generation Internet and the Transition to IPv6"

Question: "IPv6 raises some very broad and very serious policy issues. Some of these issues are squarely OMB issues, for example ensuring that agencies are planning for IPv6 and securing their current systems. Other issues, such as international challenges, economic competitiveness, and lack of IPv6 firewalls for classified systems, go beyond the purview of OMB and the CIO council. How is the administration organizing to address this challenge?"

Answer: These are three extremely complicated policy issues; each has far reaching ramifications in its significance. The first issue you raised is the challenge faced by our country from international competition in the realm of IPv6, and by extension, high technology communications networks. The European Union, Japan, South Korea, China, Indonesia, and India all have extensive, government funded IPv6 development and implementation programs. The nature of those programs tends to be direct government funding and coordination because all of those countries believe greater government involvement in the marketplace for IPv6 is warranted. The Administration believes the Federal government can best lead by example and serve as a catalyst for the market. We are doing this by setting June 2008 as an internal date for achieving IPv6 compatibility for Federal information systems thereby providing a reasonably large market for products and services. Such market growth will naturally stimulate an influx of funding for necessary research and development for IPv6. For example, since 1995 with a small amount of seed money, the Department of Commerce has been funding work with industry fora and commercial suppliers to remove barriers to IPv6, and IPv6 interoperable network services integrating voice, video, and data. In addition, NSF has provided some funds for work on the Domain Name System extension for IPv6.

The second issue you raised is the challenge the effect of a slow, or unmanaged, implementation of IPv6 in the Federal government may have on economic competitiveness for the United States in the world economy. The Federal government is frequently referred to as the "Fortune Zero" company of the Fortune 500 because of the economic impact of Government spending in our country, and as a result, the rest of the world. By leading through example and acting as a catalyst, the Federal government can help others see IPv6 as an underlying technology that permits innovation in areas such as transportation, communications, and entertainment.

Your last issue references the lack of IPv6 firewalls for classified networks. Today, commercially available firewall systems have limited IPv6 functionality. Within the next year at least three manufacturers are anticipated to have full-featured IPv6 capable firewalls available

(Cisco, Juniper, and Checkpoint). Firewalls are used to allow authorized information flow within a single security domain (from Internet to unclassified IP Router Network (NIPRNET) while preventing unauthorized access. However, firewalls are not used to secure classified networks. Instead, encryption devices are used to separate and secure classified networks from unauthorized access, although firewalls may be used for further protection. The DoD uses devices to encrypt classified information and for protection (separation/segmentation) of classified networks that have been approved for use by the National Security Agency (NSA). For several years the NSA has been developing High Assurance IP Encryption (HAIPE) devices. HAIPE IS version 3.0 fully supports IPv6 and all current HAIPE vendors have IPv6 support as a part of their technology roadmap.