AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBER SECURITY: THE CHALLENGES FACING OUR NATION IN CRITICAL INFRASTRUCTURE PROTECTION

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

APRIL 8, 2003

Serial No. 108–13

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

87–230 PDF WASHINGTON : 2003

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*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

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
JOHN F. TIERNEY, Massachusetts
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
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
RANDY KAPLAN, *Senior Counsel/Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
JOHN HAMBEL, *Counsel*
CHIP WALKER, *Professional Staff Member*
URSULA WOJCIECHOWSKI, *Clerk*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on April 8, 2003	1
Statement of:	
Clarke, Richard, former special advisor to the President for Cyberspace Security; Michael A. Vatis, director, Institute for Security Technology Studies at Dartmouth College and chairman, Institute for Information Infrastructure Protection; and Mark A. Forman, Associate Director, Information Technology and Electronic Government, Office of Management and Budget	9
MacLean, Rhonda, senior vice president and director of corporate information security for Bank of America, sector coordinator for the Financial Services Industry Public/Private Partnership on Critical Infrastructure Protection and Homeland Security; Robert F. Dacey, Director, Information Security Issues, U.S. General Accounting Office; and Thomas Pyke, Chief Information Officer, Department of Commerce	52
Letters, statements, etc., submitted for the record by:	
Clarke, Richard, former special advisor to the President for Cyberspace Security, prepared statement of	11
Dacey, Robert F., Director, Information Security Issues, U.S. General Accounting Office, prepared statement of	79
Forman, Mark A., Associate Director, Information Technology and Electronic Government, Office of Management and Budget, prepared statement of	33
MacLean, Rhonda, senior vice president and director of corporate information security for Bank of America, sector coordinator for the Financial Services Industry Public/Private Partnership on Critical Infrastructure Protection and Homeland Security, prepared statement of	55
Putnam, Hon. Adam H., a Representative in Congress from the State of Florida, prepared statement of	4
Pyke, Thomas, Chief Information Officer, Department of Commerce, prepared statement of	72
Vatis, Michael A., director, Institute for Security Technology Studies at Dartmouth College and chairman, Institute for Information Infrastructure Protection, prepared statement of	22

CYBER SECURITY: THE CHALLENGES FACING OUR NATION IN CRITICAL INFRASTRUCTURE PROTECTION

TUESDAY, APRIL 8, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:30 a.m., in room 2247, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam and Clay.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Chip Walker, Scott Klein, and Lori Martin, professional staff members; Ursula Wojciechowski, clerk; David McMillen, minority professional staff; and Jean Gosa and Early Green, minority clerks.

Mr. PUTNAM. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Good morning, and welcome to a series of planned hearings on cyber security, a topic that is critically important and one that has largely been neglected both in congressional debate, private sector action, and administrative action. It is a pleasure to have a distinguished panel of witnesses with us this morning.

Virtually every aspect of our lives is in some way, shape, or form connected to computers. Networks that stretch from coast to coast or around the world connect these computers to one another. In the traditional sense, we have thought of our security as a Nation in the physical—bridges, power plants, water supplies, airports, etc. Security of our physical infrastructures has been a high priority and a particularly visible priority since September 11, 2001.

The military, customs, and border patrol are charged with protecting and securing our borders. The Coast Guard protects our waterways. Federal, State, and local law enforcement officials protect our bridges, railways, and streets and provide for our own personal protection. But in this day and age, this type of one-dimensional thought is no longer adequate. Our critical infrastructure of the cyber kind must have the same level of protection if we are to be secure as a Nation from random hacker intrusions, malicious viruses, or worse—serious cyber terrorism.

There are several things unique to cyber attacks that make the task of preventing them particularly difficult. Cyber attacks can

occur from anywhere around the globe; from the caves of Afghanistan to the war fields of Iraq, from the most remote regions of the world or simply right here in our own back yard, perhaps in the bedroom of some 16-year-old who is particularly gifted in computers and electronics. The technology used for cyber attacks is readily available and changes continuously. And perhaps most dangerous of all is the failure of many people, critical to securing these networks and information from attack, to take the threat seriously, to receive adequate training, and to take the steps needed to secure their networks. I am happy to say today that all of the witnesses here are on the forefront of this war—on cyber terrorism—and I am looking forward to their insightful testimony.

In May 1998, President Clinton released Presidential Decision Directive No. 63. This Directive set up groups within the Federal Government to develop and implement plans that would protect Government-operated infrastructures and called for a dialog between Government and the private sector to develop a National Infrastructure Assurance Plan that would protect all of the Nation's critical infrastructures by 2003. The Directive has since been supplemented by Executive Order 13231, which established President Bush's Critical Infrastructure Protection Board and the President's National Strategy for Homeland Security.

Since January 2001, efforts to improve Federal information security have accelerated at individual agencies and at the Government-wide level. For example, implementation of Government Information Security Reform Act [GISRA] legislation, enacted by the Congress in October 2000 was a significant step in improving Federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. In implementing GISRA, agencies have noted benefits, including increased management attention to and accountability for information security. Although improvements are under way, recent GAO audits of 24 of the largest Federal agencies continue to identify significant information security weaknesses that put critical Federal operations and assets in each of those agencies at risk.

On December 17, 2002, the Federal Information Security Management Act [FISMA], was enacted as Title III of the E-Government Act of 2002. FISMA permanently authorizes and strengthens the information security program, evaluation, and reporting requirements established by GISRA. Among its provisions, it also requires the National Institute of Standards and Technology to develop standards that provide mandatory minimum information security requirements for Federal information security systems.

While securing Federal information systems is critical, so is securing the critical infrastructure of the Nation—80 percent of which is privately controlled. Reports of computer attacks abound. The 2002 report of the Computer Crime and Security Survey conducted by the Computer Security Institute and FBI's San Francisco Computer Intrusion Squad showed that 90 percent of the respondents, mostly large corporations and Federal agencies, had detected computer security breaches within the last 12 months; 90 percent. In addition, the number of computer security incidents reported to the CERT Coordination Center rose from over 9,800 in 1999 to over

52,000 in 2001 and over 82,000 in 2002. And these are only the attacks that are reported.

The director for CERT Centers, operated by Carnegie Mellon University, stated that he estimates as much as 80 percent of actual security incidents go unreported. In most cases, this is because either the organization was unable to recognize its systems have been penetrated or there were no indications of penetration or attack, or the organization was just reluctant to report.

Our own GAO has found a disturbing trend among Federal agencies. In both 2001 and 2002, GAO continued their analysis of audit reports for 24 major departments and agencies. The audits identified significant information security weaknesses in each that put critical Federal operations and assets at risk.

While the Federal Government and private sectors have made improvements in cyber critical infrastructure protection, there is still much work to be done. In July 2002, GAO identified at least 50 Federal organizations that have various national or multiagency responsibilities related to cyber critical infrastructure protection. The interrelationship of these organizations is vital to a successful cyber CIP strategy. These organizations also interrelate and coordinate with even more private sector organizations as well as the State and local governments.

The ability of all of these groups to communicate well, to understand the risks involved, accept common goals and minimum standards, and accept full accountability will be the keys to a successful national effort to protect the Nation's critical infrastructures and our Government networks.

This subcommittee accepts the serious nature of the oversight responsibility related to this topic, and this hearing today is simply the beginning of what will be a series of hearings that examine and measure the progress toward achieving true cyber security.

We are delighted to be accompanied by the gentleman from Missouri, the ranking member, Mr. Clay. I recognize you for any opening remarks. Thank you for joining us.

[The prepared statement of Hon. Adam H. Putnam follows:]

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

CONGRESSMAN ADAM PUTNAM, CHAIRMAN

April 8, 2003

"Cyber Security: The Challenges Facing Our Nation In Critical Infrastructure Protection."

STATEMENT OF THE CHAIRMAN

"Virtually every aspect of our lives is in some way, shape or form connected to computers. Networks that stretch from coast to coast, and, in fact, around the world connect these same computers to each other. In the traditional sense, we have thought of our security as a Nation in the physical...bridges, power plants, water supplies, airports, etc. Securing our physical infrastructures has been a highly visible priority, particularly since 9-11.

"The military, customs, and border patrol are charged with protecting and securing our borders. The Coast Guard protects our waterways. Federal, state, and local law enforcement protect our bridges, railways, and streets and provide for our own personal protection. However, in this day and age, this type of one-dimensional thought is no longer adequate. Our critical infrastructure, of the cyber kind, must have the same level of protection if we are to be secure as a Nation, from random hacker intrusions, malicious viruses or worse -- serious cyber terrorism.

"There are several things unique to cyber attacks that make the task of preventing them particularly difficult. Cyber attacks can occur from anywhere around the globe: from the caves of Afghanistan to the war fields of Iraq, from the most remote regions of the world or simply right here in our own back yard. The technology used for cyber attacks is readily available and changes continually. And, maybe most dangerous of all, is the failure of many people -- critical to securing these networks and information from attack -- to take the threat seriously, to receive adequate training, and to take steps needed to secure their networks. I am happy to say today that all of the witnesses here today are on the forefront of this war -- on cyber terrorism -- and I'm looking forward to their insightful testimony.

"In May 1998, President Clinton released Presidential Decision Directive No. 63. The Directive set up groups within the federal government to develop and implement plans that would protect government-operated infrastructures and called for a dialogue between government and the private sector to develop a National Infrastructure Assurance Plan that would protect all of the nation's critical infrastructures by 2003. The Directive has since been supplemented by Executive Order 13231, which established President Bush's Critical Infrastructure Protection Board and the President's *National Strategy for Homeland Security.*

"Since January 2001, efforts to improve federal information security have accelerated at individual agencies and at the government wide level. For example, implementation of Government Information Security Reform Act legislation (GISRA) enacted by the Congress in October 2000 was a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. In implementing GISRA, agencies have noted benefits, including increased management attention to and accountability for, information security. Although improvements are under way, recent GAO audits of 24 of the largest federal agencies continue to identify significant information security weaknesses that put critical federal operations and assets in each of these agencies at risk.

"On December 17, 2002, the Federal Information Security Management Act (FISMA) was enacted as Title III of the E-Government Act of 2002. FISMA permanently authorizes and strengthens the information security program, evaluation, and reporting requirements established by GISRA. Among its provisions, it also requires The National Institute of Standards and Technology to develop standards that provide mandatory minimum information security requirements for federal information systems.

"While securing federal information systems is critical, so is securing the critical infrastructure of the nation -- 80 percent of which is privately controlled. Reports of computer attacks abound. The 2002 report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad showed that 90 percent of the respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months. In addition, the number of computer security incidents reported to the CERT Coordination Center rose from 9,859 in 1999 to 52,658 in 2001 and 82,094 in 2002. And, these are only the reported attacks.

"The Director, CERT Centers, operated by Carnegie Mellon University, stated, that he estimates that as much as 80 percent of actual security incidents go unreported, in most cases, because (1) the organization was unable to recognize its systems had been penetrated or there were no indications of penetration or attack, or (2) the organization was reluctant to report.

"Our own General Accounting Office has found a disturbing trend among federal agencies. In both 2001 and 2002, GAO continued their analyses of audit reports for 24

major departments and agencies. The audits identified significant information security weaknesses in each that put critical federal operations and assets at risk.

"While the federal government and private sectors have made important improvements in cyber CIP, clearly there is still much work to be done. In July of 2002 GAO identified at least 50 federal organizations that have various national or multiagency responsibilities related to cyber CIP. The interrelationship of these organizations is critical to a successful cyber CIP strategy. These federal organizations also interrelate and coordinate with even more private sector organizations as well as state and local governments.

"The ability of all these groups to communicate well, understand the risks involved, accept common goals and minimum standards, and accept full accountability will be the keys to a successful national effort to protect the nation's critical infrastructures and our government networks.

"This Subcommittee accepts the serious nature of the oversight responsibility related to this topic, and this hearing today is just the beginning of what will be a series of hearings that examine and measure the progress towards achieving true Cyber security."

###

Mr. CLAY. Good morning. Thank you, Mr. Chairman, for calling this hearing. I would like to welcome the witnesses who are going to testify before us today. The issue before us today, as the chairman has pointed out, is as critical as any national security issue. Unfortunately, it is even more complex than most.

There are really two issues before us today. First, as the title of this hearing implies, we must examine the processes in place for protecting our Nation's critical infrastructures, like the telephone system, financial systems, the supply of electricity, natural gas, water, and emergency services. Second, and equally important, we must examine the security of the computer systems that run our Government from day to day.

Just last November, this committee issued a report on computer security where only 3 agencies got grades of C or above and 14 agencies failed. Some of the answers to these questions are the same. Computer security takes place in the trenches. If the man or woman sitting at the desk does not do the proper thing, then our systems will not be secure. If the system administrator does not install the proper patches when they become available, then our systems will not be secure. If the procurement officer does not examine software for security features before recommending or approving a purchase, then our system will not be secure. All of the security plans in the world will not make our systems secure unless those at the heart of the system do their job.

As we have learned, computer security has not been a priority at agencies. Over the past 4 years, Congress has steadily turned up the heat. Former Representative Horn issued a number of report cards, each one showing the situation was worse than we realized. One of the lessons from that experience was that when we asked agencies to evaluate themselves, they are often overly optimistic. Last year, the report cards, based primarily on audit report from the Inspector General, were the worst ever.

We may have turned the corner. Last year, we passed the Federal Information Security Management Act [FISMA], which is a significant step forward in setting out requirements for computer security that agencies must follow. Now we must assure that those requirements are implemented. It is my understanding that OMB has yet to issue the guidance required under FISMA. I hope that Mr. Forman will tell us that OMB has renewed its efforts to assure that the requirements of FISMA are implemented.

We have a long way to go but I believe we are on the right track to secure our Government's day to day computer system. I am not sure I can say the same thing about protecting our critical infrastructure. While I believe we are making progress in this arena, it is very slow. It has been almost 7 years since President Clinton established the President's Commission on Critical Infrastructure Protection and almost 5 years since President Clinton issued Presidential Decision Directive No. 63, to assure critical infrastructure protection. I expect our witnesses today will report on how we are progressing toward the goals established in that Directive.

What concerns me, however, is that we have entered an era where things like critical infrastructure protection and Homeland Security are being used to erode our open Government. Just last week, USA Today reported that we are facing the biggest rollback

of open Government laws since those laws were passed 30 years ago. What is tragic is that this renewed emphasis on secrecy is unnecessary. In the 19th century, the cryptographer August Kirkovs set down a principle that is the most advanced work in cryptography today: "In good systems, the system should not depend on secrecy and it should be able to fall into the enemy's hands without disadvantage." Put another way, the knowledge that American citizens are going to jump anyone who tries to hijack a plane does more to prevent hijacking than all of the secret plans at the Transportation Security Agency. If we sacrifice the fundamental principles of our society in the name of security, we have won neither security nor freedom. Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you very much.

At this time we will begin with our witnesses. All of you have been very gracious to provide thorough written testimony. As you know, we ask that you limit your oral presentation to 5 minutes. There is a light box on your table; the green light means that you may begin your remarks, and the red, we ask you to begin to sum up because the time has expired. We do have several witnesses and some panel members who are on a tight time schedule and we will attempt to be as thorough and as efficient as possible.

As you know, it is the policy of this committee that we swear in witnesses. So please rise and raise your right hands.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all of the witnesses responded in the affirmative.

I would like to begin the first panel with Richard Clarke. Richard Clarke is an internationally recognized expert on security, including homeland security, national security, cyber security, and counter-terrorism.

He has served the last three Presidents as a senior White House advisor. Over the course of a record setting 11 consecutive years of White House service, he has held the titles of special assistant to the President for global affairs, national coordinator for security and counter-terrorism, and special advisor to the President for cyber security.

Prior to his White House years, Mr. Clarke served for 19 years in the Pentagon, the Intelligence Community, and State Department. During the Reagan administration, he was Deputy Assistant Secretary of State for Intelligence. During the first Bush administration, he was Assistant Secretary of State for political-military affairs and coordinated diplomatic efforts to support the first Gulf war and the subsequent security arrangements.

Today Mr. Clark consults on a range of issues, including: corporate security risk management, information security technology, dealing with the Federal Government on security and IT issues, and counter-terrorism. Clearly, he is a well-qualified witness for this subcommittee hearing.

We are delighted to have you with us, Mr. Clarke. With that, you are recognized for 5 minutes.

STATEMENTS OF RICHARD CLARKE, FORMER SPECIAL ADVISOR TO THE PRESIDENT FOR CYBERSPACE SECURITY; MICHAEL A. VATIS, DIRECTOR, INSTITUTE FOR SECURITY TECHNOLOGY STUDIES AT DARTMOUTH COLLEGE AND CHAIRMAN, INSTITUTE FOR INFORMATION INFRASTRUCTURE PROTECTION; AND MARK A. FORMAN, ASSOCIATE DIRECTOR, INFORMATION TECHNOLOGY AND ELECTRONIC GOVERNMENT, OFFICE OF MANAGEMENT AND BUDGET

Mr. CLARKE. Thank you, Mr. Chairman, Mr. Clay. Mr. Chairman, first let me start by commending you for having this hearing and recognizing the importance of this issue. Your remarks were right on point. I am not surprised that you are on top of this issue. I recall very well that long before September 11th, you asked me when I was the Counter-Terrorism Czar to come up and brief you on al-Qaeda before most Members of the Congress knew what al-Qaeda was. So I am not surprised that you are on top of this issue before other people.

I would hope that with cyber security we could do more to raise our defenses before we have a major disaster. With al-Qaeda, unfortunately, we had to wait until we had a major disaster for people to get it and for people to act on that understanding. It would be nice if, for once, we were able to get the Congress and the administration and the corporate world to understand the issue before the disaster occurs.

The problems that we have had to date in cyber security are minor when compared to the potential. And the mistake a lot of people make is that they look at the past as a predictor of the future, that the past $17 billion a year worth of damage by cyber security they think is just a minor nuisance. Unfortunately, as long as we have major vulnerabilities in cyberspace and we do not address those major vulnerabilities, we run the potential for somebody doing us much more severe damage than has been done to date. So people who look at the cost of cyberspace security problems today and say those problems are not significant should instead be looking to the future and what could happen based on the vulnerabilities that exist.

Mr. Chairman, I have suggested in my written testimony 10 things which I think this committee and the Congress could do in general. Let me quickly go over them in the time allowed.

First and foremost, I think the Department of Homeland Security must be the focus, the location in the executive branch that has clear responsibility for cyberspace security. That is the intent of President Bush's National Strategy. Unfortunately, the department in its early days, and I admit these are early days, has not organized itself to take on that heavy responsibility, has not created a Cyberspace Security Center, has not recruited senior recognized cyberspace security experts. Until it does, we will continue to have a major problem.

Second, we still lack a Chief Information Security Officer for the Federal Government. I have the utmost respect for my friend and colleague Mark Forman, but he is not the Chief Information Security Officer. We do not have one. You would think that since Congress has given to OMB by law the responsibility for managing the IT security of the Federal agencies, except for the Defense Depart-

ment and the Intelligence Community, that they would have a large staff of people dedicated fully to this issue. They do not. And until they do, we are likely to continue to have 14 agencies getting Fs and no agencies getting better than C. No matter what laws we pass, no matter what acronyms we adopt—FISMA, GISRA—until there is a clear full-time responsible official in the White House with a full-time responsible staff that is sufficiently large and sufficiently qualified, we will not be able to implement these laws.

Third, the Congress passed last year the Cyber Security Research Act. I think it is important that authorization be matched with an appropriate appropriation this year.

Fourth, I think the committee ought to look at the mechanisms of the Internet itself, the things which are owned in common, not by the Government, not by a particular company, but the Internet mechanisms for traffic flow, all of which are highly vulnerable as was proved by the attack on the Domain Name System last year.

Fifth, I think rather than asking GAO to do periodic onsite inspections and come up with reports, GAO should be authorized by this committee to buy the devices which are now available to allow auditing and scanning of major enterprises for the 2,800 known vulnerabilities on a daily basis. The technology is deployed in the private sector. It allows companies' CEOs, COOs, on a daily or weekly basis, to see every machine in their network and to see whether or not it is fixed, whether or not it is vulnerable. GAO should have that technology and it should have it deployed in all of the major Government agencies, so you, Mr. Chairman, members of this committee can get a weekly report, a monthly report, rather than having these one-off GAO inspections every year, which are costly and which do not give you the same results as this kind of automated auditing against the 2,800 known vulnerabilities.

Sixth, the General Services Administration has put into place a Patch Management System. And as Mr. Clay said, there is a real problem in this Government with a lack of people fixing patches. That Patch Management System is a great place to invest additional dollars, the best place where we can invest in order to improve security.

Let me stop there, Mr. Chairman, as my time is up.

[The prepared statement of Mr. Clarke follows:]

Testimony of Richard A. Clarke

before the

COMMITTEE ON GOVERNMENT REFORM

Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

April 8, 2003

"MAJOR CYBERSPACE VULNERABILITIES WILL BE USED AGAINST US"

Mr. Chairman,

It is a pleasure to testify before your committee today, the first time I have testified before any Congressional committee since leaving the Federal service several weeks ago after thirty years.

Before I begin, however, I would like to pay tribute to Chairman Putnam, both for calling this hearing and for his keen interest in the security of the United States. Almost no one knows that when Congressman Putnam first came to the House, before the events of September 11th, he sought out a Special Assistant to the President for a briefing on the threats posed by al Qida at a time when many in Congress and most people in America did not know what al Qida was.

It is not surprising to me, therefore, that you are now focusing on Cyber Security, Mr. Chairman. Once again, you are seeking to understand the emerging threats to our country before they can damage us.

The Threat and the Vulnerabilities

Let me begin by talking a little bit about the threat and the vulnerabilities.

For many, the cyber threat is hard to understand. They think that these cyber attacks are unfortunate, but are just a cost of doing business; just a minor nuisance in a multi-trillion dollar economy. No one has died in a cyber attack, after all, there has never been a smoking ruin for cameras to see.

Such reasoning is dangerous. Implicit in such thinking is the unarticulated notion that the only cyber attacks that can happen in the future are those similar to what has happened in the past. Implicit is the 20th century notion that if it is not a smoldering heap with a body count, there has been no real damage.

That is the kind of thinking that said prior to September 11th that the only kind of hijacking we will ever have in the US would be the flights to Havana we had in the past. It is the kind of thinking that said we never had a major foreign terrorist attack in the United States, so we never would; Al Qida has just been a nuisance, so it never will be more than that.

The threat is really very easy to understand. If there are major vulnerabilities in the digital networks that make our country run, then someday, somebody will exploit them in a major way doing great damage to the economy. What could happen? Transportation systems could grind to a halt. Electric power and natural gas systems could malfunction. Manufacturing could freeze. 911 emergency call centers could jam. Stock, bond, futures, and banking transactions could be jumbled. If that major attack comes at a time when we are at war, it could put our forces at great risk by having their logistics system fail.

Meanwhile, short of the Big Attack, there is damage being done every day. The threat ranges from minor cyber vandalism to theft of intellectual property and personal identity, to extortion, industrial espionage, international spying, to stoppages of sales or production. The culprits range from cyber joy riders, to thieves, to organized criminals, to corporate spies, to terrorist groups, to nation states.

Several nation states, including our own, have formed intelligence and military units to exploit cyber vulnerabilities for information collection and for damaging enemies' infrastructure in future wars. They all must think there is some potential for doing serious damage to an enemy not with bombs and bullets but with bits and bytes.

I am not alone in thinking there is a serious cyber threat. Who is convinced that the threat is real and important to our national economy and national security? In 1997 a Presidential Commission of distinguished leaders concluded there was an urgent threat. A National Academy of Sciences panel reached the same conclusion. A Presidential Decision Directive and National Plan followed. Then in the Bush Administration, the President signed an Executive Order and a National Strategy on cyber security. President Bush requested an increase of 64% in cyber security spending to defend federal departments' systems in his first budget. The Congress approved it and added its own Cyber Security Research Act. The House of Representatives recently formed a Cyber Security sub-committee.

In the private sector, while spending is down, IT security spending is up. Companies are buying software and hardware to find and fix their vulnerabilities. Segments of the private sector have united to form groups to share information about cyber security and to develop best practices to prevent and recover from cyber attacks.

Every few weeks brings further evidence that there are significant vulnerabilities in our national cyber infrastructure.

In January, someone wrote a little piece of computer code. It was a simple enough task. They took a glitch in Microsoft's SQL Server software that Microsoft had warned about months before and for which Microsoft had provided a fix. Then the hacker added a couple of lines of code that would cause their little program to search the internet for systems that had not applied the fix. When the program found such "unpatched" systems, the code would use the glitch to enter the vulnerable computer, destroy files, and use the infected computer as a launch point to attack any other computer it could find.

Then the hacker hit "send."

Fifteen minutes later, over 300,000 computers were crashing. Some bank ATM machines went off line. Some routers that run computer networks flapped and were unable to send internet traffic. Some 911 call systems were hit. An airline cancelled flights. Some companies, unable to work, sent employees home. Untold millions of dollars were spent cleaning it up.

That was all the work of one hacker, exploiting a vulnerability in one company's server software that had been known for months, and which most systems administrators had fixed. But because of the high degree of interconnectedness and interdependency in cyberspace, systems in addition to servers crashed, companies that had fixed the vulnerability were hit anyway, and companies that were not even running the software were damaged.

That attack was not hard to write. And it was just one of many such attacks that have been tried in the last few years.

The vulnerability that was exploited was just one of the 2800 glitches in software that have been publicly revealed.

In addition to the January worm I discussed called "sapphire" recent months have seen the first concerted attack on the mechanisms of the internet itself, the Domain Name System servers. We have also seen the discovery of a major flaw in "Send Mail" a system used widely in government and industry.

They are just the tip of the iceberg.

People who ask "who is the threat" are to some extent missing the point. As long as there are major vulnerabilities in our cyber infrastructure, and there are many, some one will exploit them. We can not anticipate and stop every threat. We can, however, start systematically to eliminate the vulnerabilities they could exploit.

What is to be Done?

Mr. Chairman, the President issued a *National Strategy to Secure Cyberspace* in February. It was the work of thousands of Americans from all sectors of our economy. It was developed with 10 White House Town Hall meetings held around the country. A first draft of the Strategy was posted for all America to review and comment upon.

The five National Priorities and the numerous specific steps under each of those priorities are a road map for government partnership with the private sector to begin eliminating the cyber vulnerabilities.

I want to highlight ten specific steps, which I believe deserve immediate attention of the House and of this Committee.

First, the Department of Homeland Security must organize itself and recruit the personnel necessary to carry out its significant responsibilities under the President's approved Strategy. Three of the five priorities in the strategy call upon DHS to take the lead. To date, DHS has not formed a National Cyber Security Center to be the focal point for its responsibilities in this area. Nor have they recruited a cadre of nationally recognized cyber security experts. They are not currently in position to carry out their responsibilities under the President's *National Strategy*.

Second, the U.S. Government must have a Chief Information Security Officer to insure that the Federal departments secure their systems. That CISO must have executive authority to direct action by agencies. Without such an official departments will continue as they have for years, vulnerable to cyber intrusion and woefully behind in the deployment of modern IT security technology. To date OMB has attempted to perform this function with one or two people buried in their bureaucracy and an interagency committee of the CIO Council, which lacks both expertise and authority.

Third, the Congress should appropriate the funds authorized by the Cyber Security Research Act, even if the Administration does not seek the full authorization. In doing so, the Congress should front end load the multi-year $900 million with three year programs. Funds should not go to universities alone, as is the tradition with the National Science Foundation, but should be made available to the Federally Funded research and Development Centers and National Labs such as MITRE, Los Alamos, and Livermore.

Fourth, Congress should direct the implementation of a program to secure the mechanisms of the internet that are owned in common, specifically the Domain Name System (DNS) and the Border Gateway Protocol (BGP). These two systems are extremely vulnerable today and their destruction or damage could halt the internet and all associated networks.

Fifth, Congress should direct and fund the GAO to install vulnerability scanning sensors in all Federal departments' networks. Such sensors are available commercially are work well. These sensors could report daily, weekly, or monthly on which of the 2800 known vulnerabilities are present in each network. With this knowledge, the departments could eliminate the vulnerabilities. The reports of the sensors should be given to this Committee, to the Inspector Generals of the Departments so that they can carry out their legal responsibilities with regard to cyber security, to the department CIOs, and to the Department leadership.

Sixth, this Committee should direct the expansion of the Patch Management System recently created by GSA. Over 90% of detected intrusions utilize known vulnerabilities for which a fix or "patch" had already been made publicly available. The GSA Patch system makes these fixes freely available to departments on a voluntary basis. The new system should be expanded to identify when the patches have been applied (and when they have not been) and to identify in advance potential conflicts between the patching software and other widely utilized software. Expanding this program is the most cost effective expenditure that this Committee could direct.

Seventh, this Committee should require that all Federally employees utilize a Common Access Card similar to the DOD "CAC" program to log on to their computers. The CAC is a multi-factor authentication device that can replace vulnerable passwords and can permit encryption. DOD has proved it can work.

Eighth, this Committee should communicate to the Executive Branch agencies its support for increased out sourcing of IT security to Managed Security Providers (MSPs). We kid ourselves, Mr. Chairman, if we believe that most departments can operate 24 x 7 command centers to monitor intrusion detection devices and firewalls. Moreover, these systems constantly alarm and only trained experts with a synoptic view over a wide range of networks can tell the wheat from the chaff.

Ninth, the Congress should support the expansion of private sector Cyber Security Best Practices, Information Sharing, and Cyber Security Risk Management Insurance. These three elements are essential to the success of a voluntary, non-regulatory approach to private sector cyber security. To do so, Congress should, inter alia, hold oversight hearings into the

implementation of the voluntary guidelines and Best Practices developed by the FCC's National Interoperability and Reliability Council (NIRC) for Internet Service Providers (ISPs). Congress should consider cost sharing with the Information Sharing and Analysis Centers (ISACs) formed by industry groups. The Terrorism Risk Insurance Act should be examined for the role that in can play in encouraging the insurance industry to underwrite cyber security risk policies, based on Best Practices.

Finally, Mr. Chairman, the Congress should require every department to operate a Cyber Security Awareness program to train employees on the risks of poor IT security and the steps they can each take to help secure the networks. Many Federal employees do not know when they are placing their department's network at risk by their own practices. Boring lectures and employee handbooks will not suffice. Departments should employ Learning /Teaching Computer Games, contests, and other innovative techniques.

These ten steps alone are not sufficient, but they are within the power of this Committee or this Congress, and they would be a very good start. Thank you again for the opportunity to testify before this Committee.

Mr. PUTNAM. Thank you very much.

At this time we are pleased to welcome to the Subcommittee Michael Vatis. Mr. Vatis is Director of the Institute for Security Technology Studies at Dartmouth College and the Chairman of the Institute for Information Infrastructure Protection, or I3P. ISTS is a principal national center for research, development, and analysis of counter-terrorism and cyber security technology. I3P is a consortium of major research organizations, whose mission is to develop a national R&D agenda for information infrastructure protection, promote collaboration among researchers, and facilitate and fund research in areas of national priority.

Between 1998 and 2001, Mr. Vatis founded and served as the first director of the National Infrastructure Protection Center in Washington, now part of the Department of Homeland Security. NIPC was the lead Federal agency responsible for detecting, warning of, and responding to cyber attacks, including computer crime, cyber-terrorism, and cyber-espionage.

Mr. Vatis has also served in the U.S. Departments of Justice and Defense. As Associate Deputy Attorney General and Deputy Director of the Executive Office of National Security, he coordinated the Justice Department's national security activities and advised the Attorney General and Deputy Attorney General on issues relating to counter-terrorism, high-tech crime, counter-intelligence, and infrastructure protection. He is a graduate of Princeton and Harvard.

Welcome, Mr. Vatis.

Mr. VATIS. Thank you, Mr. Chairman. It is a pleasure to be here this morning to testify before you and the subcommittee along with my distinguished colleagues. I would like to wholeheartedly endorse the substance of both your own statement and that of Mr. Clay, as well as that of my colleague, Dick Clarke, because I think all of those statements summarize very well the nature of the problem and where we are today in terms of our capability to deal with an increasingly serious issue.

I would like to limit my oral remarks today to the part of my written testimony that deals with where I think the principal shortcomings are. I think it should be said that there are many good initiatives going on right now in individual agencies. And GSRA and FISMA were significant advances on Congress' part in dealing with the problem. But I think we have in some respects actually regressed in recent months in our ability to deal with this issue.

One of the areas has to do with the fact that with the dismantling of the President's Critical Infrastructure Protection Board and the Office of Cyberspace Security in the White House—Mr. Clarke's former office—there is at the moment a serious void in the executive branch's leadership. There is no central locus right now for policymaking and for coordination of efforts across all of the agencies at the policy level. I think that will significantly impede the Government's ability to move forward on this issue.

Many of the responsibilities that had been carried out by the Board and by Mr. Clarke's former office are supposed to be carried out now by the new Department of Homeland Security. But most of the officials who are supposed to take on those responsibilities have, to my knowledge, not yet been formally nominated, let alone

confirmed. And so that void is likely to continue at the leadership level for several months.

At the operational level, I think we see a similar void. Many different entities in the Government that had some responsibility for cyber security—including parts of my former organization, the NIPC; the Critical Infrastructure Assurance Office; and FedCIRC—all were moved into the Department of Homeland Security on the theory that the efforts of these organizations should be consolidated to achieve greater efficiency and effectiveness. The problem, however, is that for at least some of those entities, in fact, the consolidation is less than meets the eye.

My former organization, the NIPC, was supposed to contribute over 300 of the positions in the new department that would be focusing on intelligence analysis and infrastructure protection. In fact, though, if you examine what actually occurred, it was a transfer of vacant FTEs, not of actual people, because most of the people stayed at the FBI or found other jobs elsewhere in the Federal Government. And so, in fact, now DHS has a tall order: filling hundreds of job vacancies. And the capabilities that were built up at the NIPC over the 5-years since its inception have essentially been dismantled or ramped down considerably because of the lack of personnel. So, again, given the length of time that hiring of Federal employees takes, particularly when you add in the need for background investigations, it is my view unfortunately, that it could take over a year before we even get back to where we were in terms of our capability to detect, warn of, and respond to major cyber attacks.

The other issue I think that needs to be focused on is at the policy level: what is the Government's policy with regard to the privately owned critical infrastructures and how can it induce greater security of those critical infrastructures? Both the Clinton administration and the Bush administration, in my view, have primarily relied on what I call the "soapbox strategy," having officials—like Mr. Clarke, like myself when I was in the Government, like Mr. Forman—get up on a proverbial soapbox and talk about the seriousness of this problem and urge the owners and operators of infrastructures to take the problem seriously and do something about it. I think those efforts have been partially successful in raising awareness, in getting more attention focused on the problem. But I think at the end of the day those efforts clearly are not enough. More needs to be done.

And so I would urge this subcommittee to consider some more imaginative and more aggressive approaches; perhaps regulation modelled after HIPAA for health care providers, or the Graham-Leach-Bliley Act for financial service companies; and perhaps other, what I would call, softer approaches to incent the marketplace, to create incentives for companies to make more secure products and for owners and operators of infrastructures to take security more seriously. Rather than simply saying we do not want to regulate in this high-tech area, we should at least give serious consideration to measures that would move us beyond the soapbox strategy. Thank you very much.

[The prepared statement of Mr. Vatis follows:]

Testimony of Michael A. Vatis
Director, Institute for Security Technology Studies at Dartmouth College
and
Chairman, Institute for Information Infrastructure Protection
Before the U.S. House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

April 8, 2003

Cyber Security: The Challenges Facing Our Nation in Critical Infrastructure Protection

Mr. Chairman, Madam Vice Chair, Ranking Member Clay, and Members of the Subcommittee. I would like to thank you for the opportunity to testify before you today on the subject of cybersecurity. This issue is one that has been with us as long as we have had computers. But it has grown in importance in recent years as both our economy and our national security become increasingly dependent on the security of computer and information networks. This is not only a problem for the future. It is a very real problem right now. And though we face many other challenges to both our economic and national security today, the problem of cybersecurity is unique in its complexity and in its rapidly evolving character. I therefore applaud this Subcommittee for recognizing the importance of this issue.

In the immediate aftermath of the terrorist attacks of September 11, 2001, commentators and government officials described America's inability to detect and prevent the terrorists' plot as a "failure of imagination." No one imagined, they claimed, that terrorists would be able to hijack four airliners simultaneously and then crash three of the four into significant economic and political landmarks. No one could have predicted, the early story went, that terrorists would deviate from the normal course of hijackings, in which hostages were taken and used as bargaining chips for some political goal or in which the objective was simply to blow up the plane in order to kill its passengers.

Soon it became apparent, however, that this explanation was far off the mark. In fact, the U.S. intelligence community had ample indications that terrorists might attempt to hijack planes and turn them into guided missiles. In 1994, for instance, Algerian terrorists hijacked an Air France plane with 227 passengers and crew on board, wired it with explosives, and loaded it with three times the fuel needed to fly from Algeria to France. Their intention: to use the plane as a bomb and crash it into the Eiffel Tower. This fact was well known to U.S. intelligence agencies. Those agencies also knew as early as 1995 that terrorists – including Ramzi Yousef, the mastermind of the first World Trade Center bombing – had planned to crash a private aircraft into the CIA Headquarters building in Langley, Virginia. And FBI agents knew for years that suspected terrorists were taking flying lessons in the United States. By August 2001, some agents and CIA

officers had come to believe that some of these student pilots might be plotting airline suicide attacks.

Our Nation's vulnerability to such attacks was also apparent. It was clear for years before September 11 that weapons could easily be smuggled onto passenger planes, and that airplanes could be flown into sensitive airspace. Indeed, in 1994 a man crash-landed a stolen Cessna on the South Lawn of the White House grounds.

So, the events of September 11 were not unimaginable at all. The vulnerabilities were evident to anyone who paid attention, and the intentions of terrorists to commit acts similar to those that occurred on 9/11 had already been demonstrated. We just failed to take the necessary precautions – such as treating intelligence about suspected terrorists' flying lessons more seriously or adequately beefing up airport security to make smuggling a weapon on board a plane more difficult.

September 11 thus reminded us of a painful lesson: that we as a Nation – not just our law enforcement and intelligence agencies, but the entire Executive Branch, Congress, the news media, and the public – too often fail to treat new threats seriously and take the necessary steps to deal with them until after those threats have manifested themselves, often in catastrophic fashion. It has proven to be too difficult to muster the political will, avoid the distraction of more immediate concerns, and focus the attention of enough government officials or public opinion makers on such problems unless and until a major attack takes place and causes a significant loss of life or major economic disruption.

The Nation's response to the possibility of cyber attacks is in some ways an even more glaring example of this problem. For in the cyber arena, not only can we *imagine* serious cyber attacks based on the conjunction of our network vulnerabilities and the known intentions of would-be attackers, but we've actually *experienced* such attacks for over a decade. As long ago as the 1980s – ancient history in the Internet Age, when many of today's younger hackers were still in diapers – we saw the "Morris Worm" wreak havoc on the early Internet as it spread from computer to computer and caused victimized systems to cease functioning. We also saw the first known instance of cyber espionage, as West German hackers stole information from U.S. military networks and sold it to the Soviet KGB – an episode immortalized in Clifford Stohl's book, *The Cuckoo's Egg*. And throughout the 1990s and into the early 21st century, we have witnessed a steady escalation in the number and severity of attacks – ranging from politically motivated defacements or obstructions of government and private company websites; to Denial of Service Attacks against e-commerce and online news sites and Internet domain name root servers; to destructive worms and viruses that have caused significant harm to companies around the world; to intrusions by organized criminal groups into university and company networks for the sake of stealing proprietary information, credit card numbers, or money or to extort the system owner; and to intrusions into government networks to steal sensitive information. These attacks demonstrate not only that our information networks remain vulnerable to attack, but also that myriad bad actors are willing and able to exploit those vulnerabilities.

Moreover, publicly available information demonstrates that at least several foreign nation states have developed information warfare programs that could be used to target vital U.S. systems in the event of military conflict. Indeed, the Director of Central Intelligence has testified to this fact several times over the last five years. And news reports confirm what has long been feared – that al Qaeda has at least thought seriously about engaging in cyber attacks, and may have mapped out potential targets within America's critical infrastructures. Thus, while we have not yet – to our knowledge at least – experienced an actual instance of "cyber terrorism" or "information warfare" against the United States, if anything the indicators warning of the risk of such attacks vastly exceed the indicators that existed prior to September 11, 2001 of an aerial assault on the World Trade Center and Pentagon.

For many years, skeptics have pooh-poohed the cyber threat by saying that the only real threat comes from American teenagers joyriding on networks or engaging in the cyber equivalent of vandalism, or that the government has over-hyped the problem in order to invent new missions in the Post-Cold War world. But if kids can crash networks through denial of service or worm attacks or obtain system administrator level control of military or commercial networks, as we've seen on numerous occasions, surely it stands to reason that a sophisticated, and well funded, foreign military or intelligence organization or a terrorist group could accomplish the same – and much worse.

Of course, to say that cyber networks are vulnerable does not mean that the critical infrastructures that rely on those networks – such as electrical power grids, pipelines, telecommunications switching nodes, hospitals, etc. – are necessarily vulnerable, or that a cyber attack would have a sufficiently long-lasting, destructive impact to achieve a terrorist's or nation state's military or political objectives. We still do not actually know the full extent of our critical infrastructures' vulnerabilities to various types of cyber attacks and the extent of their potential impact. But it is clear at the least that computer networks themselves can be intruded into; that information can be stolen or altered in ways that could profoundly affect public confidence or the economy; that network functionality can be halted or degraded through denial of service attacks or the implantation of malicious code; and that reliant infrastructures can be impeded at least temporarily. The threat is real – we just don't yet understand the full scope of it, in part because of the complexity of infrastructures' reliance on networks and of the interdependencies among critical infrastructures. And we shouldn't wait for a major infrastructure attack to occur before we take steps to truly *learn* the full scope of our vulnerability, and to begin shoring up our weaknesses.

Yet, the willingness of both the government and the private sector to dedicate the attention and resources necessary to deal with the problem effectively has lagged. To its credit, the federal government did begin, in the mid 1990s, to take the cyber threat seriously and initiate efforts to address it. After commissioning both an internal group and a joint public-private commission to study the problem, the Clinton Administration issued Presidential Decision Directive (PDD) 63 in 1998, which set out the first federal policy framework and created new government and public-private structures to address

our vulnerability to cyber attack. In 2000, the White House issued the National Plan for Information Systems Protection, the first comprehensive strategy to deal with this issue. The Bush Administration built on these efforts with the creation of the President's Critical Infrastructure Protection Board in 2001 and the issuance of a National Strategy to Secure Cyberspace in February 2003.

Despite the government's early grasp of the issue, however, its proposed solutions have not kept pace with the fast growth of the problem. Many of its initiatives have never received adequate funding to accomplish their assigned tasks. Government agencies' efforts to secure their own networks have consistently received failing marks from congressional watchdogs, including in the most recent report by the General Accounting Office. And funding for research and development of cybersecurity technologies has remained, in Representative Sherwood Boehlert's phrase, a "backwater."

After September 11, this situation appeared to be changing, apparently as a result of the vastly increased concern about *all* threats to our domestic security. Funding for some government cybersecurity activities has begun to increase. And research and development for cybersecurity appears to be poised for significant funding increases, perhaps by FY 2004, if actual appropriations match the authorization of funding increases in the Cyber Security Research and Development Act, which was signed into law last November.

But recent events seem to indicate that the government's efforts in this area are seriously regressing. First, with the dismantling of the President's Critical Infrastructure Protection Board (PCIPB) and the White House Office of Cyberspace Security, there is now a gaping void in the Executive Branch's leadership. There is no longer any central locus for cyber security policymaking, for implementation of government-wide initiatives, or for outreach to private industry. These functions are now supposed to be carried out mainly by the new Department of Homeland Security. But the positions responsible for these tasks – including the Undersecretary for Intelligence Analysis and Infrastructure Protection (IAIP), and the Assistant Secretaries for Intelligence Analysis (IA) and for Infrastructure Protection (IP), have not yet been formally nominated, let alone confirmed by the Senate. (In March, President Bush announced his intention to nominate Frank Libutti for the Undersecretary post, Paul Redmond for Assistant Secretary for IA, and Robert Liscouski for Assistant Secretary for IP, but has not actually nominated any of them yet.) The sooner these positions are filled, the quicker the DHS can begin aggressively addressing the cybersecurity part of its mission.

Even when these positions are filled, though, there will be no office responsible solely for cybersecurity policy and coordination. Rather, the Administration apparently intends to treat cybersecurity solely as a component of the broader "critical infrastructure problem," which includes vulnerability to physical terrorist attacks. Given the effort and attention being given to the risk of physical attack during the ongoing "war on terrorism," it seems quite likely that the lack of an office dedicated to cybersecurity will lead to that issue's getting short shrift. Rumors continue to float around Washington that Howard

Schmidt, the former Vice Chair of the PCIPB and a widely respected expert in the field, is being considered as a "special advisor" on cybersecurity to Secretary Tom Ridge. But no decision has yet been made, and even this position would apparently lack any "line authority" within the Department, and so would not adequately solve the problem.

These changes themselves suggest that the Administration has purposely reduced the level of priority it is devoting to cybersecurity policy – despite the expected protestations to the contrary. The uncharacteristically quiet manner in which the National Strategy to Secure Cyberspace was released (on Friday, February 14) – in contrast to the public trumpeting of the initial draft of the plan in September 2002 – seems to confirm this suspicion.

A second area of regression has to do with the loss of operational capability, particularly in the areas of detection, analysis, and warning of cyber threats. Last month, several government entities responsible for some aspect of cybersecurity were transferred to the new DHS, including: the parts of the National Infrastructure Protection Center responsible for analysis, warning, and outreach (the investigative arm of the NIPC remains at the Federal Bureau of Investigation); the Critical Infrastructure Assurance Office (CIAO); the National Communications System; the National Infrastructure Simulation and Analysis Center; the Energy Assurance Office; and the Federal Computer Incident Response Center (FedCIRC). On its face, this consolidation should improve the government's ability to gather, analyze and disseminate information regarding vulnerabilities, threats, and incidents, and to engage with private industry. And it may do so in time. But it appears that at least some of the consolidation involves less than meets the eye.

For example, with the transfer of most of the NIPC to DHS, over three hundred *positions* were moved from the FBI to DHS. Yet, because most of the actual *people* filling those positions found other jobs at the FBI after the DHS was first proposed, only about 10-20 personnel have actually made the move. Thus, for the most part, it is vacant "FTEs" (full-time equivalents) that have been transferred to DHS, not analysts ready to hit the ground running. What this means is that the DHS's capacity to collect information on cyber threats, analyze the information, and issue warnings is going to be seriously lacking – despite the valiant efforts of the people at DHS now – until hundreds of jobs are filled, senior leadership is in place, and the new structure of the IAIP directorate is worked out and responsibilities assigned. Given how long government hiring usually takes, especially with the necessity of background investigations, it could take a year, or considerably more, for the DHS even to get back to the level of functionality that the NIPC had achieved in its five years of existence. Given that the number and severity of cyber attacks continues to increase, this regression in our warning, analysis and response capability is troubling.

In another major respect, the government's efforts have not regressed, but also have not progressed sufficiently given the magnitude of the problem. When it comes to addressing the myriad vulnerabilities in the privately owned systems that constitute the bulk of the Information Infrastructure, the government continues to rely essentially on what I call the "soapbox strategy": warning of the urgency of the problem, urging

hardware and software manufacturers to make more secure products, and cajoling owners and operators of critical business networks and utilities to devote more attention and resources to their own cybersecurity. Over the last five years, the government has consistently and vociferously rejected any talk of regulating vendors or users. And while it has not completely dismissed the notion of creating market incentives to enhance security, it has not encouraged such measures either.

The National Strategy to Secure Cyberspace continues in this vein. While it recognizes "vulnerability reduction" as part of one of its five priorities, the *means* it proposes to employ to achieve those reductions are essentially the same as those of the last Administration – urging "public private partnerships" to share information about threats and vulnerabilities and develop "best practices" for cybersecurity; and promoting research and development of more secure information systems. The strategy contains many good ideas. But I am afraid that without a more imaginative, and aggressive, set of strategies to implement them, they are likely to remain only ideas.

Good arguments can be, and have been, made against direct government intervention in this fast-moving, high-tech area. But it seems clear after more than five years that the "soapbox" strategy is not sufficient – and I say this as a veteran "soapboxer." Vulnerabilities in software persist. Attacks continue to increase. And the possibility of a significant attack by a sophisticated adversary – whether a nation state, a terrorist group, or a criminal group – remains, and in fact is growing as existing and potential future adversaries develop cyber attack capabilities. Clearly more is needed to secure our vulnerable systems. The question is what.

During the course of 2002, the Institute for Information Infrastructure Protection (I3P), a consortium of 23 leading academic and not-for-profit cybersecurity R&D organizations, hosted a series of workshops with software and hardware manufacturers, researchers, large corporate users, infrastructure owners and operators, and government officials to gather input for a national cybersecurity R&D agenda. During those workshops, which were focused largely on technical requirements and technology R&D priorities, it was striking how often experts from all of the communities stressed the need for changes in the legal, policy, and economic environment that affects cybersecurity. Without such changes, these experts asserted, advances in technical R&D would never suffice, because there would not be an adequate market for more secure products and for new security technologies.

Of course, a catastrophic cyber attack that affected numerous entities could quickly create such a market. But the goal should be to *avoid* such an attack, not wait for one to induce market forces. The question, then, is what measures can be taken to create or encourage a market for security – one that results in manufacturers making more secure products and owners of critical networks operating their networks more securely.

At the very least, research is needed to understand better the nature of the security market and the forces that affect it today and that are likely to affect it tomorrow as business transactions continue to migrate to the Internet. We must start with a clear

assessment of the risks and economic costs that stem from cyber insecurity. Again and again during the I3P agenda development process, we heard that corporate executives and government officials lack a solid understanding of the true nature of the risk to their enterprises, including the potential costs of various types of attacks, and of the costs and benefits of varying levels of security that they could implement. Cost-benefit calculations are therefore extremely difficult and often forsaken altogether.

Beyond that, we need a better understanding of the potential levers that the federal and state governments could use to improve the state of security. This is, of course, where Congress can play a critical role. Direct regulation is of course one possibility. And indeed, like it or not, some regulation is already occurring, though in limited or indirect ways. In the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act, for example, Congress imposed on health care providers and financial services firms, respectively, general requirements to take steps to ensure the security of their electronic systems. These measures were passed not out of a concern for security per se, but out of concern for protecting the privacy of patient and customer records stored on companies' networks. But the effect on the companies is the same as a regulation of security for security's sake. In addition, the Federal Trade Commission brought unfair trading practice actions against – and reached settlements with – Microsoft and Eli Lilly, claiming that both had misled consumers by not having in place security measures sufficient to live up to their promises about the security and privacy of customer information. Both settlements required the companies to institute security measures, and the FTC's actions can be viewed as setting de facto security standards for companies that handle consumer information. Finally, a new California law (effective July 1, 2003) requires entities conducting business in California to disclose computer security breaches if the breaches result in unauthorized access to California residents' unencrypted personal information (such as account, credit card, driver's license, or social security numbers). The law also provides for a civil damage action by injured customers against businesses that violate the new law. This law is likely to have broad national impact in light of the number of companies that "conduct business" in California. These varying approaches can be seen as experiments in regulation that might have broader applicability. At the very least, study is required to determine their efficacy in improving security, and their costs.

Consideration should also be given to "softer" approaches designed to foster greater security without stifling technical innovation. These might include tax incentives to increase network security expenditures; legislation to create or enhance liability on the part of manufacturers or network operators for negligent actions or omissions that harm others; insurance requirements or incentives for security investments; requirements for public companies to include a discussion of potential cyber risks or actual security breaches in their annual Form 10-K disclosure, in order to promote CEO and Board attention to security (similar to the approach utilized by the SEC to address Y2K concerns); and general standards or best practices for hardware and software manufacturers or certain critical industries. Rather than simply dismiss these types of approaches out of hand, we should acquire a solid understanding of their pros and cons and then pursue the best options.

Finally, the public discussion and understanding of the problem of cybersecurity would greatly benefit from more precision in terminology. For instance, "cyber terrorism" should not be used to describe run-of-the-mill web site defacements, network intrusions, or even denial of service attacks. That term at most should be reserved for truly destructive cyber attacks that cause death, injury, significant economic loss, or significant disruption of a critical infrastructure, and that are motivated by a desire to coerce or intimidate a government or civilian population in pursuit of some political, religious, or ideological end. To call even low-grade, routine attacks cyber terrorism risks losing credibility with company executives, government officials, and the general public – the very people from whom concerted action is needed. And we need to be careful to distinguish among the various forms of cyber attacks – whether they be cyber extortion, cyber vandalism, cyber theft, cyber espionage, cyber terrorism, or information warfare. Some of these already occur on a daily basis (like cyber theft and vandalism); some are undoubtedly occurring but are not known publicly, or perhaps even by our intelligence agencies (such as cyber espionage); and some have not yet occurred but are a distinct possibility (such as cyber terrorism and information warfare). And when we're not yet sure how to characterize an attack, we should simply refer to it as a "cyber attack" until sufficient information is available to understand the nature of the attack and the motivation of the attacker.

Conclusion

Cyber attacks are a real and growing threat. As the most information technology-dependent country in the world's history, we remain uniquely vulnerable to cyber attacks that could disrupt our economy or undermine our security. And yet our response as a society is still stuck in second gear. If we are to deal with this problem effectively, no options should be taken off the table merely because of fears of political opposition or the daunting complexity of the task. Serious study and consideration should be given to measures that could positively influence the legal, policy, and economic environment in which information technology is deployed so that our vulnerabilities can be minimized as efficiently and effectively as possible, without inhibiting technological innovation.

Mr. PUTNAM. Thank you very much.

Our next witness is Mark Forman. Mr. Forman is the Chief Information Officer for the Federal Government. Under his leadership, the U.S. Federal Government has received broad recognition for its successful use of technology and E-Government. He is charged with managing over $58 billion in IT investments and leading the President's E-Government initiative to create a more productive, citizen-centric Government.

He is also the leader in the development and implementation of the Federal information technology policy, and is responsible for a variety of oversight functions statutorily assigned to the Office of Management and Budget. He also oversees Executive branch CIOs and directs the activities of the Federal CIO Council, as well as chairing or being a member of several key IT-related boards including the President's Critical Infrastructure Board. To improve results from Federal IT spending, Mr. Forman created a framework that couples cross-agency teamwork and leadership with a Government-wide IT budget decision process built around a results-driven modernization blueprint.

Mr. Forman is a frequent witness before this subcommittee and his insight is always very helpful. We are delighted to have you again with us this morning. Welcome.

Mr. FORMAN. Thank you, Mr. Chairman. Good morning. I want to take a moment just to commend Mr. Clarke on what I think is a truly outstanding career in public service that, as you know, he has recently retired from. I think his career serves as really a benchmark for those of us in public service. Clearly, his dedication to the country, the security of Americans is remarkable and outstanding, and as an American and personally, I just appreciate his service so much.

I want to thank you for inviting me to discuss the status of the Federal Government's IT security. Cyber security is a top priority in the administration's IT and counter-terrorism efforts. The challenge, as you pointed out, is to provide the maximum protection while ensuring the free flow of information and commerce and protecting privacy. I am going to briefly summarize my statement.

First of all, I am pleased to report to you today that the Federal Government has made substantial improvements in securing the information and information systems that we protect. Let me do this by explaining the difference between where we were on September 10, 2001, and where we were 1 year later in September 2002.

September 2001, only 40 percent of Federal systems had up to date security plans; 1 year later, that was up to 61 percent. Similarly, the number of Federal systems certified and accredited was at 27 percent in 2001; 1 year later, that was up to 47 percent. The number of systems with contingency plans, 30 percent in September 2001; September of last year, 53 percent.

There are other significant improvements, and I had a table with that data in my written testimony, but items such as agencies using plans of actions and milestones as the authoritative management tool to ensure that program and system level IT security weaknesses are prioritized, tracked, and corrected. These measures reveal in some cases over 50 percent measured performance im-

provements since 2001. But they also identify an awful lot of work to be done.

The administration plans to make significant progress again this year. In our Clinger-Cohen report, which was Chapter 22 of the Analytical Perspectives of the President's 2004 budget, we included targets for improvement in critical IT security weaknesses by the end of this calendar year. Some of the key targets: All agencies shall have an adequate process in place for developing and implementing the plans of actions and milestones to ensure that program and system level IT security weaknesses are identified, tracked, and corrected.

Eighty percent of Federal IT systems shall be certified and accredited.

Eighty percent of the Federal Government's fiscal year 2004 major IT investments shall appropriately integrate security into the lifecycle of their investments.

I would like to talk a little bit about funding. Our analysis for the second year in a row shows that there is not a direct correlation between how much agencies spend on IT security and the quality of their results. That said, spending on IT security has increased 70 percent since 2002. Federal agencies plan to spend $4.25 billion this year on IT security, that is 7 percent of the Federal Government's overall IT budget and a 57 percent increase from the $2.7 billion spent last fiscal year. In next fiscal year, agencies plan to spend $4.7 billion on IT security, and that will rise to 8 percent of the overall Federal Government IT budget.

I would like to talk very briefly about some of the improvements and changes in handling cyber security incidents. Last year when I testified before the Government Reform Committee, I pointed out that we need to move to respond to threats within 24 hours. And so we have taken fairly aggressive action to do that.

OMB and the CIO Council have developed and deployed a process to rapidly identify and respond to cyber threats and critical vulnerabilities. CIOs are advised by a conference call as well as followup e-mail of specific actions needed to protect agency systems when a threat has been identified. Agencies must then report to OMB on the implementation of the required countermeasures. This emergency notification and response process has been used three times since the beginning of the year. We started out with the first vulnerability with a 90 minute cycle time to get the message out and get affirmative contact back that the process had begun—first for the Slammer Worm and then for the Sendmail and the IIS vulnerabilities. As a result of these early alerts, agencies have been able to rapidly close vulnerabilities that otherwise might have been exploited.

I would also like to talk a little bit about the integration of FedCIRC, the National Infrastructure Protection Center and the Critical Infrastructure Assurance Office [CIAO], under one department. That represents an opportunity for the administration to strengthen the Government-wide processes for intrusion detection and response through maximizing and leveraging the important resources of these previously separate offices. Now this has only been in effect for a little over a month. So I think as they produce the

results of their planning, you will see that there will be significant action.

Experts agree though, and I would just like to conclude with a final thought, it is virtually impossible to ensure perfect security of IT systems. Therefore, we must maintain constant vigilance while also maintaining the focus, as my colleagues have said, on business continuing plans. Thank you.

[The prepared statement of Mr. Forman follows:]

STATEMENT OF
MARK A. FORMAN
ASSOCIATE DIRECTOR FOR INFORMATION
TECHNOLOGY AND ELECTRONIC GOVERNMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS
U.S. HOUSE OF REPRESENTATIVES
April 8, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss the status of the Federal government's IT security. Through the requirements of the Government Information Security Reform Act (GISRA) and now the recently enacted Federal Information Security Management Act (FISMA), Federal agencies, OMB, the Congress, and the General Accounting Office (GAO) are able for the first time to clearly understand the Federal government's IT security strengths and weaknesses. For the purposes of today's hearing, I will provide the Committee with an update on both the government-wide progress realized in fiscal year (FY) 2002, and areas of continuing concern as well as the next steps OMB is undertaking with agencies to continue IT security performance gains.

I also wanted to inform you of a noteworthy E-government milestone. The March 17th Nielsen//NetRatings report which found that more than one-third of all Internet users visited a Federal government site in February. This finding is a clear indicator of the Federal government's commitment to maximizing the Internet to communicate with and provide services to Americans. The challenge that the Committee highlights at today's hearing is ensuring that the information and services are also appropriately secure.

As you know, GISRA has been instrumental in guiding Federal agencies toward greater IT security performance. Through GISRA and accompanying OMB guidance we have established a clear process to ensure effective management of IT security, sound implementation and evaluation of programs, procedures, and controls, along with appropriate and timely remediation of IT security weaknesses. OMB oversees and enforces these requirements through

traditional management and budget processes discussed later in my testimony.

Government Information Security Reform

GISRA brought together existing IT security requirements in previous legislation, namely the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Information Technology Reform Act of 1996 (Clinger-Cohen), improving upon these existing requirements. Additionally, GISRA enacted in statute existing OMB IT security policies found in OMB Circular A-130 on IT management and OMB budget guidance in Circular A-11. As a result, GISRA both integrated and reinforced long-standing IT security requirements. GISRA also introduced new review and reporting requirements and defined a critical role for agency Inspectors General (IGs) to play in independently evaluating agency IT security. Agency Chief Information Officers (CIOs) and program officials are responsible for conducting annual IT security reviews of their programs and the systems that support their programs. Agency IGs must perform annual independent evaluations of the agency's IT security program and a subset of agency systems. The results of these reviews and evaluations are reported annually to OMB and are the basis of OMB's annual report to Congress.

In July 2002, OMB provided instructions for Federal agencies' reporting the results of their annual reviews and evaluations. Agencies' FY 2001 reports established a baseline of agency IT security status. The FY 2001 and FY 2002 reporting instructions are nearly identical and are closely aligned with the requirements listed in GISRA. Additionally, as part of the FY 2002 guidance, OMB, working with the agencies, took steps to provide the Congress and GAO with additional information from agency POA&Ms. As a result, the combination of the GISRA reporting requirements, OMB's reporting instructions, and agency plans of action and milestones (POA&Ms) have resulted in a substantial improvement of the accuracy and depth of information provided to Congress relating to IT security. In addition to IG evaluations, agencies are now providing the Congress with data from agency POA&Ms and agency performance against uniform measures.

Measuring Performance

The most significant difference in the FY 2002 reporting guidance compared to the FY 2001 was the introduction of government-wide IT security performance measures. Consistent with GAO's findings, measures were incorporated within the existing instructions, requiring agencies and IGs in some instances to report the results of their reviews against the measures. Through these performance measures, the Federal government has a clear picture for the first time of IT security status and progress. From agency responses, areas of progress as well as areas of problems are evident. As a result, the FY 2002 reports clearly identify Federal agency's FY 2002 status and identify both progress made from their FY 2001 benchmark as well as new and remaining weaknesses.

I am pleased to report to you today that the Federal government has made substantial improvements in securing its information and information systems. OMB's annual report to Congress will provide more details but I would like to provide you with some examples of progress. For example:

- In FY 2001, only 40% of Federal systems had up-to-date system security plans. In FY 2002, that percentage increased to 61%.
- Similarly, the number of Federal systems certified and accredited increased from 27% in FY 2001 to 47% in FY 2002.

Table 1 below provides additional information on the Federal government's progress and is a subset of what we expect to include in the annual OMB report.

Table 1. FY 2002 Government-wide IT Security Performance

Total Number of Systems		Percentage of systems assessed for risk and assigned a level of risk		Percentage of systems that have an up-to-date IT security plan		Percentage of systems authorized for processing following certification & accreditation		Percentage of systems with a contingency plan	
FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02
7282	7957	44%	64%	40%	61%	27%	47%	30%	53%

* Data provided from agencies' FY 2002 GISRA reports to OMB.

While these measures reveal in some cases over 50% performance improvement from the FY 2001 baseline and

confirm the value of the review and reporting process in place, they also identify the magnitude of work yet to be done. The Federal government is heading in the right direction but the numbers are still too low.

Agency GISRA reports and IT budget materials provide an update on IT security spending. Federal agencies plan to spend $4.25B in FY 2003 on IT security, roughly 7% of the Federal government's overall IT budget, and a 57% increase from the $2.7B identified in FY 2002. As FY 2002 was the first budget year in which IT security costs were reported, this increase is largely attributed to improved reporting as well as a general increase in IT security. From the FY 2004 IT budget materials, agencies plan to spend $4.7B on IT security or 8% of the Federal government's overall IT budget of $59B, representing an 11% increase from FY 2003.

The FY 2002 GISRA reports also identify a number of other positive outcomes: 1) More Departments are exercising greater oversight over their bureaus; 2) At many agencies, program officials, CIOs, and IGs are engaged and working together; 3) IGs have greatly expanded their work beyond financial systems and related programs and their efforts have proved invaluable to the process; and 4) More agencies are using their POA&Ms as authoritative management tools to ensure that program and system level IT security weaknesses, once identified, are tracked and corrected.

Six Common Government-wide IT Security Weaknesses From F 2001

In the FY 2001 summary report to Congress, OMB identified six common government-wide weaknesses based on our review of agency and IG reports. A year later, progress is clearly evident across these six areas and while additional efforts are still warranted, the Federal government is heading in the right direction.

1. *Increasing agency senior management attention to IT security.* At the end of each fiscal year, agency heads now submit the security program review to OMB. The conditional approval or disapproval of agency IT security programs is directly communicated between the OMB Director and each agency head. In addition, OMB used the President's Management Agenda Scorecard to focus attention on serious IT security weaknesses. Through the scorecard, OMB and

senior agency officials monitor agency progress on a quarterly basis. As a result, senior executives at most agencies are paying greater attention to IT security.

2. *Development of IT security performance measures.* The absence of government-wide IT security performance measures was addressed in the FY 2002 reporting instructions. These high-level management performance measures assist agencies in evaluating their IT security status and the performance of officials charged with implementing specific IT security requirements. Agencies reported the results of their security evaluations and their progress implementing their corrective action plans according to these performance measures. These measures are mandatory and help to ensure that accountability follows authority.

3. *Improving security education and awareness.* Through the Administration's "GoLearn" e-government initiative on establishing and delivering electronic training, IT security courses were available to all Federal agencies in late 2002. Initial courses are targeted to CIOs and program managers, with additional courses to be added for IT security managers, and the general workforce. Additionally, NIST has developed and issued for review guidance to agencies on building an IT security awareness and training program.

4. *Increasing integration of security into capital planning and investment control.* OMB continues to aggressively address this issue through the budget process, to ensure that adequate security is incorporated directly into and funded over the life cycle of all systems and programs before funding is approved. Through this process agencies can demonstrate explicitly how much they are spending on security and associate that spending with a given level of performance. OMB also provided agencies guidance in determining IT security costs of their IT investments. As a result, Federal agencies will be far better equipped to determine what funding is necessary to achieve improved IT security performance.

Agencies have made improvements in integrating security into new IT investments. However, significant problems remain in regards to ensuring security of legacy systems.

5. *Working toward ensuring that contractor services are adequately secure.* Through the Administration's Committee on Executive Branch Information Systems Security of the President's Critical Infrastructure Protection Board, an issue group was created to review this problem and develop recommendations for its resolution, to include addressing how security is handled in contracts themselves. This issue is currently under review by the Federal Acquisition Regulatory Council to develop, for government-wide use a clause to ensure security is addressed as appropriate in contracts.

6. *Improving process of detecting, reporting, and sharing information on vulnerabilities.* Early response for the entire Federal community starts with detection of threats, vulnerabilities and attacks by individual agencies who report to incident response centers at the Department of Homeland Security (DHS), DOD, or elsewhere. While it is critical that agencies and their components report all incidents in a timely manner it is also essential that agencies actively install corrective patches for known vulnerabilities. To further assist agencies in doing so, the Federal Computer Incident Response Center (FedCIRC) awarded a contract on patch management. Through this work FedCIRC will be able to disseminate patches to all agencies more effectively. To date, 19 of the 24 Chief Financial Officer Act agencies have established patch authentication and distribution accounts. There are currently 176 active users in these agencies, and that number is increasing steadily as this new service continues to be implemented.

In addition, FedCIRC has implemented a 7X24 emergency notification process to rapidly alert agency CIOs to emerging cyber threats and critical vulnerabilities. CIOs are notified of specific actions needed to protect agency systems and agencies must then report to OMB on the implementation of the required countermeasures. The emergency notification and reporting process has been used three times since the beginning of the year - first for the Slammer Worm and then for the Sendmail and IIS vulnerabilities. As a result of these early alerts, agencies have been able to rapidly close vulnerabilities that otherwise might have been exploited. As FedCIRC and related organizations have moved to DHS, additional progress is being made on sharing information needed for Federal agencies to respond to vulnerabilities and cyber threats.

IT Security and E-government Initiatives

OMB's work on Expanding E-Government under the President's Management Agenda identifies IT security as a key issue. Two of the initiatives, E-Training and E-Authentication, provide significant opportunities for leveraging the Federal government's resources to improve IT security. The benefits of the E-Training initiative were identified above. Through the E-Authentication e-government initiative, the Administration deployed and tested a prototype e-Authentication capability in September. Applications are in the process of being migrated to this service, which will allow for the sharing of credentials across government and allows for secure transactions, electronic signatures, and access controls across government. The full capability is expected in September 2003.

Improvements in Critical Infrastructure Protection and Federal Incident Response

Experts agree that it is virtually impossible to ensure perfect security of IT systems. Therefore in addition to constant vigilance on IT security we require agencies to maintain business continuity plans. OMB directed all large agencies to undertake a Project Matrix review to ensure appropriate continuity of operations planning in case of an event that would impact IT infrastructure. Project Matrix was initially developed by the Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce. As you know the CIAO and its functions were transferred to DHS. A Matrix review identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector.

Coordination of the Federal government's cyber security and critical infrastructure protection efforts continues under the leadership of the new Homeland Security Council's (HSC) Special Assistant to the President for Critical Infrastructure Protection, and the Assistant Secretary for Infrastructure Protection at DHS (who is responsible for cybersecurity coordination within DHS), in partnership with OMB. OMB works with the HSC and DHS, and all Federal agencies to ensure that through IT security policy and management and budget processes, our critical

operations and assets are appropriately identified along with the resources necessary to secure them. We are also working with DHS to improve the Federal government's response to cyber attacks, and vulnerabilities. The integration of FedCIRC, the National Infrastructure Protection Center (NIPC), and the CIAO under one Department, partnering with the Science and Technology directorate on research and development needs, presents an opportunity for the Administration to strengthen government-wide processes for intrusion detection and response through maximizing and leveraging the important resources of these previously separate offices.

Continuing Efforts to Improve IT Security

Budgeting for IT Security

All Federal systems require security. To identify the appropriate security controls, agencies must first assess the risks to their information and systems. Security must be incorporated into the life-cycle of every IT investment. As part of the IT business case (Form 300) for major systems, agencies report on that risk as well as their compliance with security requirements, i.e., development of security plans and certification and accreditation. Failure to appropriately incorporate security in new and existing IT investment automatically requires it be scored as "at-risk". As a result, that system is not approved to proceed for the fiscal year in which the funds were requested until the security weaknesses are addressed. As of the submission of this report, there are approximately 700 systems in the FY 2004 budget, totaling nearly $19 billion, at-risk either solely or in part due to IT security weaknesses. Additionally, many agencies are not adequately prioritizing their IT investments and therefore are seeking funding to develop new systems while significant security weaknesses exist in their legacy systems. OMB will assist agencies in reprioritizing their resources through the budget process.

Government-wide IT Security Milestones

OMB set targeted milestones for improvement for some of the critical IT security weaknesses and included them in the President's FY 2004 budget. Targets for improvement include:

- More agencies must establish and maintain an agency-wide process for developing and implementing program and system level plans. Plans of action and milestones must serve as an agency's authoritative management tool, to ensure that program and system level IT security weaknesses, once identified, are tracked and corrected. By the end of 2003, all agencies shall have an adequate process in place.

- Many agencies find themselves faced with the same security weaknesses year after year. They lack system level security plans and certifications. Through the budget process, OMB will continue to assist agencies in prioritizing and reallocating funds to address these problems. By the end of 2003, 80 percent of Federal IT systems shall be certified and accredited.

- While agencies have made improvements in integrating security into new IT investments, significant problems remain in ensuring security of new and in particular, legacy systems. By the end of 2003, 80 percent of the Federal Government's FY 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment.

Department-wide Plan of Action and Milestone Process

Clearly, the more reviews agencies and IGs conduct, the more weaknesses they will find. As a result agency and IG reports are identifying an increased number of IT security weaknesses. To ensure that appropriate and timely corrective actions are taken, OMB guidance directs Federal agencies to develop POA&Ms for every program and system where an IT security weakness has been found. POA&Ms must serve as an agency's authoritative management tool, to ensure that program and system level IT security weaknesses, identified by the agency, IG, GAO, or OMB, are prioritized, tracked, and corrected. These plans must be developed, implemented, and managed by the agency official who owns the program or system (program official or CIO depending on the system) where the weakness was found. System-level POA&Ms must also be tied directly to the budget request for the system through the IT business case. This is an important step that ties the justification for IT security funds to the budget process.

Expanding E-Government under the President's Management Agenda

To ensure successful remediation of security weaknesses throughout an agency, every agency must maintain a central process through the CIO's office to monitor agency compliance. OMB's draft FY 2003 guidance to agencies for reporting under FISMA will direct agency IGs to verify whether or not an agency has a process in place that meets criteria laid out in OMB guidance. OMB has and will continue to reinforce this policy through the budget process and the President's Management Agenda Scorecard. An IG approved agency-wide POA&M process is one of a number of milestones necessary for agencies to improve their status on the Expanding E-Government Scorecard.

IT Security Performance Measures

OMB will also incorporate the performance measures I discussed earlier into the quarterly POA&M reporting, coinciding with the Scorecard assessment. Agencies will report each quarter on their progress, by bureau, against those measures.

Conclusion

GISRA has clearly had a tremendous impact on the state of Federal IT security. The framework and processes in law and OMB policy have reinforced the importance of management, implementation, evaluation, and remediation to achieving real IT security progress. Due to the significant work of Federal agencies and IGs, along with the Congress and GAO, we are able to point to real advancement in closing the Federal government's IT security performance gaps. With all of that progress, we still have a long way to go to appropriately secure our information and systems. Many pervasive IT security weaknesses remain, leaving the Federal government with unacceptable risks. OMB will continue to work with agencies, Congress, and GAO to ensure that appropriate risk-based, and cost-effective IT security programs, policies, and procedures are in place to secure our operations and assets.

Mr. PUTNAM. Thank you very much, Mr. Forman. I thank all of our panelists. We will get right to the questions.

All of you have touched on the simple fact that most of the critical infrastructure is controlled by the private sector. Mr. Vatis, in particular, singled out the need for an aggressive innovative approach that goes beyond merely the soapbox to incent or coerce greater accountability and compliance, greater focus on cyber security in the private sector. Could you elaborate a little bit more, beginning with Mr. Vatis, and then the other two as well, on the best way for the Federal Government to approach the regulation of and the incentivizing of better cyber security in the private sector.

Mr. VATIS. Mr. Chairman, thank you. I do not have any particular silver bullet that I think is the answer to the problem. But I think there are a number of ideas that have been discussed but over the past few years have basically been dismissed out of hand because of the fear of even getting into anything that might smack of regulation. So what I am really urging is a considered study of several different options. The fact of the matter is we do have some instances of direct regulation, of coercion, if you will, that are already in place but which were not instituted for security's sake, per se, but more out of a concern for privacy: of HIPAA and Graham-Leach-Bliley, for example.

So I think one thing that should be done is to study those acts as they are implemented to see if they actually result in a net increase of security, and if so, at what cost, in terms of efficiency or other things. I think there are other ideas that have been talked about, such as requiring disclosure of security plans for security breaches by companies that suffer breaches so that there is a further incentive to take security seriously. Because what we have seen over the years again and again and again is that many companies are simply sweeping the problem under rug so that it does not become public. I think if there were some sort of disclosure requirement, as the State of California, for example, is now instituting for companies that do business in that State, as of this summer, that could create an additional incentive. Requiring disclosure of plans in a 10k form for publicly traded companies is another idea that has been talked about. Tax incentives for upgrading of technology to address security is another idea. Best practices for hardware and software manufacturers.

So there are many ideas. I think the wonderful congressional staff that are out there are a good resource to look into these ideas. And some of the Federal R&D moneys should be devoted not just to technical R&D, but to research into the legal, policy, and economic factors that affect the implementation of technical security requirements.

Those are some of the things that I would urge.

Mr. PUTNAM. Mr. Clarke.

Mr. CLARKE. Mr. Chairman, I think we want to avoid regulation here. The thought of having a Federal cyber security regulation agency and a Federal cyber security police scares me to death. But I think there are some things we can do to stimulate the private sector without regulation. One, Michael just mentioned, is we can have the SEC do what it did for Y2K, which is to require that publicly traded companies have in their reports a report against some

set of auditing standards that the auditing industry could come up with, a report on their performance. Now we do not want their security plans revealed publicly and we do not want them to have to report individual incidents. But they ought to get a grade from an outside auditing firm, IT security auditing firm, and that ought to be reported as part of their public annual disclosure. That had a great effect during Y2K and we ought to think seriously about asking the SEC to look into that.

Similarly, cyber insurance could have a big effect. The insurance industry could set standards for cyber security insurance and the rates that they charge could reflect how good a company is doing. Requiring certain kinds of companies that are doing business with the Federal Government, not small businesses, but larger businesses to have cyber security insurance would have an enormous effect on the market.

Mr. PUTNAM. Before we go to Mr. Forman, let me followup on that. You mentioned as part of your 10 point plan in your testimony the need for any congressional action on terrorism risk insurance to include a cyber insurance provision. Presumably, that would have some type of Federal backstop or subsidy in that risk insurance, and you mentioned that alone would raise the bar of security on the cyber side. But you differ from Mr. Vatis in saying that companies should not have to report breaches of security. Why is that?

Mr. CLARKE. I do not think you want to have specific breaches of security reported because I think it gives too much information to the people who want to do the breaches. I think what you want is an overall grade. All too often when there is one minor security violation that gets into the press because it has been reported, a company suffers disproportionately from what its real security problem is. So I do not think you want to force companies to report individual security violations, but to report an overall grade on performance.

The Cyber Risk Insurance Act, of course, has passed. The committee language suggests it covers cyber security. That is not clear in the language of the bill. But the real problem with cyber insurance right now is it is not clear that there is a Federal backstop against catastrophic terrorism as there is for other forms of terrorism, and there really is not a decent actuarial data base yet that allows underwriters to decide on what policy should be. So if the Government could collect information, statistics, or, better yet, get someone like Mike to do it, not have a Government agency do it, but somebody, Carnegie Mellow, Dartmouth, someone to collect enough information so that the underwriters in the insurance industry would feel better writing more policy, and requiring when they do write policy that companies live up to certain standards and best practices, that would go a long way.

Mr. PUTNAM. How would you have an actuarially sound policy if breaches are not required to be reported?

Mr. CLARKE. Not reported publicly. I think they should be reported perhaps in an anonymized way to a third party.

Mr. PUTNAM. Mr. Forman.

Mr. FORMAN. I think you have to look at a couple of factors. First of all, you have got to ask what is the market failure here. We be-

lieve that normal market approaches would not suggest regulation if there is something holding the companies accountable in the marketplace. In other words, if a company loses customers because they are not protecting their security well, then we expect normal marketplace forces to work. And I think there is pretty strong evidence of that. If you look at a couple years ago, we had firewalls, we had antivirus technology. By looking at the growth over the last year and the trends in the marketplace on how to protect against cyber threats, well, threat management systems and software, and then highly reliable redundant systems that leverage the architecture of the internet so it is moved out of the security technology realm into hosting and other architecture tools; companies such as Akamai growing terrifically fast. So it is clear the marketplace will respond.

I would give you a couple of thoughts on the issue. First of all, are the issues essentially related to criminal type threats. Those may not be made public for a number of reasons. But that may be something to deal with and look at as a tradeoff between how do we associate law enforcement structures, is that right for the internet age. And the other is what do you do about organized cyber terrorism. You have different Government roles and responsibilities issues there. That should basically guide, we believe, the regulatory answer to the question of whether regulation is even needed in the first place.

Mr. PUTNAM. Mr. Clarke and Mr. Vatis both alluded to or specifically said that we do not have a centralized mechanism in the Federal Government for overseeing cyber security compliance, cyber security coordination and collaboration. So are you satisfied with the current framework that calls for its placement in Homeland Security, or is it still too diffused between FBI and Homeland Security and OMB and other agencies?

Mr. FORMAN. There are two parts of the picture I think that you have to look at. First of all, we do spend an awful lot of money. We are the world's largest buyer of information technology. So have we got enough central focus and the right structures in place, I am very confident now, and I think the data show, we are able to track and measure the gaps in cyber security, we are able to hit the cycle time that we are looking for.

I do not know that private sector industries have anything like that. We can focus because we do have an organizational structure. So the question is when you get into the other industries, should it be dealt with on an industry by industry approach, should it be dealt with on a company by company approach. And there is a real question on what that structure should be. I think that was thoroughly vetted in creation of the Information Integration and Infrastructure Assurance under secretariat, it was vetted within the administration, it was vetted within the House and the Senate.

Now one thing that I should correct for the record. The under secretary is a confirmed position. But the assistant secretary that has key responsibilities here is an appointed position. And that person is in his job now, Bob Wiskowski, and he has been there a couple of weeks. He comes from Coca Cola and, of course, people would say the formula for Coke is one of the most protected secrets in the world today. So there is an interesting background that he

brings. But, again, the department has only been up for several weeks now. I think when you see their go forward plan, you will see how they have integrated things, building on the successes and giving some innovation to that as well.

Mr. PUTNAM. Mr. Vatis, do you want to comment on that?

Mr. VATIS. I am hopeful, Mr. Chairman, that Mr. Forman will prove to be right and that once the key personnel are in place in the new department we will see things start to roll. But I think, to be realistic, it will take some time, because the operational personnel are not likely to be in place for over a year, and there are so many vacant positions now that are responsible for infrastructure protection and intelligence analysis.

I would make one other point about something that worries me. And that is what appears to be the administration's policy that cyber security is a subset of critical infrastructure protection as a whole, including physical vulnerabilities of our critical infrastructures. I think there is definitely a logic to that view in that we do need to look at the infrastructures as a whole and consider all the different vulnerabilities. But the worry I have is that if an official or a subset of DHS is looking at both physical and cyber vulnerabilities and threats, cyber will always get short-shrift, especially in these years so soon after September 11th when so much focus is on the vulnerability to physical terrorist attack. I think we have seen that happen in prior years. When we tried to do both things through the same offices, through the same people, cyber always got less attention than it was due. So that is another thing I think we need to keep an eye on, to make sure that does not happen.

Mr. PUTNAM. Mr. Clarke, when you analyze the threat environment out there, what particular nations or particular non-state actors are out there that have made cyber security a priority as their way of getting at capitalism or the United States or western civilization or whatever?

Mr. CLARKE. Mr. Chairman, there is a classified answer to that in terms of what we know about other nations that have created offensive cyber security organizations. Suffice it to say in an open hearing there are nations, including our own, that have created cyber security offensive organizations. And there are terrorist groups, organized criminal groups that are interested in this. I am not very good at predicting the who here. And I think we make a mistake by focusing on who is going to do it to us.

I think rather than focus on the who, we should focus on the what, what are they going to do. And it is real simple. As long as we have major cyber security vulnerabilities that would allow someone who does not like us to screw up our economy, then someone will. It may not happen this year. We may not be able to guess who it is in advance. But it is a very high probability that as long as we have very well known major vulnerabilities that are cheaply exploited, somebody will do it. And I do not think the emphasis ought to be on trying to figure out who that is in advance and getting them before they do it, because someone else will do it. What we should try to do is raise the barrier.

And in answer to your last question about DHS and OMB, I think the question answers itself when you ask who is the highest

level official in the Department of Homeland Security whose full-time job is cyber security. What office in the Department of Homeland Security does nothing but cyber security? Who is the highest ranking person in OMB who does nothing but cyber security? How many people in OMB, the organization to which the Congress has given the full responsibility for cyber security in the Federal Government, how many people in OMB have that as their full-time responsibility? The answers to those questions are pretty frightening I think.

Mr. PUTNAM. Mr. Forman, do you want to answer those questions?

Mr. FORMAN. We have an interesting change going on in our society. I think from a policy perspective as it relates to Federal IT, we cannot differentiate the work that we need to do in our architectures from cyber security. I certainly have spent a lot of time, but I think we as an administration have spent an awful lot of time making sure that we get the communications between the CIOs and the cyber security community. These are two separated communities that have to talk to each other. So, for example, when we have denial service attacks, we find increasingly over the last few months people organize over the Web and they will target the White House Web site because in areas outside of America people feel that is similar to attacking the administration.

Mr. PUTNAM. That is the whitehouse.gov Web site?

Mr. FORMAN. That is correct. As opposed to others that may be out there that I have never known about. So these people will organize and they are known. They will run advertisements in the newspaper, they will run advertisements on the Internet. Essentially, the characterization will be come to our Web site if you want to attack President Bush for some action. The cyber security community will be aware of that and never communicate that to the CIO of the White House, the CIO of the Energy Department, and others. We have worked pretty hard over the last 2 months to correct that problem. And the integration of these two communities is absolutely critical; we cannot separate them.

Mr. PUTNAM. And you are satisfied that integration will occur under the new structure of Homeland Security once they are up and running?

Mr. FORMAN. Absolutely. In fact, as I pointed out in my oral and put in more detail in the written testimony, as it relates to Federal cyber security, we have had to make that happen. As I pointed out, we have had three major events this year. We started out with a 90 minute cycle time and we have been able to shrink that down even more so.

But there is the longer term issue of how we secure the infrastructure. There is the fast response issue of what do we do. And to give you a feel, I tend to think of this as three dimensions. We have literally thousands of vulnerabilities. Anybody who could know all the vulnerabilities and make sure the patches are deployed is truly detail oriented, and, as Dick said, there is software that does that for you. You have to rely on the technology to manage the technology. The second dimension are the threats. There are people out there, some of whom are organized, some of whom will leverage the Internet to organize very rapidly. And the third

thing is what will it mean for the actual technology, your architecture that you have deployed as a department.

So, as an example, we worried and fast responded to the Slamer threat. But as you recall, the Congress was affected by this. There was a cyber sit-in where people called and used the Internet as a way to show their response to the administration's policy in the war in Iraq. Our policy decision on that was that was not a cyber security threat; that was e-democracy moving into the Internet age. The cyber security community view on that was that was a cyber threat. So if we do not meld these two groups together and look at this from the standpoint of the CIO overall, as was laid out going back to the Clinger-Cohen Act, we will not be able to get that decision properly placed as a policy decision.

Mr. PUTNAM. Correct me if I am wrong or if I am heading in the wrong direction on this. But from my perspective, the OMB role would be an internal Federal IT management role, protecting and preserving the sanctity of Federal systems, of the Federal networks, of containing the costs of a breach that would spread agency-wide or department-wide or Government-wide. The role of Homeland Security would be analyzing the threats, detecting as quickly as possible when a virus or some other cyber attack has occurred, and then distributing that word as quickly as possible to the public and private sector—State, local governments, the remainder of the Federal Government, and critical infrastructure. So how well is Homeland Security equipped to handle that, not from an internal Federal IT perspective, but from the external perspective?

Mr. FORMAN. Again, a lot of this may change, but let me tell you because there is an area of overlap between the Federal and the external. FedCIRC maintains the catalogue, if you will, of the vulnerabilities and the patches that are associated with fixing that vulnerability. Generally, when we see a threat materialize that we have to respond quickly to, the threat targets a certain vulnerability. And if the patch gets rapidly deployed or if it had already been deployed, there is no impact. And so we have been fairly effective, certainly this year we have been 100 percent effective, in making sure that when the threat is identified FedCIRC puts out, in coordination with the CIO Council, the link to the patch and the characterization of that vulnerability, the threat, etc.

There is a partner organization, the National Infrastructure Protection Center, that was not totally but the key elements moved from the FBI to that same office to integrate this together better. They produce a daily report. I expect that will continue. I do not know that for a fact. We will see I think some innovation there. But that tells you the threats that are current, the patches that are current, hot links, and so forth. So I think that part is focusing fairly well on the topical threats.

In the area outside of Government, the longer term remediation and maintenance of the architectures is an area where I think there is a big question as to how to proceed. There is a multifaceted approach laid out in the President's National Cyberspace Strategy. And that was thoroughly vetted, as in Dick Clarke's testimony. So I am fairly comfortable we are going to see a good implementation plan for that as Bob has the time to make that work at Depart-

ment of Homeland Security and they are ready to release their implementation plan for that strategy.

Mr. PUTNAM. I know that there has been a great deal of focus on this and I know that it is a daunting task. But in the latest report in 2002, after 4 solid years of focused, specific attention to this issue of cyber security, we only had 3 out of 24 agencies that received a report card grade that was better than a D, and 14 of the 24 got an F. What are we doing wrong? What is Congress' role? That is just unacceptable, obviously. And while it does not reflect a lack of effort on the part of OMB perhaps to manage this, it certainly reflects a lack of success on the part of agencies to improve outcomes. So I will let you get situated and then answer that.

Mr. FORMAN. I share 100 percent this focus. First of all, we did have differences in scores and ratings between what Mr. Horn scored the agencies on and how we scored them in 2001. I will say 2001 was the first year that we actually measured progress and that set the benchmark. So it was not until the end of 2001 that we even knew quantitatively how bad it was and subsequent to that put in place a process, these plans of actions and milestones, that laid out the workload to fix that.

Last year, we had pretty much quarterly oversight for both OMB as well as Congress. I would ask that we maintain that because I think we made a lot of progress. It is documented in the data that we shared in the testimony, in some more detailed data we shared with the staff and GAO in the 2002 GISRA report, and we will be able to see to the agency. But the progress of going from 27 percent to 53 percent, is 53 percent acceptable? Absolutely not. By the end of this year, we believe, it is a slight stretch goal, but with the constant vigilance, we believe we get up to 80 percent on a couple of these security measures and 100 percent on putting in place a process. That is going to take a lot of continued oversight throughout this year to get there. But at that point we are talking about significantly improved security. And I would put that up against any company and you will find very few that hit those benchmarks.

Mr. PUTNAM. Just very briefly, would you put that up against any other country?

Mr. FORMAN. I think that there are a couple—I have not really thought about that. But certainly our view is that the United States spends the most, we have to protect our citizens and the information, and so we are going to be the best not because we are competing with other countries, but because it is the right thing to do for Americans.

Mr. PUTNAM. Mr. Clarke, Mr. Vatis, what other countries out there are ahead of us on protecting critical infrastructure from cyber attack?

Mr. CLARKE. The good news, Mr. Chairman, is that nobody is ahead of us. The bad news is that we are pretty bad. I disagree with Mark in saying that the Federal Government is as good as any company. That just is not true. The private sector is way ahead of the Federal Government.

Mr. PUTNAM. So who do I need—I do not mean to interrupt, I am going to let you finish—what company's CIO do I need to bring in to our next hearing?

Mr. CLARKE. Rhonda MacLean, from Bank of America, will tell you, if you ask her the right questions, how she is doing it. She is doing a great job. Bank of America is better than any Federal Government agency in terms of its IT security. That is true of most major banks in the United States. They are doing a much better job. Why? Because they have got someone who is a senior person who is full-time in charge of IT security. I did not hear in Mark's answer who is the senior OMB official who is full-time in charge of IT security and nothing else. I did not hear who in the Department of Homeland Security is in charge of cyber security and nothing else full-time. I did not hear how many people we have in OMB full-time working on cyber security.

I think there is another big mistake we are making, and that is we are trying to get the departments to do this themselves essentially. And with all due respect to civil servants, I was one for 30 years, you are not going to get this done without outsourcing it. There is a real reluctance in Federal departments to outsource IT security. But there is a solution. Take the Department of Labor, take the Department of Agriculture and have it contract to any of the big integrators or any of the IT security firms and then hold them responsible and fine them in terms of their contract if there is not performance. Instead of just bringing the CIO of Labor or Agriculture up here and berating them that they got an F again, have them outsource it to a company that has penalties in its contract if that grade is an F again.

Mr. PUTNAM. Does the law currently preclude them from doing that?

Mr. CLARKE. No, it does not.

Mr. PUTNAM. Mr. Vatis.

Mr. VATIS. I agree 100 percent with what——

Mr. PUTNAM. With which one, Mr. Clarke or Mr. Forman?

Mr. VATIS. With Mr. Clarke. I think he is exactly right on the lack of sufficient high level personnel devoted to this issue. I think the cyber issue will always get short-shrift. I think the idea that we need a hammer to truly make progress happen within the agencies is also exactly right. I served in the FBI for a few years and lived within an infrastructure that, despite some efforts over those years to improve it, never really got anywhere. And I think that is a case study of how not to manage information systems in a crucial Federal agency.

Mr. PUTNAM. Sort of a recurring theme in these E-Government issues in our subcommittee hearings is that we have a cultural challenge, a human capital challenge throughout the Federal Government in dealing with this issue.

We could go on, but I have a second panel. I want to thank all of you for your very insightful and thoughtful testimony. I will give each of you 1 minute to say whatever is on your heart that I did not ask you about or to rebut or give a counterpoint to something that somebody else has said. We want to be as thorough and as fair as possible.

We will begin with Mr. Forman. You have 1 minute to say whatever you would like to say to conclude.

Mr. FORMAN. Thank you, Mr. Chairman. I just want to congratulate you again for this hearing. Oversight of progress has been and

will continue to be incredibly important to our success. I will pledge to you that the administration is focused on this all the way to the highest levels, that we are holding deputy secretaries and secretaries accountable. And I would ask for your cooperation and support in doing the same.

Mr. PUTNAM. You have it. Mr. Vatis.

Mr. VATIS. I think from our testimony you can gather that how the DHS evolves is going to be critical, especially at the operational level. So I think one thing that this committee could fruitfully do is keep the heat on to make sure that DHS devotes the requisite attention to cyber security and that they do not let it get lost in the shuffle of dealing with physical terrorism and reducing our vulnerability to physical terrorist attacks. Make sure that they hire people as quickly as possible, and that the consolidation actually achieves the promises that have been made about new efficiencies among all these entities that were formerly separate. Without some heat from Congress, it will not be done nearly quickly enough or well enough.

Mr. PUTNAM. Mr. Clarke.

Mr. CLARKE. Mr. Chairman, just again to thank you for your recognition of this issue. And to echo Mike Vatis, you personally have a great opportunity here to be a pain in the rear end to the administration, and I encourage you to do that.

Mr. PUTNAM. That is very kind of you, Mr. Clarke. [Laughter.]

The first panel is dismissed.

The subcommittee will stand in recess for about 2 minutes while we set up the second panel.

[Recess.]

Mr. PUTNAM. I will reconvene the subcommittee hearing.

We would like to welcome our second panel of witnesses. As is the custom with the committee, we swear in our witnesses. So please rise and raise your right hands and repeat after me.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all of the witnesses have responded in the affirmative.

We welcome you to the subcommittee. You have had an opportunity to hear the testimony of the first panel and some of the interchange. Following the ladies first rule, we will begin with Ms. MacLean, who has received a warm introduction and very high praise in the first panel.

Rhonda MacLean is senior vice president and director of corporate information security for Bank of America. Ms. MacLean joined Bank of America in 1996 as the director of corporate information security and is responsible for providing global leadership for information security policy, procedures, risk management, security technology implementation, cyber investigations/forensics, and general information security awareness. In addition, she is responsible for enterprise business continuity planning and the company's regional recovery centers.

In May 2002, the Department of the Treasury appointed Ms. MacLean as the private sector coordinator for the financial services industry public/private partnership on critical infrastructure protection and homeland security. She will act in concert with Treasury's private sector liaison to draw together industry initiatives re-

lated to critical infrastructure protection and homeland security. In addition, she was elected to the Board of Directors for the Partnership for Critical Infrastructure Security, which brings together leaders from across multiple critical sectors such as energy, telecommunications, finance, etc.

We welcome you to the panel, and recognize you for 5 minutes for your opening statement.

STATEMENTS OF RHONDA MACLEAN, SENIOR VICE PRESIDENT AND DIRECTOR OF CORPORATE INFORMATION SECURITY FOR BANK OF AMERICA, SECTOR COORDINATOR FOR THE FINANCIAL SERVICES INDUSTRY PUBLIC/PRIVATE PARTNERSHIP ON CRITICAL INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY; ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE; AND THOMAS PYKE, CHIEF INFORMATION OFFICER, DEPARTMENT OF COMMERCE

Ms. MACLEAN. Thank you, Chairman Putnam, and thank you for inviting me here today to testify at the hearing. I am very honored to speak on behalf of the financial services sector in my role as the Department of Treasury-appointed private sector coordinator for critical infrastructure protection.

In listening to the testimony this morning, something struck me that I wanted to add to this statement. This challenge that we have before us takes vision, leadership, execution, and accountability. I want to touch on those things today with the information that I provide you about the financial services industry's involvement in critical infrastructure protection, the current work of our financial services sector coordinating council, and discuss some of the opportunities where I think Government and industry really can partner to address some of the challenges we have in securing our cyber space.

The administration's National Strategy to Secure Cyber Space identified the critical infrastructures as consisting of physical and cyber assets of the public and private sector and institutions. Though the basic approach of security must fundamentally address people, process, and technology aspects of the infrastructure, I do want to iterate that there is no single solution to this challenge. Creating the appropriate balance of these elements is based on an operational risk management consideration that addresses the critical nature of the systems as well as the exposures to which they can be subjected.

I would like to talk about the sector's critical infrastructure protection efforts, and specifically about our Council. At the time of my appointment, there was no integrated entity that could represent the entire financial services sector. Individual associations were actively and effectively working on their Members' behalf and provided much leadership for our critical infrastructure protection efforts. To ensure coordination across the sector, with the public sector's support and encouragement, and with the leadership of the Department of Treasury, we formed the Financial Services Sector Coordinating Council. Today, we have 24 organizations consisting of key national exchanges, clearing organizations, trade associations in banking, securities, bond and insurance segments of our

industry, and we are working together to improve the critical infrastructure protection for our sector as well as others on which we depend.

Through our Council members, we engage nearly all financial service sector entities. Let me highlight three of the five strategic areas on which we have focused.

The first area is in information dissemination and information sharing. Our goal is to ensure that a universal service to disseminate trusted and timely information will be made available to all sector participants.

Second, crisis and response management needs to be implemented. When events occur with broad sector or national impact, a planned and adopted approach for communicating and responding as a sector, including coordination with Government entities, is the focus of this particular effort.

Third, we are leading the sector's efforts to revise our, the financial services sector's, national strategy component in response to the two national strategies released in February by the President. We believe this is our opportunity to define strategic as well as tactical, actionable, and measurable actions as part of our sector-wide critical infrastructure and homeland security efforts.

In my chairperson role for the Financial Services Sector Coordinating Council, I work closely with the lead agency, the Department of Treasury, and specifically the Office of Critical Infrastructure Protection and Compliance which was created by the Treasury Assistant Secretary Wayne Abernathy and led by Deputy Assistant Secretary Michael Dawson. Together, they lead the Financial and Banking Information Infrastructure Committee. That council is really the public side of what I would call the public-private partnership. It is through council members and our Government partners' cooperative efforts that we are able to maximize our resources and achieve our objectives to ensure protection of our critical infrastructures to the benefit of the economy and to the financial services customers.

Let me transition the discussion to some opportunities for continuing the progress that has been made both by the government and the private sector.

First, let us talk a little bit more about information analysis and information infrastructure protection. The need for synergy between information analysis and infrastructure protection has clearly been recognized in the assignment of those responsible to the undersecretary within the Department of Homeland Security. We expect this to provide a much more robust alerting, threat warning, and information flow from the public sector based on the vast resources that they have made available through their integration.

Second is understanding the threat. Based on the Government's visibility of threats to the private sector, a clear understanding of the protection needs must exist between the public and the private sector. Gaps between the private sector's protection efforts and the Government's view of the necessary protections must be defined and clearly understood. There may be situations where, unknown to the private sector, normal business practices will not adequately address the level of threat understood by the Government. Where market focus does not provide the appropriate incentives to provide

these protections, augmentation of market mechanisms, such as incentives, may be appropriate.

Third, product security. Because the private sector mainly employs commercial products, services, and software to implement cyber security protection and monitoring, those efforts that improve the security of such products have broad benefit. As a sector, we work closely with our vendors to achieve higher levels of security. BITS, or the Bankers' Information Technology Secretariat—the technology group for the Financial Services Round Table—and a member of our Coordinating Council, has implemented a product certification program as a prime example of our industry's efforts in this area.

And finally, the voluntary sharing of threat and incident information. We must continue to encourage processes that accommodate companies' voluntary sharing of sensitive information, such as the provisions outlined in the Homeland Security Act of 2002.

In closing, Mr. Chairman, and members of the committee, we believe the strong public-private sector partnership that is emerging is the right approach. And it is finally with that vision, leadership, and execution, we believe that we can continue to make progress in this important area.

[The prepared statement of Ms. MacLean follows:]

STATEMENT

OF

RHONDA MACLEAN
PRIVATE SECTOR COORDINATOR
FINANCIAL SERVICES CRITICAL INFRASTRUCTURE PROTECTION
AND HOMELAND SECURITY
&
DIRECTOR, CORPORATE INFORMATION SECURITY
BANK OF AMERICA

BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
UNITED STATES CONGRESS

April 8, 2003

TESTIMONY OF RHONDA MACLEAN

Chairman Putman, Ranking Member Clay, and members of the Subcommittee, thank you for inviting me here today to testify at this hearing on "Cyber Security: The Challenges Facing Our Nation in Critical Infrastructure Protection." I am honored to appear today to speak on behalf of the financial services sector in my role as the Department of Treasury-appointed private-sector coordinator for critical infrastructure protection.

My name is Rhonda MacLean. I am a Senior Vice President at Bank of America Corporation responsible for Corporate Information Security. My responsibilities also include the Bank of America enterprise business continuity planning and the company's regional recovery centers. This encompasses organizing disaster recovery exercise activities and program capability implementation to ensure the ongoing delivery of services to our customers.

Before joining Bank of America in 1996, I worked for The Boeing Company for 14 years, and as the senior manager for computer and communications security, I was responsible for all commercial airplane and government information security initiatives. I have served in a number of external advisory roles and in professional activities related to information security; I currently serve on the University of North Carolina – Charlotte, Board of Advisors for the College of Information Technology.

Let me first compliment the subcommittee for holding these hearings. Our sector looks forward to working with you as you explore cyber security issues. Today, I plan to provide you with background on the financial services industry's involvement in critical infrastructure protection efforts, the current work of our Financial Services Sector Coordinating Council, and to discuss opportunities where industry and government can partner to address some of the challenges we face in securing cyber space.

At all levels across our sector, including executive leadership, operations personnel, our trade associations, professional institutes, and our customers, we are very aware of the new global realities and the importance of the vital financial services we provide globally to the nation and our customers.

The Department of the Treasury recently noted, "We continue to work with the financial and banking communities so that our financial system remains functioning efficiently and effectively. We are confident America's financial

infrastructure is strong and resilient."[1] There should be no doubt that the public-private partnership is well engaged to ensure the safety, soundness and resiliency of our industry is not only maintained but also enhanced.

In May of 2002, consistent with public-private sector partnership objectives expressed in Presidential Decision Directive 63, subsequent Executive Orders, and the published National Strategies for Homeland Security and Cyber Space Security, I accepted an appointment to serve as the private sector coordinator from the Department of the Treasury, which is the lead agency for the banking and finance sector. To assist me in these responsibilities, Bank of America is demonstrating its well-recognized industry leadership by providing three additional full-time staff resources to support me in carrying out these responsibilities for our industry.

The "National Strategy to Secure Cyber Space," published by the Administration in February 2003, identified the nation's critical infrastructures as consisting of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. These infrastructures have been deemed critical because "... their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[2]

The information technology, telecommunications and electric power industries provide components and services vital to the operation of all these infrastructures. More than ever before, computer technology is imbedded at many levels consisting of servers, routers, and switches and connected by fiber optic cables, wire lines, and wireless technology. We depend upon these systems and components to make our critical infrastructures work. Thus, maintaining the availability and integrity of those mission-critical assets is essential to our economy and our national security.

Those who own and operate these critical Infrastructures maintain the availability and integrity of these system components through the application of a variety of security disciplines, operational controls, and response and contingency initiatives. Though the basic approach to security must fundamentally address the people, process, and technology aspects of the infrastructure implementations, there is no single solution to the security challenges. Because threats and technology continue to change, cyber security approaches and process employed must continuously evolve – this is what is often characterized

[1] Treasury Statement on Measures to Protect the Financial Markets during Hostilities with Iraq, March 17, 2003.

[2] Executive Order 13010, Critical Infrastructure Protection, July 15, 1996.

as "good practices."

These "good practices' involve implementation of an appropriate balance of prevention, detection, protection, response and recovery measures. Creating the appropriate balance of these elements is based on operational risk management considerations that address the critical nature of the systems as well as the exposures to which they can be subjected. The wider use of a common enterprise network to conduct business operations creates an architectural model that organizations must recognize and one that requires an enterprise-level risk management governance process.

To address these common enterprise environments, organizations must adjust their decision-making and risk management accordingly. The creation of this "shared risk environment" necessitates an enterprise-wide process and centralization of risk management decisions whenever those decisions could impact the enterprise's availability or integrity. For large enterprises consisting of many business elements, this is an organizational challenge for those with distributed and multiple business models. The individual businesses may have different risk tolerances but the enterprise network is an area for "shared risk management." In my view and experience, centralization of an enterprise's key security services produces the most consistent degree of strong security and improves the ability to effectively monitor and determine enterprise-wide compliance with security practice and appropriate configurations. Our experience with this model has demonstrated significant cost efficiencies while at the same time providing more consistent security.

Historical Perspective

For the past 6 years, infrastructure protection has been the increasing focus of U.S. government policy and initiatives, and encouragement of an active public-private partnership has been a hallmark of their strategy.

Historically, the financial services sector has been a leader in addressing the challenges associated with operating the vast array of information technology and processing inherent throughout the financial services industry. Vigilance and the dedication of significant resources over time have allowed us to develop a wealth of expertise, experience and talent to address issues of security, risk management and protection against crimes such as fraud.

The shift to electronic – and increasing mobile – commerce, extended the need for security to individual customers and to implementing networks, servers, software and other devices.

To address the many recommendations proposed in the President's Commission on Critical Infrastructure Protection report, an action plan was developed in May 1998: the Presidential Decision Directive (PDD) 63. The primary banking and

finance sector goal established in PDD-63 was to ensure the orderly functioning of the economy and the delivery of essential services.

The private sector working with its lead agency was to contribute to a sector plan, that included:

- Assessing the vulnerabilities of the sector to cyber or physical attacks,
- Recommending a plan to eliminate significant vulnerabilities,
- Proposing a system for identifying and preventing attempted major attacks, and
- Developing a plan for alerting, containing and rebuffing an attack.

Task areas of initial focus by the sector included:

- Vulnerability education and awareness
- Vulnerability analyses
- Creation of a private sector information sharing and analysis center
- Sector research and development needs

Working groups were established by the banking and finance sector to address these goals. This working group recommended creating the Financial Services Information Sharing and Analysis Center (FS-ISAC), a private-sector partnership among eligible financial services companies designed to anonymously share information regarding security incidents, threats, vulnerabilities and solutions. The financial services sector responded by forming the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC, LLC was created to govern the FS-ISAC for the financial services industry. A board of managers, consisting of interested industry information professionals, was formed. The FS-ISAC was launched on October 1, 1999, by its founding members.

In that same period, industry working groups, consisting of representatives from concerned institutions, were examining awareness and education initiatives and efforts to identify the sector's research and development needs.

Further, to address critical infrastructure interdependency issues or cross-sector critical infrastructure issues, the Partnership for Critical Infrastructure Security (PCIS) was founded in 1999. The PCIS's purpose is to promote and ensure reliable critical infrastructures through cross-sector coordination. PCIS provided a forum for different critical infrastructure sectors to collaborate on cross-sector knowledge sharing and coordination.

In July 2002, in response to a government-issued national cyber security strategy, a working group of our sector's institutions developed an initial national strategy document to address critical infrastructure protection.

These initial efforts on critical infrastructure protection were given more national focus as a result of the terrorist attacks on September 11, 2001. The importance

of ensuring rapid recovery and improved resiliency of business functions and telecommunications were given renewed importance.

Additionally, new global realities and threat environment made it necessary to consider the impact of potential situations that could have broad regional consequences. For the financial services sector, many of these new concerns were discussed in a "Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U. S. Financial System." The agencies had reached conclusions regarding "...the necessity to assure the resilience of critical U.S. financial markets in the face of wide-scale, regional disruptions and identified a number of sound practices to strengthen the resiliency of the overall U.S. financial system and the respective U.S. financial centers."

Most institutions reviewed and enhanced their business continuity efforts in light of these new realities. Collectively, we have been examining and increasing our sector's ability to provide for business continuity and business resumption against situations that may have regional impacts. Our industry is examining and implementing solutions to some multi-faceted issues in this area, which include economic implications, changes in recovery strategies, new back-up facilities and enhanced telecommunications contingencies.

The new realities and challenges we are facing have caused institutions to organize "executive teams" working in a multi-disciplined manner on physical security, cyber security, life safety, disaster recovery, business continuity and business resumption issues.

At Bank of America, we have such an executive team. Collectively, the team is working to provide integrated leadership to address the new realities. This can be viewed as a microcosm at the institution level of the leadership opportunities also being undertaken at the financial services sector level.

Let me discuss further the telecommunications area. Our sector has been working closely with the telecommunications industry to understand ways to improve redundancy and diversity of telecommunication services that support critical financial services functions.

In the telecommunications area, we are not only concerned with addressing reliability resulting from random system failures, but also "survivability" of telecommunications services from targeted attacks on such infrastructures. This is of increased concern when considering the new global realities. This area provides a prime example of opportunities, including research and development that would help achieve resiliency goals, for both the telecommunications and financial services sectors to partner for their collective benefit.

Let me discuss how our sector level critical infrastructure protection efforts have evolved.

Financial Services Sector Coordinating Council

At the time of my appointment, no single entity could legitimately say it represented the financial services sector. Individual associations were actively and effectively working on their members' behalf to provide tools and resources necessary to enhance infrastructure protection. The associations and their members have provided much leadership for our sector and have done outstanding work on various areas, including crisis management efforts, "good practices" knowledge sharing, business continuity practices, and education and awareness initiatives.

Immediately after my appointment in May 2002, we began forming the Financial Services Sector Coordinating Council, with the public sectors' support and encouragement, and with the leadership of the Department of the Treasury.

The council consists of the primary organizations that, through their constituencies, represent the majority of the financial services sector. These include key national exchanges, clearing organizations, trade associations in the banking, securities, bond, and insurance segments of our industry and key professional institutes.

Today, 24 organizations, listed below, are working together to identify and coordinate strategic initiatives that will improve critical infrastructure protection for our sector and with other sectors upon which we depend. The council is a limited liability corporation that has been institutionalized to carry on the sector's work long after my tenure as sector coordinator is completed. Through our council members, we engage nearly all financial services sector institutions, exchanges and utilities.

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security

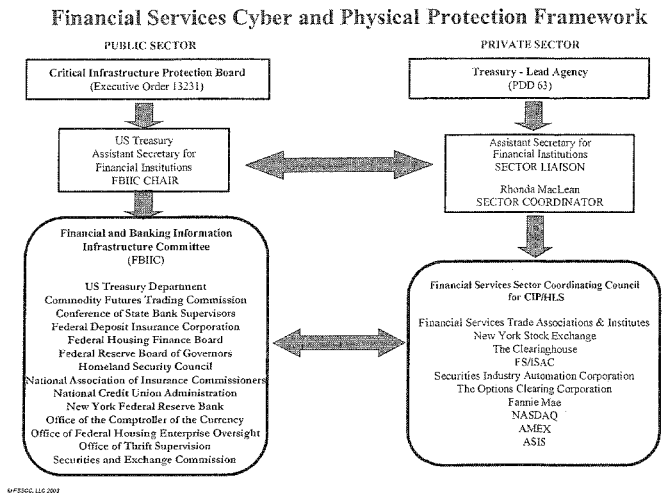
Members

- **ABA** – American Bankers Association
- **ACLI** – American Council of Life Insurers
- **ASIS** – American Society for Industrial Security
- **ACB** – America's Community Bankers
- **BAI** – Bank Administration Institute
- **BITS/FSR** – BITS and The Financial Services Roundtable
- **CUNA** – Credit Union National Association
- **Fannie Mae**
- **CBA** – Consumer Bankers Association
- **FS/ISAC** – Consumer Bankers Association
- **FIA** – Futures Industry Association
- **ICBA** – Independent Community Bankers of America
- **ICI** – Investment Company Institute
- **MFA** – Managed Funds Association
- **NASD** – NASD, Inc.
- **NASQ** – NASDAQ Stock Market, Inc
- **NAFCU** – National Association of Federal Credit Unions
- **NACHA** – National Automated Clearinghouse Association
- **SIA** – Securities Industry Association
- **The BMA** – The Bond Market Association
- **The Clearing House**
- **The OCC** – The Options Clearing Corporation

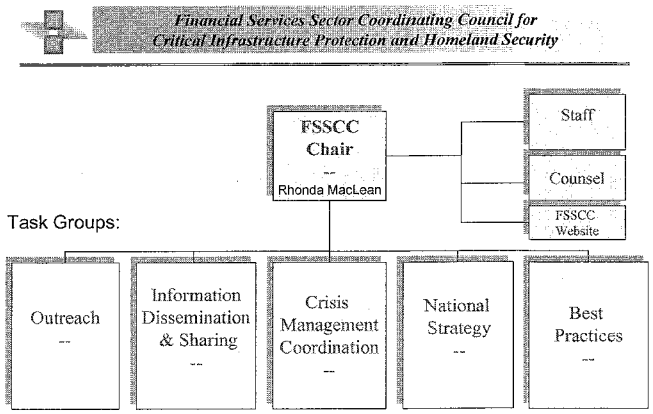
©FSSCC, LLC 2003

At the sector level, this is an example of 'macro' collective leadership being taken to address the new realities. Through this collective leadership and collaboration, we are leveraging the work being performed across the sector for the benefit of the "common good" of our industry. The council model and approach being taken by our sector is being examined by other national critical infrastructure sectors.

This council provides an efficient approach for coordinating the many and diverse participants that comprise our industry sector. Additionally, because there is a corresponding group within the public sector the Financial and Banking Information Infrastructure Committee (FBIIC), chaired by the Treasury Department, we have the opportunity for direct dialogue on common issues and challenges. The result is an emerging agreement on strategic initiatives we believe will improve infrastructure protection and homeland security.



Five initial strategic areas are the current focus of the council's work. Our approach is to leverage the work already accomplished by our council member organizations to achieve our objectives. Council members are taking primary leadership roles, based on their natural areas of expertise.



©FSSCC 2003

Information Dissemination and Information Sharing – Our goal is to ensure that a universal service to disseminate trusted and timely information will be available to all sector participants to increase knowledge about physical and cyber security operational risks faced by the financial services sector. Enhancing the needed services provided by our sector's ISAC is a major focus of our current sector efforts.

Crisis and Response Management – When events occur with broad sector or national impact, a planned and adopted approach for sector-wide crisis management coordination exists, including coordination with government entities. The focus of our efforts is on the ability to communicate and respond as a sector when such events occur.

Sector and Cross Sector Outreach – It is important for each organization to determine how to optimally support and commit efforts for achieving the goals of the executive orders and national strategies. We are developing a strategy for sector-wide outreach on homeland security and critical infrastructure protection initiatives that includes regional forums we are conducting jointly with the FBIIC.

Knowledge Sharing - Best Practices – There are numerous "lessons learned" activities and knowledge sharing of "good practices" within various trade associations and among institutions and government entities. We are developing an organized repository to provide this information to authorized institutions and individuals.

National Strategy – We are also leading the sector's effort to revise our sector's "national strategy" document in response to the two national strategies released in February by the President. The strategies are focused on "The Physical Protection of Critical Infrastructures and Key Assets" and "Securing Cyberspace." This is our opportunity to define strategic as well as tactical, actionable and measurable programming, to direct and advance our sector-wide critical infrastructure and homeland security efforts and to address the recommendations outlined in the national documents strategies referenced above.

In my chairperson role for the FSSCC, I work closely with our lead agency, the Department of Treasury, and the Financial and Banking Information Infrastructure Committee (FBIIC).

It is through council members' cooperative efforts, their member institutions, and the strong leadership provided by the Treasury and through FBIIC, that we are able to maximize our resources and achieve our objectives to ensure protection of our critical infrastructures to the benefit of the economy and to all financial services customers.

Opportunities

Let me transition and discuss several areas of importance to continuing the progress that has been made by both the government and the private sector.

Information Analysis and Infrastructure Protection
The early critical infrastructure protection visionaries of the 90's clearly understood that raising awareness of these issues was an essential first step. That aspect has been fairly well accomplished. Additionally, addressing holistically both the physical and cyber security aspects of critical infrastructure protection and other issues in response to more sophisticated attacks have now been institutionalized in the Department of Homeland Security (DHS). The need for synergy between information analysis and infrastructure protection has clearly been recognized in the assignment of those responsibilities to an undersecretary within DHS. We expect this to provide a much more robust alerting, threat warning and information flow from the public sector based on the vast resources they have available to integrate.

National Strategy
The National Strategy to Secure Cyberspace correctly recognizes a national effort is required. According to the strategy, "The federal government alone cannot sufficiently defend America's cyberspace. Our traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts. Every American who can contribute to securing part of cyberspace is encouraged to do so. The federal government invites the creation of, and participation in, public-private partnerships to raise cyber security awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations."[3]

Understanding the Threat
Based on the governments' visibility of threats to the private sector, a clear understanding of the protection needs must exist between the public and private sector. Gaps between the private sector's protection efforts and the government's view of the necessary protections must be defined and understood. There may be situations where, unknown to the private sector, normal business practices do not adequately address the level of threat understood by the government. Where market forces do not provide the appropriate incentives to provide these protections, augmentation of market mechanisms with such incentives may be appropriate.

Product Security
Because the private sector mainly employs commercial services, products and software to implement cyber security protection and monitoring, those efforts that improve the security of such products have broad benefit As a sector, we work

[3] National Strategy to Secure Cyberspace, February 2003

closely with our vendors to achieve higher levels of security. This is an area that has benefited from both private and public sector efforts. The BITS product certification program is a prime example of our industry's efforts to work closely with the product vendors to meet common criteria and minimum acceptable security standards established by the financial services industry.

Skilled Workforce
In all areas of cyber security, having the best-trained and skilled people is essential to engendering a leadership position for a company and the nation.

The Computing Technology Industry Association commissioned a recent study, the results of which strongly suggest that more training and certification for IT professionals will help America become better protected against mounting cyber threats.

Any incentives and encouragement that bolsters the available talent pool of software developers with a strong security component of their training should result in improved software products.

Voluntary Sharing of Threat and Incident Information
And finally, we must continue to encourage processes that accommodate companies' voluntary sharing of sensitive information, such as the provisions outlined in the Homeland Security Act of 2002. Such provisions of the Critical Information Infrastructure Act of 2002 encourage sharing by providing companies with necessary Freedom of Information Act (FOIA) protections, without giving up the option for government to pursue legal and regulatory action when necessary.

Summary

In summary, our industry is focused on protecting the integrity of the infrastructure for physical as well as electronic delivery of financial services. We have taken steps to ensure the global architecture for financial transactions is as safe, secure and sound as possible.

Our sector has evolved its sector-wide efforts and has committed to a formal structure and entity, the Financial Services Sector Coordinating Council, to foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security.

We are committed to a close public-private partnership to address the new global realities we face as a nation. Where market forces do not adequately address the threats the public sector has identified, appropriate incentives must be structured for those services critical to the national security and national and global economic prosperity. Also, continuing to provide the legal and legislative

mechanisms that permit the exchange of sensitive infrastructure protection information with the government is an essential element of the partnership.

Continually improving commercial product security and increasing the required pool of talented and trained personnel to meet the security development and implementation demands of the innovative information technology all infrastructures employ is a challenge for us all.

Mr. Chairman and Members of the Committee, we believe the strong public/private sector partnership that is emerging is the right approach. The FSSCC would be happy to work with your Committee, staff and other Members of Congress to discuss aspects of the testimony in greater detail.

Thank you for this opportunity to testify.

****

About the Financial Services Sector Coordinating Council for Critical Information Protection and Homeland (CIP/HLS)

The Financial Services Sector Coordinating Council for CIP/HLS fosters and facilitates financial services sector-wide activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The council was created in June 2002, by the private sector, with recognition from the U.S. Treasury, to coordinate critical infrastructure and homeland security initiatives for the financial services industry. The five major areas of immediate focus for the council include: Effective and Rapid Information Dissemination; Crisis Management and Response Coordination; Outreach and Organizational Engagement; Knowledge Sharing and Best Practices and the National Strategies for Homeland and Cyber Security.

About Bank of America

One of the world's leading financial services companies, Bank of America is committed to making banking work for customers and clients like it never has before. Through innovative technologies and the ingenuity of its people, Bank of America provides individuals, small businesses and commercial, corporate and institutional clients across the United States and around the world new and better ways to manage their financial lives. The company enables customers to do their banking and investing whenever, wherever and however they choose through the nation's largest financial services network, including approximately 4,400 domestic offices and 13,000 ATMs, as well as 30 international offices serving clients in more than 150 countries, and an Internet Web site that provides online banking access to 4 million active users, more than any other bank.

Mr. PUTNAM. Thank you very much.

I now recognize Tom Pyke. As Chief Information Office of the U.S. Department of Commerce, Mr. Pyke is responsible for guiding the Department's effective use of information technology and managing the Department's IT resources, with an annual budget of over $1.5 billion. His responsibilities include IT policy, planning, and capital investment review, IT security and critical infrastructure protection, IT architecture, information quality, E-Government, information dissemination through the Internet and the Next Generation Internet, and the oversight of IT operations.

He has been a senior manager of information technology in the Commerce Department for over 30 years, most recently serving as CIO and Director for Higher Performance Computing and Communications of the National Oceanic and Atmospheric Administration and Director of the GLOBE program.

Welcome. You are recognized.

Mr. PYKE. Thank you, Mr. Chairman. I am pleased to be here this morning to share with the subcommittee a summary of the actions that the Commerce Department has taken over the last 2 years to strengthen our information security posture.

The Department's actions to improve its management of information security started at the top. Secretary Don Evans, in June 2001, directed all Commerce agency heads to focus their personal attention on establishing information technology or IT security as a priority. He directed them to allocate the necessary resources to ensure that the Department's data and information systems are adequately protected against risks resulting from misuse or unauthorized access. This important action ensures accountability for IT security by all of the Department's senior managers, and both the Secretary as well as Deputy Secretary Sam Bodman have emphasized this personal responsibility of Commerce agency heads as they have communicated with these senior managers in the Department about the importance of IT security over the past 2 years.

The Secretary also instituted a Department-wide IT management restructuring plan that empowered the Department's CIOs by providing them with the necessary authority to manage IT security as well as other aspects of information technology planning and operations and IT capital investment review. As the Department CIO, I issue security policy and provide IT security guidance to the Commerce agency heads and to the Commerce agency CIOs. I participate in the annual review of the performance of each of the Commerce agency CIOs, which bolsters the authority that my staff and I have at the Department level as we oversee the management of the expenditure of $1.5 billion in information technology each year on a Department-wide basis. This $1.5 billion, by the way, includes the resources that we devote to protecting our systems and information assets through our Department-wide IT security program.

We have issued this January a comprehensive Department-wide IT security policy, as well as minimum standards for management, operational, and technical controls, and other key aspects of implementing this policy. We also issued a Password Management Policy and a Remote Access Security Policy. Policy implementation guides have been issued that address critical corrective action plans to identify and correct security weaknesses, to document security and

privacy in the IT capital asset planning process, and to maintain complete inventories of all of our systems relative to their security status.

The Department instituted a compliance monitoring process in 2002, through which we determine Commerce agency compliance with Department IT security policies, standards, and guidance. This process includes tests of all management, operational, and technical controls, including tests of systems and networks to ensure that they are adequately protected against unauthorized access. We also established an IT security training program, through which every Commerce employee and every contractor employee has received IT security awareness training, and is receiving updated training every year. Specialized training for IT security personnel, managers, and system administrators is also being provided.

The Department has established a computer incident response capability that supports actions to protect systems and data when incidents do occur, and facilitates proper reporting of incidents. A Department-wide IT security alert capability has also been established, that ensure 24 x 7 transmittal of IT security alerts throughout the Department and activation of Commerce agency IT security emergency mobilization plans, as appropriate.

Especially since the Commerce Department has been coming from behind as it has implemented this comprehensive IT security program, numerous corrective actions have been identified that need special attention to correct IT security weaknesses. A Department-wide data base of needed corrective actions has been created and is being maintained. It includes every IT security action that has resulted from GAO and Commerce Office of Inspector General audits, as well as actions that have resulted from Department IT security compliance reviews and from self-assessments by the Commerce agencies themselves. We expect to complete by this September all of the corrective actions that were open at the beginning of fiscal year 2003. Over 74 percent of these actions are already completed. We expect to have completed by the end this fiscal year all but 2 of the over 200 corrective actions that have been identified during this fiscal year.

The top level measure we use to manage IT security across the Department is what we call IT security program maturity. By the end of fiscal year 2003, we expect that every Commerce agency will be operating at ease at a level 3 maturity, which requires that all IT systems have implemented policies and procedures. We have identified our national critical and mission critical IT assets and the IT system components of those assets, and we expect to have certification and accreditation for full operation of these systems completed by the end of this fiscal year.

I would like to tell you very briefly how we are doing against some of the performance measures that Mark Forman introduced in his testimony this morning, in which he provided Government-wide data. At Commerce, we have assessed 96 percent of our systems for risk, 90 percent of our systems have contingency plans, 92 percent are certified and accredited, and 98 percent of our systems have up to date IT security plans.

Thank you for this opportunity to tell you about what we have done in the Commerce Department to improve our information security posture. We have come a long way in these last 2 years, and we are working hard to complete the next steps that are essential to provide adequate protection of our data and systems. We understand, however, that IT security is a never-ending process, and we are committed to maintaining a high level of vigilance to ensure that the Department is able to carry out its mission without disruption caused by cyber threats.

[The prepared statement of Mr. Pyke follows:]

TESTIMONY OF
THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF COMMERCE
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
UNITED STATES HOUSE OF REPRESENTATIVES

APRIL 8, 2003

Good morning, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer of the Department of Commerce. I am pleased to be here this morning to share with the Subcommittee a summary of the actions the Department of Commerce has taken over the last two years to strengthen our cyber security, or information security, posture.

The Department's actions to improve its management of information security started at the top. Secretary Don Evans directed all Commerce agency heads to focus their attention on establishing information technology (IT) security as a priority in June 2001. He directed that they allocate necessary resources to ensure that the Department's data and information systems are adequately protected against risks resulting from misuse or unauthorized access. This important action ensures accountability for IT security by all of the Department's senior managers, and both the Secretary and Deputy Secretary Sam Bodman have emphasized this personal responsibility of Commerce agency heads as they have communicated with them about the importance of IT security during the last two years.

The Secretary also instituted a Department-wide IT restructuring plan that empowered the Department's CIOs by providing them with the necessary authority to manage IT security as well as IT planning and operations and IT capital investment review. As the Department CIO, I issue IT security policy and provide IT security guidance to the Commerce agency heads and to their CIOs. I participate in the annual review of the performance of each of the Commerce agency CIOs, which bolsters the authority I have to ensure effective management of the Department's $1.5 billion annual expenditure on information technology, including the protection of our IT resources through a Department-wide IT Security Program.

We have issued in January 2003, a comprehensive, Department-wide IT Security policy, as well as minimum standards for management, operational, and technical controls and other key aspects of implementing this policy. We also issued a password management policy, in June 2002, and a Remote Access Security Policy, in December 2002. Policy implementation guides have been issued that address corrective action planning to identify and correct security weaknesses, documentation of security and privacy in the IT capital asset planning process, and maintaining complete inventories of the security status of all IT systems.

The Department instituted a compliance monitoring process in 2002, through which we determine Commerce agency compliance with Department IT security policies, standards, and guidance. This process includes tests of all management, operational, and technical controls, including tests of systems and networks, to ensure that they are

adequately protected against unauthorized access. We have also established an IT security training program, through which every Commerce employee and contractor employee has received IT security awareness training, and is receiving updated training every year. Specialized training for IT security personnel, managers, and system administrators is also being provided.

The Department has established a computer incident response capability that supports actions to protect systems and data when incidents occur, and facilitates proper reporting of incidents. A Department-wide IT security alert capability has also been established, that ensures 24 hours a day, 7 days a week transmittal of IT security alerts throughout the Department and activation of Commerce agency emergency mobilization plans, as appropriate.

Especially since the Commerce Department has been "coming from behind" as it has implemented this comprehensive IT security program, numerous corrective actions have been identified that need special attention to correct identified weaknesses. A Department-wide database of needed corrective actions has been created and is being maintained. It includes every IT security action resulting from GAO and Commerce Office of Inspector General audits, as well as actions resulting from Department IT security compliance reviews and Commerce agency self-assessments. We expect to complete by this September all of the corrective actions that were open at the beginning of FY 2003. Over 74% of these actions are already completed. We also expect to have

completed by the end of FY 2003 all but two of the over 200 new needed corrective actions that have been identified during FY 2003.

The top level measure we use to manage IT security across the Department is what we call IT security program "maturity." By the end of FY 2003, we expect that every Commerce agency will be operating at least at a Level 3 maturity, which requires that all IT systems have implemented policies and procedures. We have identified our national critical and mission critical IT assets and the IT system components of those assets, and we expect to have certification and accreditation for full operation of these systems completed by the end of FY 2003. This represents a very important step toward a greatly strengthened Department-wide IT security program.

I would like to call to your attention a resource that has been especially helpful as we have strengthened the Department's IT security program. This resource is our very own Computer Security Division within the Department's National Institute of Standards and Technology. The standards and guidelines and related products issued by the Computer Security Division are intended for use throughout the Federal Government, and I am proud to say that the Department itself is benefiting significantly from use of these products.

Thank you for this opportunity to tell you about what we have done in the Commerce Department to improve our information security posture. We have come a long way during the last two years, and we are working hard to complete the next steps that are

essential to provide adequate protection of our data and systems. We understand, however, that IT security is a never-ending process, and we are committed to maintaining a high level of vigilance to ensure that the Department is able to carry out its mission without disruption caused by cyber threats. I would be pleased to respond to any questions you may have.

Mr. PUTNAM. Thank you, Mr. Pyke.

At this time, the subcommittee recognizes Robert Dacey. Mr. Dacey is currently Director of Information Security Issues at the U.S. General Accounting Office. His responsibilities include evaluating information systems security in Federal agencies and corporations, including the development of related methodologies; assessing the Federal infrastructure for managing information security; evaluating the Federal Government's efforts to protect our Nation's private and public critical infrastructure from cyber threats; and identifying the best security practices at leading organizations and promoting their adoption by Federal agencies.

Previously, Mr. Dacey led GAO's annual audits of the consolidated financial statements of the U.S. Government, audits I think which revealed about the same grades as they have been getting on their IT scorecards; GAO's financial audit quality assurance efforts, including methodology and training; and other GAO financial statement audit efforts, including HHS and the IRS.

Welcome to the subcommittee. You are recognized for 5 minutes.

Mr. DACEY. Thank you, Mr. Chairman, Mr. Clay. I am pleased to be here today to discuss the challenges our Nation faces concerning Federal information security and critical infrastructure protection. CIP involves activities that enhance the security of our Nation's cyber and physical public and private infrastructures that are essential to national security, economic security, and/or public health and safety. As you requested, I will briefly summarize my written statement which provides details on the status and progress of efforts to address these challenges.

We have identified and made numerous recommendations over the last several years concerning Federal information security and CIP challenges that need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in progress. However, much more is needed to fully address them. These challenges include: One, addressing pervasive weaknesses in Federal information security. Our analysis of audit and evaluation reports in November of last year continued to show significant pervasive weaknesses in Federal unclassified computer systems for all 24 major agencies reviewed that put critical operations and assets at risk. The implementation of GISRA continues to play a significant role in the improvement of Federal information security. Second year agency GISRA reports indicate agency progress, provide comparative performance information and an improved performance baseline, and highlight areas where additional efforts are necessary. The administration has taken important actions to address information security, such as integrating it into the President's Management Agenda Scorecard.

The successful implementation of FISMA, which permanently authorizes and strengthens GISRA requirements, is essential to sustaining these agency efforts to identify and correct significant weaknesses. As FISMA is implemented, it will be important to continue efforts to certify, accredit, and regularly test systems to identify and correct vulnerabilities in all agency systems; two, to complete development and test contingency plans to ensure that critical systems can resume after an emergency; three, to validate

agency reported information through independent evaluation; and four, to achieve other FISMA requirements.

The second major challenge is the development of a national CIP strategy. A more complete strategy is still needed that addresses specific roles, responsibilities, and relationships for all CIP entities, that clearly defines interim objectives and milestones and sets timeframes for achieving them, and establishes appropriate performance measures and a monitoring process. The President's National Homeland Security strategy, the President's cyber and physical CIP strategies, and the Homeland Security Act call for a comprehensive national infrastructure plan.

The third major challenge is improving information sharing on threats and vulnerabilities. Information sharing needs to be enhanced both within the Federal Government and between the Federal Government and the private sector and State and local governments. The President's national strategies identify partnering with non-Federal entities as a major initiative. Information sharing and analysis centers continue to play a key role in this strategy.

The fourth major challenge is improving analysis and warning capabilities. More robust warning and analysis capabilities are needed to identify threats and provide timely warning. Such capabilities need to address both cyber and physical threats. Again, the President's national strategies call for major initiatives in this area.

The fifth challenge is encouraging non-Federal entities to increase their CIP efforts. The Federal Government needs to assess whether additional incentives, such as grants or regulation, are needed to encourage non-Federal entities to increase their efforts to implement suggested CIP activities.

The Homeland Security Act and the President's national strategies acknowledge the need to address many of these challenges. However, much work remains to effectively respond to them. Until a comprehensive and coordinated strategy is developed, our Nation risks not having a consistent and appropriate structure to deal with the growing threat of attacks on its Federal systems and on its critical infrastructures.

Mr. Chairman, Mr. Clay, this concludes my oral statement. I would be pleased to answer any questions at this time.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
9:30 a.m. EDT
Tuesday,
April 8, 2003

INFORMATION SECURITY

Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-03-564T

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-03-564T, a testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

Why GAO Did This Study

Protecting the computer systems that support federal agencies' operations and our nation's critical infrastructures—such as power distribution, telecommunications, water supply, and national defense—is a continuing concern. These concerns are well-founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks. GAO first designated computer security as high risk in 1997, and in 2003 expanded this high-risk area to include protecting the systems that support our nation's critical infrastructures, referred to as cyber critical infrastructure protection or cyber CIP.

GAO has made previous recommendations and periodically testified on federal information security weaknesses—including agencies' progress in implementing key legislative provisions on information security—and the challenges that the nation faces in protecting our nation's critical infrastructures. GAO was asked to provide an update on the status of federal information security and CIP.

www.gao.gov/cgi-bin/getrpt?GAO-03-564T.

To view the full testimony, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

April 8, 2003

INFORMATION SECURITY

Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures

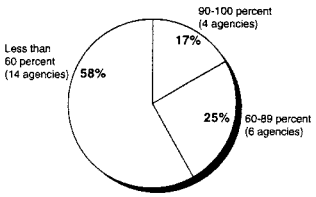
What GAO Found

With the enactment of the Federal Information Security Management Act of 2002, the Congress continued its efforts to improve federal information security by permanently authorizing and strengthening key information security requirements. The administration has also made progress through a number of efforts, among them the Office of Management and Budget's emphasis of information security in the budget process.

However, significant information security weaknesses at 24 major agencies continue to place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. Although recent reporting by these agencies showed some improvements, GAO found that agencies still have not established information security programs consistent with the legal requirements. For example, periodic testing of security controls is essential to security program management, but for fiscal year 2002, 14 agencies reported they had tested the controls of less than 60 percent of their systems (see figure below). Further information security improvement efforts are also needed at the governmentwide level, and these efforts need to be guided by a comprehensive strategy in which roles and responsibilities are clearly delineated, appropriate guidance is given, adequate technical expertise is obtained, and sufficient agency information security resources are allocated. Although improvements have been made in protecting our nation's critical infrastructures and continuing efforts are in progress, further efforts are needed to address critical challenges that GAO has identified over the last several years. These challenges include

- developing a comprehensive and coordinated national CIP plan;
- improving information sharing on threats and vulnerabilities between the private sector and the federal government, as well as within the government itself;
- improving analysis and warning capabilities for both cyber and physical threats; and
- encouraging entities outside the federal government to increase their CIP efforts.

Percentage of systems with security controls tested during fiscal year 2002



Source: Agency-reported data

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the challenges that our nation faces concerning federal information security and critical infrastructure protection (CIP). Federal agencies and other public and private entities rely extensively on computerized systems and electronic data to support their missions. CIP involves activities that enhance the security of the cyber and physical public and private infrastructures that are essential to our national security, national economic security, and/or national public health and safety. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of sensitive information. Further, protecting against computer-based attacks on critical infrastructures is an important aspect of homeland security.

The Congress has continued to hold important hearings and has passed legislation that the President has signed into law to strengthen information security practices throughout the federal government and to better address threats to the nation's critical computer-dependent infrastructures. Such legislation includes Government Information Security Reform provisions (commonly known as "GISRA"), which established information security program, evaluation, and reporting requirements for federal agencies;[1] the recently enacted Federal Information Security Management Act of 2002 ("FISMA"), which permanently authorized and strengthened GISRA;[2] and the Homeland Security Act of 2002, which, among other things, consolidated certain essential CIP functions and organizations in the Department of Homeland Security.

In my testimony today, I will provide an overview of the increasing nature of cyber security threats and vulnerabilities and of the continuing pervasive weaknesses that led GAO to initially begin reporting information security as a governmentwide high-risk issue in 1997. I will then discuss the status of actions taken by the Office of Management and Budget (OMB) to address overall weaknesses and challenges identified through its GISRA analyses, as well as the federal government's continuing need to be guided by a comprehensive improvement strategy. I will also discuss the results of our evaluation of efforts by 24 of the largest federal agencies to implement the requirements of GISRA and to identify and correct their

[1]Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L.106-398, October 30, 2000.

[2]Title III—Federal Information Security Management Act of 2002, E-Government Act of 2002, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.

information security weaknesses.[3] Finally, I will discuss the federal government's evolving approach to and current strategies for protecting our nation's critical infrastructures. In this discussion, I will highlight the challenges, identified in prior GAO work that the nation continues to face in implementing CIP. These challenges include developing a comprehensive and coordinated national CIP plan, implementing better information sharing on threats and vulnerabilities, improving analysis and warning capabilities, and ensuring appropriate incentives to encourage nonfederal CIP efforts. In January 2003, GAO expanded its information security high-risk issue to include cyber CIP.[4]

As agreed, this testimony incorporates the preliminary results of our analyses of federal agencies' efforts to implement GISRA information security requirements during fiscal year 2002, which was originally requested by the chair and ranking minority member of a former subcommittee of the House Government Reform Committee. In conducting this review, we analyzed (1) executive summaries and reports that summarized management reviews by the 24 agencies for their information security programs, (2) inspector general (IG) summaries and reports on their independent evaluations of these agencies' programs, and (3) agency plans to correct their identified information security weaknesses. We did not validate the accuracy of the data provided in these summaries, reports, and plans. We also discussed with OMB officials the status of their actions and initiatives to improve and provide additional guidance for federal information security. We performed our work from September 2002 to April 2003 in accordance with generally accepted government auditing standards.

Results in Brief

Protecting the computer systems that support our nation's critical operations and infrastructures is a continuing concern. Telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. Yet with this dependency comes an increasing concern about attacks from individuals and groups

[3]These are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, the Environmental Protection Agency, Federal Emergency Management Agency (FEMA), General Services Administration, Office of Personnel Management, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[4]U.S. General Accounting Office, *High Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. Such concerns are well founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks.

With the enactment of FISMA, the Congress continued its efforts to improve federal information security by permanently authorizing and strengthening the information security program, evaluation, and reporting requirements established by GISRA. The administration has also made progress through a number of efforts, including OMB's emphasis of information security in the budget process and e-government initiatives and the National Institute of Standards and Technology's (NIST) issuance of additional computer security guidance. However, our recently reported analyses of audit and evaluation reports issued from October 2001 to October 2002 for 24 major agencies showed that significant information security weaknesses continue to place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, all 24 agencies had weaknesses in security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. In addition, although our most recent analyses of fiscal year 2002 GISRA reporting by these agencies showed some improvements, agencies still have not established information security programs consistent with the requirements of GISRA. For example, although the percentage of systems assessed for risk increased for 13 agencies, for 9 agencies, less than 60 percent of their systems had risk assessments (an essential element of risk management and overall security program management that helps ensure that the greatest risks have been identified and addressed). Further, although 15 agencies reported increases in the number of systems for which controls had been tested and evaluated, 14 reported that controls had been tested for less than 60 percent of their systems.

As we have previously recommended, further information security improvement efforts are needed at the governmentwide level, and it is important that these efforts are guided by a comprehensive strategy. As the development of this strategy continues, there are a number of important steps that the administration and the agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These steps include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of CIP; providing more specific guidance on the controls that agencies need to implement; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems; and allocating sufficient agency resources for information security.

Federal awareness of the importance of securing our nation's critical infrastructures has continued to evolve since the mid-1990s. Over the years, a variety of working groups has been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. Although the actions taken to date are major steps to more effectively protect our nation's critical infrastructures, we have identified and made numerous recommendations over the last several years concerning critical infrastructure challenges that need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in progress. However, even greater efforts are needed to address them. These challenges include the following:

- *Developing a comprehensive and coordinated national CIP plan.* A more complete plan is needed that will address specific roles, responsibilities, and relationships for all CIP entities; clearly define interim objectives and milestones; set time frames for achieving objectives; and establish performance measures.
- *Improving information sharing on threats and vulnerabilities.* Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber and physical attacks, which could threaten the national welfare. Information sharing needs to be enhanced both within the government and between the federal government and the private sector and state and local governments.
- *Improving analysis and warning capabilities.* More robust analysis and warning capabilities, including an effective methodology for strategic analysis and framework for collecting needed threat and vulnerability information, are still needed to identify threats and provide timely warnings. Such capabilities need to address both cyber and physical threats.
- *Encouraging entities outside the federal government to increase their CIP efforts.* Although budget requests include funds (1) to identify key critical infrastructure vulnerabilities and support the necessary steps to ensure that our nation's critical infrastructures are adequately secured across all critical infrastructure sectors and (2) for outreach efforts to state and local government and the private sector, incentives will still be needed to encourage nonfederal entities to increase their CIP efforts. These incentives could include grants, regulations, tax incentives, and regional coordination and partnership.

It is also important that CIP efforts are appropriately integrated with the transition of certain CIP functions and entities to the new Department of Homeland Security (DHS).

Incidents, Threats, and Potential Attack Consequences are Significantly Increasing

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups.

However, in addition to such benefits, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. The speed and accessibility that create the enormous benefits of the computer age on the other hand, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Table 1 summarizes the key threats to our nation's infrastructures, as observed by the Federal Bureau of Investigation (FBI).

Table 1: Threats to Critical Infrastructure Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence,* can affect the daily lives of Americans across the country.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation unless otherwise indicated

*Prepared Statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.[5] In addition, the disgruntled organization insider is a significant

[5] *Virus:* a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse:* a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Worm:* an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Logic bomb:* in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer:* synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

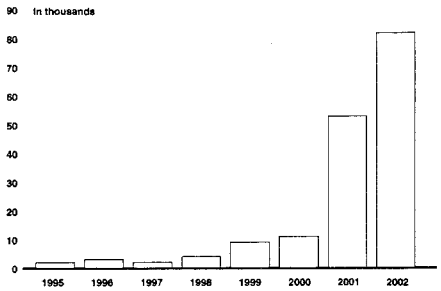
threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology (IT), the likelihood increases that information attacks will threaten vital national interests.

As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A hacker can literally download tools from the Internet and "point and click" to start an attack. Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

Along with these increasing threats, the number of computer security incidents reported to the CERT® Coordination Center[8] has also risen dramatically from 9,859 in 1999 to 52,658 in 2001 and 82,094 in 2002. And these are only the reported attacks. The Director of CERT Centers stated that he estimates that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attack, or (2) the organization was reluctant to report. Figure 1 shows the number of incidents reported to the CERT Coordination Center from 1995 through 2002.

[8]The CERT® Coordination Center (CERT® CC) is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT Coordination Center from 1995 through 2002



Source: Carnegie-Mellon's CERT® Coordination Center.

According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in February 2002, the threat to these infrastructures was highlighted by the Special Advisor to the President for Cyberspace Security in a Senate briefing when he stated that although to date none of the traditional terrorists groups, such as al Qaeda, have used the Internet to launch a known assault on the United States' infrastructure, information on water systems was discovered on computers found in al Qaeda camps in Afghanistan.[7] Also, in his February 2002 statement for the Senate Select Committee on Intelligence, the director of central intelligence discussed the possibility of cyber warfare attack by terrorists.[8] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

[7]"Administrative Oversight: Are We Ready for A CyberTerror Attack?" Testimony before the Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, by Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the President's Critical Infrastructure Protection Board (Feb. 13, 2002).

[8]Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 6, 2002.

Since September 11, 2001, the critical link between cyberspace and physical space has been increasingly recognized. In his November 2002 congressional testimony, the Director of the CERT Centers at Carnegie-Mellon University noted that supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems, and that these control systems are increasingly being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions.[9] These computer-controlled and network-connected systems are potential targets for individuals bent on causing massive disruption and physical damage, and the use of commercial, off-the-shelf technologies for these systems without adequate security enhancements can significantly limit available approaches to protection and may increase the number of potential attackers.

The risks posed by this increasing and evolving threat are demonstrated in reports of actual and potential attacks and disruptions. For example:

- On February 11, 2003, the National Infrastructure Protection Center (NIPC) issued an advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq.[10] This advisory noted that during a time of increased international tension, illegal cyber activity often escalates, such as spamming, Web page defacements, and denial-of-service attacks. Further, this activity can originate within another country that is party to the tension; can be state sponsored or encouraged; or can come from domestic organizations or individuals independently. The advisory also stated that attacks may have one of several objectives, including political activism targeting Iraq or those sympathetic to Iraq by self-described "patriot" hackers, political activism or disruptive attacks targeting United States systems by those opposed to any potential conflict with Iraq, or even criminal activity masquerading or using the current crisis to further personal goals.
- According to a preliminary study coordinated by the Cooperative Association for Internet Data Analysis (CAIDA), on January 25, 2003, the SQL Slammer worm (also known as "Sapphire") infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the Internet, making it the fastest computer worm in

[9]Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, November 19, 2002.

[10]National Infrastructure Protection Center, *National Infrastructure Protection Center Encourages Heightened Cyber Security as Iraq—U.S. Tensions Increase*, Advisory 03-002 (Washington, D.C.: Feb.11, 2003).

history. As the study reports, exploiting a known vulnerability for which a patch has been available since July 2002, Slammer doubled in size every 8.5 seconds and achieved its full scanning rate (55 million scans per second) after about 3 minutes. It caused considerable harm through network outages and such unforeseen consequences as canceled airline flights and automated teller machine (ATM) failures. Further, the study emphasizes that the effects would likely have been more severe had Slammer carried a malicious payload, attacked a more widespread vulnerability, or targeted a more popular service.

- In November 2002, news reports indicated that a British computer administrator was indicted on charges that he broke into 92 U.S. computer networks in 14 states; these networks belonged to the Pentagon, private companies, and the National Aeronautics and Space Administration during the past year, causing some $900,000 in damage to computers. According to a Justice Department official, these attacks were one of the biggest hacks ever against the U.S. military. This official also said that the attacker used his home computer and automated software available on the Internet to scan tens of thousands of computers on U.S. military networks looking for ones that might suffer from flaws in Microsoft Corporation's Windows NT operating system software.

- On October 21, 2002, NIPC reported that all the 13 root-name servers that provide the primary roadmap for almost all Internet communications were targeted in a massive "distributed denial of service" attack. Seven of the servers failed to respond to legitimate network traffic, and two others failed intermittently during the attack. Because of safeguards, most Internet users experienced no slowdowns or outages.

- In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure.[11] As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For instance, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack. Consistent with this threat, NIPC also released an information

[11]National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption* (Washington, D.C.: July 2002).

bulletin in April 2002 warning against possible physical attacks on U.S. financial institutions by unspecified terrorists.[12]

- In August 2001, we reported to a subcommittee of the House Government Reform Committee that the attacks referred to as Code Red, Code Red II, and SirCam had affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations. Then in September 2001, the Nimda worm appeared using some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus that allowed it to spread widely in a short amount of time. Security experts estimate that Code Red, Sircam, and Nimda have caused billions of dollars in damage.[13]

Significant Weaknesses Persist in Federal Information Security

For the federal government, we have reported since 1996 that poor information security is a widespread problem with potentially devastating consequences.[14] Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. For the past several years, we have analyzed audit results for 24 of the largest federal agencies and found that all 24 had significant information security weaknesses.[15] Further, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2003.[16]

As we reported in November 2002, our analyses of reports issued from October 2001 through October 2002, continued to show significant weaknesses in federal computer systems that put critical operations and

[12]National Infrastructure Protection Center, *Possible Terrorism Targeting of US Financial System*–Information Bulletin 02-003 (Washington, D.C.: Apr. 19, 2002).

[13]U.S. General Accounting Office, *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures*, GAO-01-1073T (Washington, D.C.: Aug. 29, 2001).

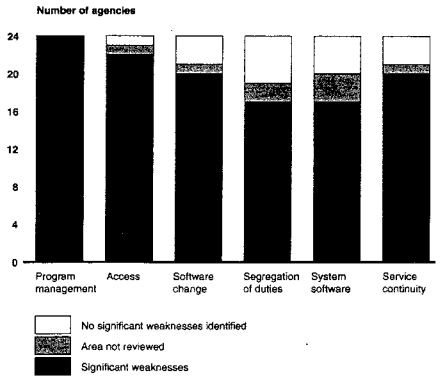
[14]U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

[15]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000); *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001), and *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk, GAO-02-303T (Washington, D.C.: Nov. 19, 2002).*

[16]GAO-03-121.

assets at risk.[17] Weaknesses continued to be reported in each of the 24 agencies included in our review,[18] and they covered all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. Figure 2 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

Figure 2: Computer Security Weaknesses at 24 Major Federal Agencies



Source: Audit reports issued October 2001 through October 2002.

[17] *GAO-03-303T.*

[18] *Does not include the Department of Homeland Security that was created by the Homeland Security Act in November 2002.*

Although our analyses showed that most agencies had significant weaknesses in these six control areas, as in past years' analyses, weaknesses were most often identified for security program management and access controls.

- For *security program management*, we identified weaknesses for all 24 agencies in 2002—the same as reported for 2001, and compared to 21 of the 24 agencies (88 percent) in 2000. Security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls, covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.

- For *access controls*, we found weaknesses for 22 of 24 agencies (92 percent) in 2002 (no significant weaknesses were found for one agency, and access controls were not reviewed for another). This compares to access control weaknesses found in all 24 agencies for both 2000 and 2000. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise.

Our analyses also showed service-continuity-related weaknesses at 20 of the 24 agencies (83 percent) with no significant weaknesses found for 3 agencies (service continuity controls were not reviewed for another). This compares to 19 agencies with service continuity weaknesses found in 2001 and 20 agencies found in 2000. Service continuity controls are important in that they help ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. If service continuity controls are inadequate, an agency can lose the capability to process, retrieve, and protect electronically maintained information, which can significantly affect an agency's ability to accomplish its mission. Further, such controls are particularly important in the wake of the terrorist attacks of September 11, 2001.

These analyses of information security at federal agencies also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. These increases in reported weaknesses do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security

weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 2 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily nonfinancial, such as DOD and the Department of Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of individual systems supporting nonfinancial operations. However, in response to congressional interest, beginning in fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations—a trend we expect to continue. Audit coverage for nonfinancial systems has also increased as agencies and their IGs reviewed and evaluated their information security programs as required by GISRA.

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high.

The weaknesses identified place a broad array of federal operations and assets at risk. For example,

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and

- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Congress Consolidates and Strengthens Federal Information Security Requirements

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, on October 30, 2000, Congress enacted GISRA, which became effective November 29, 2000, for a period of 2 years. GISRA supplemented information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and was consistent with existing information security guidance issued by the Office of Management and Budget (OMB)[19] and the National Institute of Standards and Technology (NIST),[20] as well as audit and best practice guidance issued by GAO.[21]

Most importantly, however, GISRA consolidated these separate requirements and guidance into an overall framework for managing information security and established new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight. GISRA assigned specific responsibilities to OMB, agency heads and chief information officers (CIOs), and IGs. OMB was responsible for establishing and overseeing policies, standards, and guidelines for information security. This included the authority to approve agency information security programs, but delegated OMB's responsibilities regarding national security systems to national security agencies. OMB was also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs. GISRA does not specify a date for this report, and OMB released its fiscal year 2001 report in February 2002. It has not yet released its fiscal year 2002 report.

[19] *Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.*

[20] *Numerous publications made available at http://www.itl.nist.gov/ including National Institute of Standards and Technology,* Generally Accepted Principles and Practices for Securing Information Technology Systems, *NIST Special Publication 800-14, September 1996.*

[21] *U.S. General Accounting Office,* Federal Information System Controls Manual, Volume I—Financial Statement Audits. *GAO/AIMD-12.19.6 (Washington, D.C.: January 1999);* Information Security Management: Learning from Leading Organizations. *GAO/AIMD-98-68 (Washington, D.C.: May 1998).*

GISRA required each agency, including national security agencies, to establish an agencywide risk-based information security program to be overseen by the agency CIO and ensure that information security is practiced throughout the life cycle of each agency system. Specifically, this program was to include

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- the development and implementation of risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained by or for the agency;
- training on security responsibilities for information security personnel and on security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;
- a process for identifying and remediating any significant deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- an annual program review by agency program officials.

In addition to the responsibilities listed above, GISRA required each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. The evaluations of non-national-security systems were to be performed by the agency IG or an independent evaluator, and the results of these evaluations were to be reported to OMB. For the evaluation of national security systems, special provisions included having national security agencies designate evaluators, restricting the reporting of evaluation results, and having the IG or an independent evaluator perform an audit of the independent evaluation. For national security systems, only the results of each audit of an evaluation are to be reported to OMB.

With GISRA expiring on November 29, 2002, on December 17, 2002, FISMA was enacted as title III of the E-Government Act of 2002. This act permanently authorizes and strengthens the information security program, evaluation, and reporting requirements established by GISRA. In addition, among other things, FISMA requires NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and

information systems in each category. In addition, FISMA requires each agency to develop, maintain, and annually update an inventory of major information systems (including major national security systems) operated by the agency or under its control. This inventory is also to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

Agencies Show Progress in Implementing Security Requirements, but Further Improvement Needed

In our March 2002 testimony, we reported that the initial implementation of GISRA was a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses.[22] Agencies also noted benefits of this first-year implementation, including increased management attention to and accountability for information security, and the administration undertook other important actions to address information security, such as integrating information security into the President's Management Agenda Scorecard. However, along with these benefits, agencies' reviews of their information security programs showed that agencies had not established information security programs consistent with the legislative requirements and that significant weaknesses existed. We also noted that although agency actions were under way to strengthen information security and implement these requirements, significant improvement would require sustained management attention and OMB and congressional oversight.

Our analysis of second-year or fiscal year 2002 implementation of GISRA showed progress in several areas, including the types of information being reported and made available for oversight, governmentwide efforts to improve information security, and agencies' implementation of information security requirements. Despite this progress, our analyses of agency and IG reports showed that the 24 agencies have not yet established information security programs consistent with legislative requirements and that corrective action plans did not always include all identified weaknesses and need independent validation to ensure that weaknesses are corrected.

[22]U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation, GAO-02-470T (Washington, D.C.: Mar. 6, 2002).*

OMB Includes New Reporting Requirements to Improve Information Available for Oversight

For fiscal year 2002 GISRA reporting, OMB provided the agencies with updated reporting instructions and guidance on preparing and submitting plans of action and milestones (corrective action plans).[23] Like instructions for fiscal year 2001, this updated guidance listed specific topics that the agencies were to address, many of which were referenced back to corresponding requirements of GISRA.[24] However, in response to agency requests and recommendations we made to OMB as a result of our review of fiscal year 2001 GISRA implementation,[25] this guidance also incorporated several significant changes to help improve the consistency and quality of information being reported for oversight by OMB and the Congress. These changes included the following:

- Reporting instructions provided new high-level management performance measures that the agencies and IGs were required to use to report on agency officials' performance. According to OMB, most agencies did not provide performance measures or actual levels of performance where asked to do so for fiscal year 2001 reporting, and the agencies requested that OMB develop such measures. These required performance measures include, for example, the number and percentage of systems that have been assessed for risk, the number of contractor operations or facilities that were reviewed, and the number of employees with significant security responsibilities that received specialized training.
- Instructions confirmed that agencies were expected to review all systems annually. OMB explained that GISRA requires senior agency program officials to review each security program for effectiveness at least annually, and that the purpose of the security programs discussed in GISRA is to ensure the protection of the systems and data covered by the program. Thus, a review of each system is essential to determine the program's effectiveness, and only the depth and breadth of such system reviews are flexible.
- Agencies were generally required to use all elements of NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, to review their systems. This guide accompanies

[23] *"Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones," Memorandum for Heads of Executive Departments and Agencies, Mitchell E. Daniels, Jr., M-02-09, July 2, 2002.*

[24] *OMB required the agency heads to submit their reports on September 16, 2002, and to include (1) the executive summary developed by the agency CIO, agency program officials, and the IG that is based on the results of their work; (2) copies of the IG's independent evaluations; and (3) for national security systems, audits of the independent evaluations. Agencies' corrective action plans were due to OMB by October 1, 2002, with updates required quarterly beginning January 1, 2003.*

[25] *U.S. General Accounting Office,* Information Security: Additional Actions Needed to Fully Implement Reform Legislation, *GAO-02-407 (Washington, D.C.: May 2, 2002).*

NIST's Security Assessment Framework methodology, which agency officials can use to determine the current status of their security programs.[26] The guide itself uses an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. For the fiscal year 2001 reporting period, OMB encouraged agencies to use this guide, but did not require its use because it was not completed until well into the reporting period. NIST finalized the guide in November 2001, and for fiscal year 2002 reporting, OMB required its use unless an agency and its IG confirmed that any agency-developed methodology captured all elements of the guide. To automate the completion of the questionnaire, NIST also developed a tool that can be found at its Computer Security Resource Center Web site: http://csrc.nist.gov/asset/.

- OMB requested IGs to verify that agency corrective action plans identify all known security weaknesses within an agency, including components, and are used by the IG and the agency, major components, and program officials within them, as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps.
- OMB authorized agencies to release certain information from their corrective action plans to assist the Congress in its oversight responsibilities. Agencies could release this information, as requested, excluding certain elements, such as estimated funding resources and the scheduled completion dates for resolving a weakness.

OMB Initiatives to Improve Federal Information Security Show Progress

OMB's report to the Congress on fiscal year 2001 GISRA implementation provided an overview of OMB and agencies' implementation efforts, summarized the overall results of OMB's analyses, and included individual agency summaries for the 24 of the largest federal departments and agencies.[27] Overall, OMB reported that although examples of good security exist in many agencies, and others were working very hard to improve their performance, many agencies had significant deficiencies in every important area of security. In particular, the report highlighted six common security weaknesses. These weaknesses are listed below along with an update of the activities under way to address them.

1. *Lack of senior management attention to information security*—Last year, OMB reported that, to address this issue, it was working through the

[26] National Institute of Standards and Technology, *Federal Information Technology Security Assessment Framework*, prepared for the Federal CIO Council by the NIST Computer Security Division Systems and Network Security Group, Nov. 28, 2000.

[27] *Office of Management and Budget, FY 2001 Report to Congress on Federal Government Information Security Reform*. February 2002.

President's Management Council and the Critical Infrastructure Protection Board to promote sustained attention to security as part of its work on the President's Management Agenda and the integration of security into the Scorecard. OMB also reported that it included security instructions in budget passback guidance and sent security letters to each agency highlighting the lack of senior management attention and describing specific actions OMB is taking to assist the agency. According to OMB officials, although the President's Critical Infrastructure Protection Board was recently dissolved, OMB continues to coordinate security issues with the President's Homeland Security Council and the Department of Homeland Security. These officials also said that they are continuing to work with the agencies and that security is an integral part of assessing agencies' performance for the E-Government component of the Scorecard.

2. *Inadequate accountability for job and program performance related to IT security*—OMB reported that it was working with the agencies and other entities to develop workable measures of job and program performance to hold federal employees accountable for their security responsibilities. As discussed previously, OMB instructions to federal agencies for fiscal year 2002 GISRA reporting included high-level management performance measures. Related to this initiative, in October 2002, NIST also issued an initial public draft of a security metrics guide for IT systems to provide guidance on how an organization, through the use of metrics, can determine the adequacy of in-place security controls, policies, and procedures. The draft also explains the metric development and implementation process and how it can also be used to adequately justify security control investments.[28]

3. *Limited security training for general users, IT professionals, and security professionals*—OMB reported that along with federal agencies, it was working through the Critical Infrastructure Protection Board's education committee and the CIO Council's Workforce Committee to address this issue. OMB also reported that work was under way to identify and disseminate security training best practices through NIST's Federal Agency Security Practices Web site and that one of the administration's electronic government initiatives is to establish and deliver electronic-training on a number of mandatory topics, including security, for use by all federal agencies, along with state and local governments. As an example of progress on this initiative, OMB officials pointed to an online training initiative, www.golearn.gov. Launched in July 2002 by the Office of Personnel Management (OPM), this site offers training in an online environment, including IT security courses, such as security awareness, fundamentals of Internet security, and managing network security. Other activities for this area include NIST's July 2002 issuance of draft guidance

[28] *National Institute of Standards and Technology,* Security Metrics Guide for Information Technology Systems, *NIST Draft Special Publication 800-55 (October 2002).*

on designing, developing, implementing, and maintaining an awareness and training program within an agency's IT security program.[29]

4. *Inadequate integration of security into the capital planning and investment control process*—OMB reported that it was integrating security into the capital planning and investment control process to ensure that adequate security is incorporated directly into and funded over the life cycle of all systems and programs before funding is approved. Specifically, OMB established criteria that agencies must report security costs for each major and significant IT investment, document in their business cases that adequate security controls have been incorporated into the life cycle planning and funding of each IT investment, and tie their corrective action plans for a system directly to the business case for that IT investment. Another criterion was that agency security reports and corrective action plans were presumed to reflect the agency's security priorities and, thus, would be a central tool for OMB in prioritizing funding for systems. OMB officials confirmed that these activities were continuing and included providing additional guidance in OMB Circular A-11 on identifying security costs. In addition, they said that draft NIST guidelines for federal IT systems would help to ensure that agencies consider security throughout the system life cycle.[30] Under OMB policy, responsible federal officials are required to make a security determination (called accreditation) to authorize placing IT systems into operation. In order for these officials to make sound, risk-based decisions, a security evaluation (known as certification) of the IT system is needed. The NIST guidelines are to establish a standard process, general tasks and specific subtasks to certify and accredit systems and provide a new approach that uses the standardized process to verify the correctness and effectiveness of security controls employed in a system. The guidelines will also employ the use of standardized, minimum security controls and standardized verification techniques and procedures that NIST indicates will be provided in future guidance.

5. *Poor security for contractor-provided services*—OMB reported last year that under the guidance of the OMB-led security committee established by Executive Order 13231 (since eliminated), an issue group would develop recommendations to include addressing how security is handled in contracts. OMB also reported that it would work with the CIO Council and the Procurement Executives Council to establish a training program that ensures appropriate contractor training in security. OMB officials stated that these activities are continuing and the issue group had made recommendations to the Federal Acquisition Regulation Council. In addition,

[29] *National Institute of Standards and Technology*, Building an Information Technology Security Awareness and Training Program, *NIST Draft Special Publication 800-50 (July 19, 2002)*.

[30] *National Institute of Standards and Technology*, Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems, *NIST Draft Special Publication 800-37 (October 28, 2002)*.

in October 2002, NIST issued a draft guide on security considerations in federal IT procurements, which includes specifications, clauses, and tasks for areas such as IT security training and awareness, personnel security, physical security, and security features in systems.[31]

6. *Limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections*—OMB reported that the Federal Computer Incident Response Center (FedCIRC) reports to it on a quarterly basis on the federal government's status on IT security incidents. OMB also reported that under OMB and Critical Infrastructure Protection Board guidance, GSA was exploring methods to disseminate patches to all agencies more effectively. OMB officials pointed to the Patch Authentication and Dissemination Capability Program, which FedCIRC introduced in January 2003 as a free service to federal civilian agencies.[32] According to FedCIRC, this service provides a trusted source of validated patches and notifications on new threats and vulnerabilities that have potential to disrupt federal government mission critical systems and networks. It is a Web-enabled service that obtains patches from vendors, validates that the patch only does what it states that it was created to correct, and provides agencies notifications based on established profiles. We also noted that in August 2002, NIST published procedures for handling security patches that provided principles and methodologies for establishing an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches.[33]

In addition to activities identified for these specific weaknesses, in last year's report, OMB reported that it would direct all large agencies to undertake a Project Matrix review to more clearly identify and prioritize the security needs for government assets. Project Matrix is a methodology developed by the Critical Infrastructure Assurance Office (CIAO) (recently transferred to the Department of Homeland Security) that identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector.[34] OMB

[31]National Institute of Standards and Technology, *Security Considerations in Federal Information Technology Procurements: A Guide for Procurement Initiators, Contracting Officers, and IT Security Officials*, NIST Draft Special Publication 800-4A (Oct. 9, 2002).

[32]FedCIRC, formerly within the General Services Administration and now part of the Department of Homeland Security, was established to provide a central focal point for incident reporting, handling, prevention and recognition for the federal government. Its purpose is to ensure that the government has critical services available in order to withstand or quickly recover from attacks against its information resources.

[33]*National Institute of Standards and Technology*, Procedures for Handling Security Patches — Recommendations of the National Institute of Standards and Technology, *NIST Special Publication 800-40 (August 2002).*

[34]*The Project Matrix methodology defines "critical" as the responsibilities, assets, nodes, and networks that, if incapacitated or destroyed, would jeopardize the nation's survival; have a serious, deleterious effect on the nation at large; adversely affect large portions of the American populace; and require near-term, if not immediate, remediation (currently defined as within 72 hours). It defines "assets" as*

reported that once reviews have been completed at each large agency, it would identify cross-government activities and lines of business for Project Matrix reviews so that it will have identified both vertically and horizontally the critical operations and assets of the federal government's critical enterprise architecture and their relationship beyond government.

As of July 2002, a CIAO official reported that of 31 agencies targeted for Project Matrix reviews, 18 had begun their reviews; and of those, 5 had completed the first step of the methodology to identify their critical assets, 2 found no candidate assets to undergo a process to identify critical assets, 5 had begun the second step to identify other federal government assets, systems, and networks upon which their critical assets depend to operate, and none had begun the third step to identify all associated dependencies on private-sector owned and operated critical infrastructures.[35] According to a CIAO official in December 2003, the office's goal was to complete Project Matrix reviews for 24 of the 31 identified agencies by the end of fiscal year 2004 and for the remaining 7 in fiscal year 2005. However, this official also said that at the request of the Office of Homeland Security, CIAO was revising and streamlining its Project Matrix methodology to be less labor intensive for the agencies and reduce the time needed to identify critical assets. In our recent discussions with OMB officials, they said they were requiring Project Matrix reviews for 24 large departments and agencies and that as part of their GISRA reporting, agencies were required to report on the status of their efforts to identify critical assets and their dependencies. However, they acknowledged that OMB did not establish any deadlines for the completion of Project Matrix reviews. In our February 2003 report, we also reported that neither the administration nor the agencies we reviewed had milestones for the completion of Project Matrix analyses and recommended that agencies coordinate with CIAO to set these milestones.

Finally, in February 2002, OMB reported that a number of efforts were under way to address security weaknesses in industry software development, and that chief among them were national policy-level activities of the Critical Infrastructure Protection Board (since eliminated). At the technical product-level, OMB reported that the National Information Assurance Partnership, operated jointly by NIST and the National Security Agency, was certifying private-sector laboratories to which product vendors may submit their software for analysis and certification, but that this certification process was a lengthy one and often cannot accommodate the "time-to-market" imperative that the technology industry faces. According to recent discussions with OMB

tangible equipment, applications, and facilities that are owned, operated, or relied upon by the agency, such as information technology systems or networks, buildings, vehicles (aircraft, ships, or land), satellites, or even a team of people.

[35] *U.S. General Accounting Office,* Critical infrastructure Protection: Challenges for Selected Agencies and Industry Sectors, *GAO-03-233 (Washington, D.C.: Feb. 28, 2003).*

officials, the National Information Assurance Partnership efforts are still under way.

Agency GISRA Reporting Shows Progress, but Highlights Continued Weaknesses

Fiscal year 2002 GISRA reporting by CIOs and independent evaluations by IGs for the 24 agencies provided an improved baseline for measuring improvements in federal information security not only because of performance measures that OMB now requires, but also because of agencies' increased review coverage and use of consistent methodologies. For example, 16 agencies reported that they had reviewed the security of 60 percent or more of their systems and programs for their fiscal year 2002 GISRA reporting, with 10 of these reporting that they reviewed from 90 to 100 percent. Further, 13 agencies reported that coverage of agency systems and programs increased for fiscal year 2002 compared to fiscal year 2001. However, with 8 agencies reporting that they reviewed less than half of their systems, improvements are still needed.* Regarding their methodologies, 21 agencies reported that, as required by OMB, they used NIST's *Security Self-Assessment Guide for Information Technology Systems* or developed their own methodology that addressed all elements of the guide, and only 3 agencies reported that they did not. By not following the NIST guide, agencies may not identify all weaknesses. For example, one agency reported that the methodology it used incorporated many of the elements of NIST's self-assessment guide, but the IG reported that the methodology did not call for the detailed level of system reviews required by the NIST guide nor did it include the requirement to test and evaluate security controls.

In performing our analyses, we summarized and categorized the reported information including data provided for the OMB-prescribed performance measures. There were several instances where agency reports either did not address or provide sufficient data for a question or measure. In addition, IGs' independent evaluations sometimes showed different results than CIO reporting or identified data inaccuracies. Further, IG reporting also did not always include comparable data, particularly for the performance measures. In part, this was because although OMB instructions said that the IGs should use the performance measures to assist in evaluating agency officials' performance, the IG was not required to review the agency's reported measures. Summaries of our analyses for key requirements follow below.

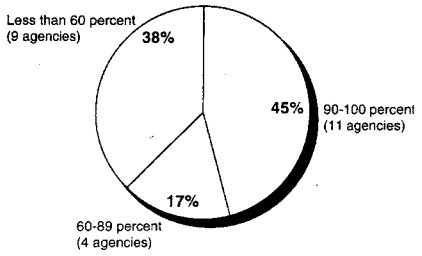
*One agency did not specifically report this information, but its IG reported that the agency reviewed less than half of its systems.

Many Systems Still Do Not Have Risk Assessments or Up-to-Date Security Plans

GISRA required agencies to perform periodic threat-based risk assessments for systems and data. Risk assessments are an essential element of risk management and overall security program management and, as our best practice work has shown, are an integral part of the management processes of leading organizations.[37] Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls. Our reviews of federal agencies, however, frequently show deficiencies related to assessing risk, such as security plans for major systems that are not developed on the basis of risks. As a result, the agencies had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable.

As one of its performance measures for this requirement, OMB required agencies to report the number and percentage of their systems that have been assessed for risk during fiscal year 2001 and fiscal year 2002. Our analyses of reporting for this measure showed some overall progress. For example, of the 24 agencies we reviewed, 13 reported an increase in the percentage of systems assessed for fiscal year 2002 compared to fiscal year 2001. In addition, as illustrated in figure 3 below, for fiscal year 2002, 11 agencies reported that they had assessed risk for 90 to 100 percent of their systems. However, it also shows that further efforts are needed by other agencies, including the 9 that reported less than 60 percent of their systems had been assessed for risk.

Figure 3: Percentage of systems with risk assessments during fiscal year 2002



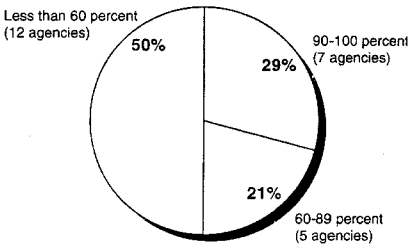
Source: Agency-reported data.

Note: Rounding used to total 100 percent.

[37]GAO/AIMD-98-68.

GISRA also required the agency head to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. In its reporting instructions, OMB required agencies to report whether the agency head had taken specific and direct actions to oversee that program officials and the CIO are ensuring that security plans are up to date and practiced throughout the life cycle. They also had to report the number and percentage of systems that have an up-to-date security plan. Our analyses showed that although most agencies reported that they had taken such actions, IG reports disagreed for a number of agencies, and many systems do not have up-to-date security plans. Specifically, 21 agencies reported that the agency head had taken actions to oversee that security plans are up to date and practiced throughout the life cycle compared to the IGs reporting that only 9 agencies had taken such actions. One IG reported that the agency's security plan guidance predates revisions to NIST and OMB guidance and, as a result, does not contain key elements, such as the risk assessment methodology used to identify threats and vulnerabilities. In addition, another IG reported that although progress had been made, security plans had not been completed for 62 percent of the agency's systems. Regarding the status of agencies' security plans, as shown in figure 4, half of the 24 agencies reported that they had up-to-date security plans for 60 percent or more of their systems for fiscal year 2002, including 7 that reported these plans for 90 percent or more.

Figure 4: Percentage of systems with up-to-date security plans during fiscal year 2002



Source: Agency-reported data

Security Training Efforts Show Mixed Progress

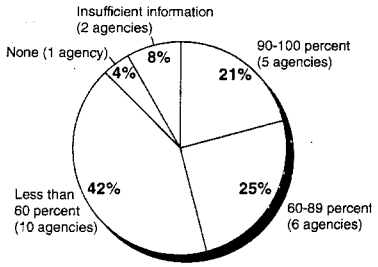
GISRA required agencies to provide training on security awareness for agency personnel and on security responsibilities for information security personnel. Our studies of best practices at leading organizations have shown that they took steps to ensure that personnel involved in various aspects of their information security programs had the skills and

knowledge they needed. They also recognized that staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. However, our past information security reviews at individual agencies have shown that they have not provided adequate computer security training to their employees, including contractor staff.

Among the performance measures for these requirements, OMB required agencies to report the number and percentage of employees including contractors that received security training during fiscal years 2001 and 2002 and the number of employees with significant security responsibilities that received specialized training. For agency employee/contractor security training, our analyses showed 16 agencies reported that they provided security training to 60 percent or more of their employees and contractors for fiscal year 2002, with 9 reporting 90 percent or more. Of the remaining 8 agencies, 4 reported that such training was provided for less than half of their employees/contractors, 1 reported that none were provided this training, and 3 provided insufficient data for this measure.

For specialized training for employees with significant security responsibilities, some progress was indicated, but additional training is needed. As indicated in figure 5, our analyses showed 11 agencies reported that 60 percent or more of their employees with significant security responsibilities had received specialized training for fiscal year 2002, with 5 reporting 90 percent or more. Of the remaining 13 agencies, 4 reported less than 30 percent and one reported that none had received such training.

Figure 5: Percentage of employees with significant security responsibilities receiving specialized security training during fiscal year 2002

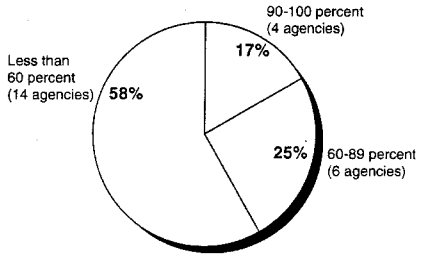


Source: Agency-reported data.

Under GISRA, the agency head was responsible for ensuring that the appropriate agency officials, evaluated the effectiveness of the information security program, including testing controls. The act also required that the agencywide information security program include periodic management testing and evaluation of the effectiveness of information security policies and procedures. Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an organization to manage its information security risks cost effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Further, management control testing and evaluation as part of the program reviews can supplement control testing and evaluation in IG and GAO audits to help provide a more complete picture of the agencies' security postures.

As a performance measure for this requirement, OMB required the agencies to report the number and percentage of systems for which security controls have been tested and evaluated during fiscal years 2001 and 2002. Our analyses of the data agencies reported for this measure showed that although 15 agencies reported an increase in the overall percentage of systems being tested and evaluated for fiscal year 2002, most agencies are not testing essentially all of their systems. As shown in figure 6, our analyses showed that 14 agencies reported that they had tested the controls of less than 60 percent of their systems for fiscal year 2002. Of the remaining 10 agencies, 4 reported that they had tested and evaluated controls for 90 percent or more of their systems.

Figure 6: Percentage of systems with security controls tested during fiscal year 2002

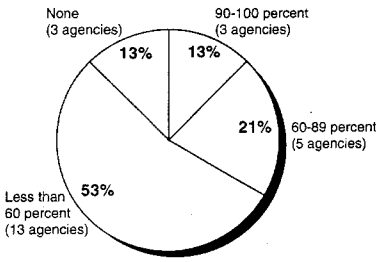


Source: Agency-reported data.

As another measure, OMB also required agencies to report the number and percentage of systems that have been authorized for processing following certification and accreditation. According to NIST's draft *Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems* (Special Publication 800-37), *accreditation* is the authorization of an IT system to process, store, or transmit information, granted by a management official that provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. *Certification* is the comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. Certification provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. The accreditation decision is based on the implementation of an agreed upon set of management, operational, and technical controls, and by accrediting the system, the management office accepts the risk associated with it.

Our analysis of agencies' reports showed mixed progress for this measure. For example, 10 agencies reported increases in the percentage of systems authorized for processing following certification and accreditation compared to fiscal year 2001, but 8 reported decreases and 3 did not change (3 others did not provide sufficient data). In addition, as shown in figure 7, 8 agencies reported that for fiscal year 2002, 60 percent or more of their systems had been authorized for processing following certification and accreditation with only 3 of these reporting from 90 to 100 percent. And of the remaining 16 agencies reporting less than 60 percent, 3 reported that none of their systems had been authorized.

Figure 7: Percentage of systems during fiscal year 2002 that are authorized for processing by management after certification and accreditation



Source: Agency-reported data

In addition to this mixed progress, IG reports identified instances where agencies' certification and accreditation efforts were inadequate. For example, one agency reported that 43 percent of its systems were authorized for processing following certification and accreditation. IG reporting agreed, but also noted that over a fourth of the systems identified as authorized had been operating with an interim authorization and did not meet all of the security requirements to be granted accreditation. The IG also stated that, due to the risk posed by systems operating without certification and full accreditation, the department should consider identifying this deficiency as a material weakness.

Incident-Handling Capabilities Established, but Implementation Incomplete

GISRA required agencies to implement procedures for detecting, reporting, and responding to security incidents. Although even strong controls may not block all intrusions and misuse, organizations can reduce the risks associated with such events if they promptly take steps to detect intrusions and misuse before significant damage can be done. In addition, accounting for and analyzing security problems and incidents are effective ways for an organization to gain a better understanding of threats to its information and of the cost of its security-related problems. Such analyses can also pinpoint vulnerabilities that need to be addressed to help ensure that they will not be exploited again. In this regard, problem and incident reports can provide valuable input for risk assessments, help in prioritizing security improvement efforts, and be used to illustrate risks and related trends in reports to senior management. Our information security reviews also confirm that federal agencies have not adequately (1) prevented intrusions before they occur, (2) detected intrusions as they occur, (3) responded to successful intrusions, or (4) reported intrusions to staff and management. Such weaknesses provide little assurance that unauthorized attempts to access sensitive information will be identified and appropriate actions taken in time to prevent or minimize damage.

OMB included a number of performance measures in agency reporting instructions that were related to detecting, reporting, and responding to security incidents. These included the number of agency components with an incident-handling and response capability, whether the agency and its major components share incident information with FedCIRC in a timely manner, and the numbers of incidents reported. OMB also required that agencies report on how they confirmed that patches have been tested and installed in a timely manner. Our analyses of agencies' reports showed that although most agencies reported that they have established incident response capabilities, implementation of these capabilities is still not complete. For example, 12 agencies reported that for fiscal year 2002, 90 percent or more of their components had incident handling and response capabilities and 8 others reported that they provided these capabilities to components through a central point within the agency. However, although most agencies report having these capabilities for most components, in at

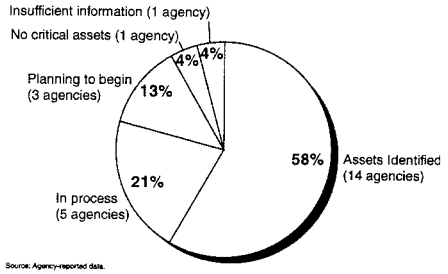
least two instances, the IGs' evaluations identified instances where incident response capabilities were not always implemented. For example, one IG reported that the department established and implemented its computer security incident-response capability on August 1, 2002, but had not enforced procedures to ensure that components comply with a consistent methodology to identify, document, and report computer security incidents. Another IG reported that the agency had released incident-handling procedures and established a computer incident response team, but had not formally assigned members to the team or effectively communicated procedures to employees.

Our analyses also showed that for fiscal year 2002, 13 agencies reported they had oversight procedures to verify that patches have been tested and installed in a timely manner and 10 reported they did not. Of those that did not have procedures, several specifically mentioned that they planned to participate in FedCIRC's patch management process.

Agencies Show Progress in Identifying Critical Assets, but Most Have Not Identified Interdependencies

GISRA required that each agencywide information security program ensure the integrity, confidentiality, and availability of systems and data supporting the agency's critical operations and assets. In addition, as mentioned previously, OMB directed 24 of the largest agencies to undergo a Project Matrix review to identify and characterize the operations and assets and these assets' associated infrastructure dependencies and interdependencies that are most critical to the nation. For example, as part of its GISRA reporting, OMB required the agencies to report whether they had undergone a Project Matrix review or used another methodology to identify their critical assets and their interdependencies and interrelationships. Our analyses of agencies' reports showed some overall process in identifying critical assets, but limited progress in identifying interdependencies. As shown in figure 8, a total of 14 agencies reported they had identified their critical assets and operations—10 using Project Matrix and 4 using other methodologies. In addition, five more agencies reported that they were in some stage of identifying their critical assets and operations, and three more planned to do so in fiscal year 2003.

Figure 8: Percentage of agencies that had identified their critical assets and operations—fiscal year 2002



Source: Agency-reported data.

Our analyses also showed that three agencies reported they had identified the interdependencies for their critical assets, and four others reported that they were in some stage of undertaking this process.

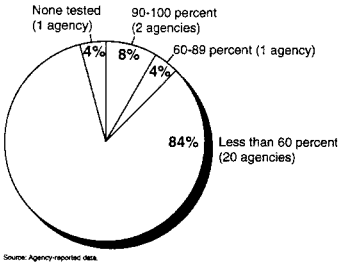
Lack of Contingency Plan Testing Is a Major Weakness

Contingency plans provide specific instructions for restoring critical systems, including such things as arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. At many of the agencies we have reviewed, we found incomplete plans and procedures to ensure that critical operations can continue when unexpected events occur, such as a temporary power failure, accidental loss of files, or a major disaster. These plans and procedures were incomplete because operations and supporting resources had not been fully analyzed to determine which were most critical and would need to be restored first. Further, existing plans were not fully tested to identify their weaknesses. As a result, many agencies have inadequate assurance that they can recover operational capability in a timely, orderly manner after a disruptive attack.

As another of its performance measures, OMB required agencies to report the number and percentage of systems for which contingency plans have been tested in the past year. As shown in figure 9, our analyses showed that for fiscal year 2002, only 2 agencies reported they had tested contingency plans for 90 percent or more of their systems, while 20 had

tested contingency plans for less than 60 percent of their systems. One reported that none had been tested.

Figure 9: Percentage of systems with recently tested contingency plans for fiscal year 2002



Note: Rounding used to total 100 percent.

Some Reported Improvement in Efforts to Ensure Security of Contractor-Provided Services

GISRA requires agencies to develop and implement risk-based, cost-effective policies and procedures to provide security protection for information collected or maintained either by the agency or for it by another agency or contractor. In its fiscal year 2001 GISRA report to the Congress, OMB identified poor security for contractor-provided services as a common weakness and for fiscal year 2002 reporting, included performance measures to help indicate whether the agency program officials and CIO used appropriate methods, such as audits and inspections, to ensure that service provided by a contractor are adequately secure and meet security requirements. Our analyses showed that a number of agencies reported that they have reviewed a large percentage of services provided by a contractor, but others have reviewed only a small number.

For operations and assets under the control of agency program officials, 16 agencies reported that for fiscal year 2002 they reviewed 60 percent or more of contractor operations or facilities, with 7 of these reporting that they reviewed 90 percent or more; and 4 reported that they reviewed less than 30 percent.

For operations and assets under the control of the CIO, 11 agencies reported that for fiscal year 2002 they reviewed 60 percent or more of contractor operations or facilities, with 7 of these reporting they reviewed 90 percent or more; 3 reported that they reviewed less than 30 percent;

and 5 agencies reported that they had no services provided by a contractor or another agency.

Reporting of Security Costs Shows Improvement

GISRA requires that each agency examine the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports related to annual agency budgets and other statutory performance reporting requirements. The act also requires each agency to describe the resources, including budget, staffing, and training, that are necessary to implement its agencywide information security program. For GISRA reporting, OMB required agencies to report information on total security funding included in their fiscal year 2002 budget request, fiscal year 2002 budget enacted, and the President's fiscal year 2003 budget and to include (1) a breakdown of security costs by each major operating division or bureau and (2) CIP costs that apply to the protection of government operations and assets.

Most agencies (21) reported total security funding for these budgets, although 13 did not show costs by major operating division or bureau and/or for CIP. Further, most agencies reported including security costs in their budget requests and justifications. For example:

- For the fiscal year 2003 budget, 16 agencies reported that they had submitted capital asset plans and justifications to OMB with all requisite security information, and of the remaining 8 agencies, 5 reported that less than 30 percent of their capital asset plans and justifications did not include this information. Last year, 19 agencies reported that they had not included security requirements and costs on every fiscal year 2002 capital asset plan submitted to OMB.
- For fiscal year 2003, 18 agencies reported that security costs were reported on the Exhibit 53[38] for all agency systems, with 5 reporting that these costs were not reported for all agency systems.

Corrective Action Plans Provide Potential Tool for Monitoring Agency Progress

GISRA required that agencies develop a process for ensuring that remedial action is taken to address significant deficiencies. As a result, OMB required the agency head to work with the CIO and program officials to provide a strategy to correct security weaknesses identified through annual GISRA program reviews and independent evaluations, as well as other reviews or audits performed throughout the reporting period by the IG or GAO. Agencies were required to submit a corrective action plan for all programs and systems where a security weakness had been identified

[38]The Agency IT Investments Portfolios as required by OMB Circular A-11.

plus quarterly updates on the plan's implementation. OMB guidance required that these plans list the identified weaknesses and for each identify a point of contact, the resources required to resolve the weakness, the scheduled completion date, key milestones with completion dates for the milestones, milestone changes, the source of the weakness (such as a program review, IG audit, or GAO audit), and the status (ongoing or completed). Agencies were also required to submit quarterly updates of these plans that list the total number of weaknesses identified at the program and system level, as well as the numbers of weaknesses for which corrective actions were completed on time, ongoing and on schedule, or delayed. Updates were also to include the number of new weaknesses discovered subsequent to the last corrective action plan or quarterly update.

Our analyses of agencies' fiscal year 2002 corrective action plans and IGs' evaluations of these plans showed that most agencies followed the OMB-prescribed format, but also that several used an existing tracking system to meet this requirement. In theory, these plans could prove to be a useful tool for the agencies in correcting their information security weaknesses. However, their usefulness could be impaired to the extent that they do not identify all weaknesses or provide realistic completion estimates. For example, for the 24 agencies, only 5 IGs reported that their agency's corrective action plan addressed all identified significant weaknesses and 9 specifically reported that their agency's plan did not. Our analyses also showed that in several instances, corrective action plans did not indicate the current status of a weaknesses identified or include information regarding whether actions were on track as originally scheduled.

Plan progress must be appropriately monitored and the actual correction of weaknesses may require independent validation. Our analyses showed that three IGs reported that their agencies did not have a centralized tracking system to monitor the status of corrective actions. Also, one IG specifically questioned the accuracy of unverified, self-reported corrective actions reported in the agency's plan.

Further Action Needed to Improve Federal Information Security

Recent audits and reviews, including annual GISRA program reviews and independent evaluations, show that although agencies have made progress in addressing GAO and IG recommendations to improve the effectiveness of their information security, further action is needed. In particular, overall security program management continues to be an area marked by widespread and fundamental problems. Many agencies have not developed security plans for major systems based on risk, have not documented security policies, and have not implemented a program for testing and evaluating the effectiveness of the controls they rely on. As a result, they could not ensure that the controls they had implemented were operating

as intended and they could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Further information security improvement efforts are also needed at the governmentwide level, and it is important that these efforts are guided by a comprehensive strategy and, as development of this strategy continues, that certain key issues be addressed. These issues and actions currently under way are as follows.

First, the federal strategy should delineate the roles and responsibilities of the numerous entities involved in federal information security and describe how the activities of these organizations interrelate, who should be held accountable for their success or failure, and whether these activities will effectively and efficiently support national goals.

Second, more specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently, agencies have wide discretion in deciding which computer security controls to implement and the level of rigor with which to enforce these controls. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.[39] In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. FISMA requires NIST to develop standards that provide mandatory minimum information security requirements.

Third, ensuring effective implementation of agency information security and CIP plans will require active monitoring by the agencies to determine whether milestones are being met and testing is being performed to determine whether policies and controls are operating as intended. With routine periodic evaluations, such as those required by GISRA and now FISMA, performance measurements can be more meaningful. In addition, the annual evaluation, reporting, and monitoring process established through these provisions is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective.

Fourth, the Congress and the executive branch can use audit results, including the results of GISRA and FISMA reporting, to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies

[39]GAO/AIMD-98-68.

accountable for their performance, as was demonstrated by OMB and congressional efforts to oversee the Year 2000 computer challenge.

Fifth, agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. As highlighted during the Year 2000 challenge, the availability of adequate technical and audit expertise is a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their information security and infrastructure protection activities. In our review of first-year GISRA implementation, we reported that many agencies emphasized the need for adequate funding to implement security requirements, and that security funding varied widely across the agencies. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, additional amounts are likely to be needed to address specific weaknesses and new tasks. At the same time, OMB and congressional oversight of future spending on information security will be important for ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk-management process. Further, we agree with OMB that much can be done to cost-effectively address common weaknesses, such as limited security training, across government rather than individually by agency.

Seventh, expanded research is needed in the area of information systems protection. Although a number of research efforts are under way, experts have noted that more is needed to achieve significant advances. In this regard, the Congress recently passed and the President signed into law the Cyber Security Research and Development Act to provide $903 million over 5 years for cybersecurity research and education programs.[40] This law directs the National Science Foundation to create new cybersecurity research centers, program grants, and fellowships. It also directs NIST to create new program grants for partnerships between academia and industry.

[40] P.L. 107-305, November 27, 2002.

CIP Policy Has Continued to Evolve Since the Mid-1990s

CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are critical to national security, national economic security, and/or national public health and safety. Federal awareness of the importance of securing our nation's critical infrastructures has continued to evolve since the mid-1990s. Over the years, a variety of working groups has been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. The following sections summarize key developments in federal CIP policy to provide historical perspective.

President's Commission Studied Critical Infrastructure Protection

In October 1997, the President's Commission on Critical Infrastructure Protection issued a report[41] describing the potentially devastating implications of poor information security for the nation. The report recommended measures to achieve a higher level of CIP that included industry cooperation and information sharing, a national organization structure, a revised program of research and development, a broad program of awareness and education, and a reconsideration of related laws. It further stated that a comprehensive effort would need to "include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyberthreats." The report also urged the FBI to continue its efforts to develop warning and threat analysis capabilities, which would enable it to serve as the preliminary national warning center for infrastructure attacks and to provide law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

Presidential Decision Directive 63 Established Initial CIP National Strategy

In 1998, the President issued Presidential Decision Directive 63 (PDD 63), which described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. PDD 63 called for a range of actions intended to improve federal agency security programs, improve the nation's ability to detect and respond to serious computer-based and physical attacks, and establish a partnership between the government and the private sector. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved and designated lead agencies to work with private-sector and government organizations. Further, it established CIP as a national goal

[41]President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures (October 1997).*

and stated that, by the close of 2000, the United States was to have achieved an initial operating capability to protect the nation's critical infrastructures from intentional destructive acts and, by 2003, have developed the ability to protect the nation's critical infrastructures from intentional destructive attacks.

To accomplish its goals, PDD 63 established and designated organizations to provide central coordination and support, including

- the Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies;
- the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation/response; and
- the National Infrastructure Assurance Council (NIAC), which was established to enhance the partnership of the public and private sectors in protecting our critical infrastructures.

To ensure coverage of critical sectors, PDD 63 also identified eight private-sector infrastructures and five special functions. For each of the infrastuctures and functions, the directive designated lead federal agencies, referred to as sector liaisons, to work with their counterparts in the private sector, referred to as sector coordinators. To facilitate private-sector participation, PDD 63 also encouraged the voluntary creation of information sharing and analysis centers (ISACs) to serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. Figure 3 displays a high-level overview of the organizations with CIP responsibilities, as outlined by PDD 63.

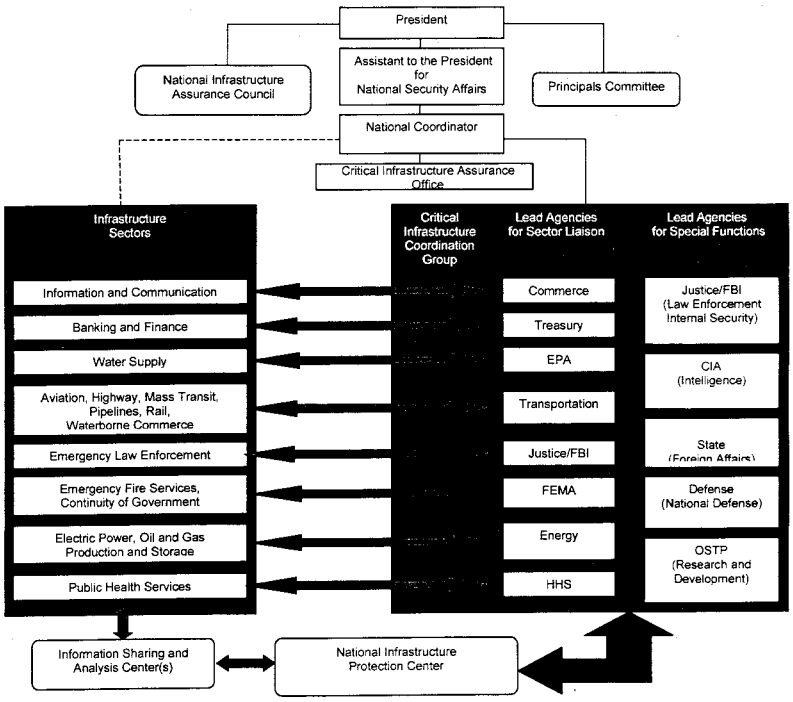


Figure 10: Organizations with CIP Responsibilities, as Outlined by PDD 63

Source: CIAO.

Note: In February 2001, the Critical Infrastructure Coordination Group was replaced by the Information Infrastructure Protection and Assurance Group under the Policy Coordinating Committee on Counter-terrorism and National Preparedness. In October 2001, Executive Order 13231 replaced the National Infrastructure Assurance Council with the National Infrastructure Advisory Council, and cyber CIP functions performed by the national coordinator were assigned to the chair of the President's Critical Infrastructure Protection Board. In February 2003, Executive Order 13231 was amended in its entirely by

Executive Order 13286, dissolving the President's Critical Infrastructure Board and stating that the National Infrastructure Advisory Council chairpersons are to be selected from among its members.

PDD 63 called for a range of activities intended to establish a partnership between the public and private sectors to ensure the security of our nation's critical infrastructures. The sector liaison and the sector coordinator were to work with each other to address problems related to CIP for their sector. In particular, PDD 63 stated that they were to (1) develop and implement vulnerability awareness and education programs and (2) contribute to a sectoral National Infrastructure Assurance Plan by

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing major attacks; and
- developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

PDD 63 also required every federal department and agency to be responsible for protecting its own critical infrastructures, including both cyber-based and physical assets. To fulfill this responsibility, PDD 63 called for agencies' CIOs to be responsible for information assurance, and it required every agency to appoint a chief infrastructure assurance officer to be responsible for the protection of all other aspects of an agency's critical infrastructure. Further, it required federal agencies to:

- develop, implement, and periodically update a plan for protecting its critical infrastructure;
- determine its minimum essential infrastructure that might be a target of attack;
- conduct and periodically update vulnerability assessments of its minimum essential infrastructure;
- develop a recommended remedial plan based on vulnerability assessments that identifies time lines for implementation, responsibilities, and funding; and
- analyze intergovernmental dependencies, and mitigate those dependencies.

Other PDD 63 requirements for federal agencies are that they provide vulnerability awareness and education to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cybersystems; that they establish a system for responding to a

significant infrastructure attack while it is under way, to help isolate and minimize damage; and that they establish a system for rapidly reconstituting minimum required capabilities for varying levels of successful infrastructure attacks.

National Plan for Information Systems Protection Provided Plan for Federal Government

In January 2000, the White House issued its *National Plan for Information Systems Protection.*[42] The national plan provided a vision and framework for the federal government to prevent, detect, respond to, and protect the nation's critical cyber-based infrastructure from attack and reduce existing vulnerabilities by complementing and focusing existing federal computer security and information technology requirements. Subsequent versions of the plan were expected to (1) define the roles of industry and of state and local governments working in partnership with the federal government to protect physical and cyber-based infrastructures from deliberate attack and (2) examine the international aspects of CIP.

Executive Order 13228 Established the Office of Homeland Security

In October 2001, the President issued Executive Order (EO) 13228,[43] establishing the Office of Homeland Security within the Executive Office of the President and the Homeland Security Council. It stated that the Office of Homeland Security was "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks." In addition, EO 13228 stated that, among other things, the Office of Homeland Security was to coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attacks. Further, it established the Homeland Security Council to advise and assist the President with respect to all aspects of homeland security, to serve as the mechanism for ensuring coordination of homeland security-related activities of executive departments and agencies, and to develop and implement homeland security policies.

Executive Order 13231 Established the CIP Board

In October 2001, President Bush signed EO13231, establishing the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our

[42] *The White House*, Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue *(Washington, D.C.: January 2000).*

[43] *"Establishing the Office of Homeland Security and the Homeland Security Council," Executive Order 13228, October 8, 2001.*

nation's critical infrastructures. Executive Order 13231 tasked the board with recommending policies and coordinating programs for protecting CIP-related information systems. The Special Advisor to the President for Cyberspace Security chaired the board. The executive order also established 10 standing committees to support the board's work on a wide range of critical information. According to EO 13231, the board's responsibilities were to recommend policies and coordinate programs for protecting information systems for critical infrastructures, including emergency preparedness communications and the physical assets that support such systems. The Special Advisor reported to the Assistant to the President for National Security Affairs and to the Assistant to the President for Homeland Security and coordinated with the Assistant to the President for Economic Policy on issues relating to private-sector systems and economic effects and with the Director of OMB on issues relating to budgets and the security of federal computer systems. Executive Order 13231 emphasized the importance of CIP and the ISACs, but neither order identified additional requirements for agencies to protect their critical infrastructures or suggested additional activities for the ISACs.

National Strategy for Homeland Security Included CIP Components

In July 2002, the President issued the *National Strategy for Homeland Security,* with strategic objectives to (1) prevent terrorist attacks within the United States, (2) reduce America's vulnerability to terrorism, and (3) minimize the damage and recovery from attacks that do occur. To ensure coverage of critical infrastructure sectors, this strategy identified 13 industry sectors, expanded from the 8 originally identified in PDD 63, as essential to our national security, national economic security, and/or national public health and safety. Lead federal agencies were identified and directed to work with their counterparts in the private sector to assess sector vulnerabilities and to develop plans to eliminate vulnerabilities. The sectors and their lead agencies are listed in table 2.

Table 2: Critical Infrastructure Lead Agencies and Sectors

Lead agency	Sectors
Homeland Security	▪ Information and telecommunications ▪ Transportation (aviation; rail; mass transit; waterborne commerce; pipelines; and highways, including trucking and intelligent transportation systems) ▪ Postal and shipping ▪ Emergency services ▪ Continuity of government
Treasury	▪ Banking and finance
Health and Human Services	▪ Public health (including prevention, surveillance, laboratory services, and personal health services) ▪ Food (all except for meat and poultry)
Energy	▪ Energy (electrical power, oil and gas production and storage)
Environmental Protection Agency	▪ Water ▪ Chemical industry and Hazardous materials
Agriculture	▪ Agriculture ▪ Food (meat and poultry)
Defense	▪ Defense industrial base

Source: *National Strategy for Homeland Security* and *National Strategy to Secure Cyberspace*

The Homeland Security Act Created the Department of Homeland Security

The Homeland Security Act of 2002 (signed by the President on November 25, 2002) established the Department of Homeland Security (DHS). Regarding CIP, the new department is responsible for, among other things, (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States; (2) recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities; and (3) disseminating, as appropriate, information analyzed by the department both within the department and to other federal agencies, state and local government agencies, and private-sector entities to assist in the deterrence, prevention, preemption of, or response to terrorist attacks. To help accomplish these functions, the act created the Information Analysis and Infrastructure Protection Directorate within the new department and transferred to it the functions, personnel, assets, and liabilities of several existing organizations with CIP responsibilities, including NIPC (other than the Computer Investigations and Operations Section) and the CIAO.

The *National Strategy for Homeland Security* called for the Office of Homeland Security and the President's Critical Infrastructure Protection Board to complete cyber and physical infrastructure protection plans, which would serve as the baseline for later developing the comprehensive national infrastructure protection plan. Such a plan was subsequently required by the Homeland Security Act of 2002. On February 14, 2003, the President released the *National Strategy to Secure Cyberspace* and the complementary *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*[44] These two strategies identify priorities, actions, and responsibilities for the federal government, including lead agencies and DHS, as well as for state and local governments and the private sector.

The National Strategy to Secure Cyberspace Provided Initial Framework for Cyber CIP

The *National Strategy to Secure Cyberspace* is intended to provide an initial framework for both organizing and prioritizing efforts to protect our nation's cyberspace. It is also to provide direction to federal departments and agencies that have roles in cyberspace security and to identify steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The strategy reiterates the critical infrastructure sectors and the related lead federal agencies as identified in *The National Strategy for Homeland Security.* In addition, the strategy identifies DHS as the central coordinator for cyberspace efforts. As such, DHS is responsible for coordinating and working with other federal entities involved in cybersecurity. This strategy is organized according to five national priorities, with major actions and initiatives identified for each:

1. **A National Cyberspace Security Response System**—Coordinated by DHS, this system is described as a public/private architecture for analyzing and warning, managing incidents of national significance, promoting continuity in government systems and private-sector infrastructures, and increasing information sharing across and between organizations to improve cyberspace security. The system is to include governmental entities and nongovernmental entities, such as private-sector ISACs. Major actions and initiatives identified for cyberspace security response include providing for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments; expanding the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security; coordinating processes for voluntary public/private participation in the development of national public/private continuity and contingency plans; exercising cybersecurity continuity

[44] *The White House,* The National Strategy to Secure Cyberspace *(Washington, D.C.: February 2003); and* The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets *(Washington, D.C.: February 2003).*

plans for federal systems; and improving and enhancing public/private information sharing involving cyber attacks, threats, and vulnerabilities.

2. **A National Cyberspace Security Threat and Vulnerability Reduction Program**—This priority focuses on reducing threats and deterring malicious actors through effective programs to identify and punish them; identifying and remediating those existing vulnerabilities that, if exploited, could create the most damage to critical systems; and developing new systems with less vulnerability and assessing emerging technologies for vulnerabilities. Other major actions and initiatives include creating a process for national vulnerability assessments to better understand the potential consequences of threats and vulnerabilities, securing the mechanisms of the Internet by improving protocols and routing, fostering the use of trusted digital control and supervisory control and data acquisition systems, understanding infrastructure interdependencies and improving the physical security of cybersystems and telecommunications, and prioritizing federal cybersecurity research and development agendas.

3. **A National Cyberspace Security Awareness and Training Program**—This priority emphasizes promoting a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own parts of cyberspace. Other major actions and initiatives include fostering adequate training and education programs to support the nation's cybersecurity needs; increasing the efficiency of existing federal cybersecurity training programs; and promoting private-sector support for well-coordinated, widely recognized professional cybersecurity certification.

4. **Securing Governments' Cyberspace**—To help protect, improve, and maintain governments' cybersecurity, major actions and initiatives for this priority include continuously assessing threats and vulnerabilities to federal cyber systems; authenticating and maintaining authorized users of federal cyber systems; securing federal wireless local area networks; improving security in government outsourcing and procurement; and encouraging state and local governments to consider establishing information technology security programs and participating in ISACs with similar governments.

5. **National Security and International Cyberspace Security Cooperation**—This priority identifies major actions and initiatives to strengthen U.S. national security and international cooperation. These include strengthening cyber-related counterintelligence efforts, improving capabilities for attack attribution and response, improving coordination for responding to cyber attacks within the U.S. national security community, working with industry and through international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures, and

fostering the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets Provided National Policy for Physical CIP

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* provides a statement of national policy to remain committed to protecting critical infrastructures and key assets from terrorist attacks. Although the strategy does not explicitly mention PDD 63, it builds on the directive with its sector-based approach that includes the 13 sectors defined in the *National Strategy for Homeland Security*, identifies federal departments and agencies as sector liaisons, and calls for expanding the capabilities of ISACs. The strategy is based on eight guiding principles, including establishing responsibility and accountability, encouraging and facilitating partnering among all levels of government and between government and industry, and encouraging market solutions wherever possible and government intervention when needed. The strategy also establishes three strategic objectives. The first is to identify and assure the protection of the most critical assets, systems, and functions, in terms of national-level public health and safety, governance, and economic and national security and public confidence. This would include establishing a uniform methodology for determining national-level criticality. The second strategic objective is to assure the protection of infrastructures and assets facing specific, imminent threats; and the third is to pursue collaborative measures and initiatives to assure the protection of other potential targets that may become attractive over time. Under this strategy, DHS will provide overall cross-sector coordination and serve as the primary liaison and facilitator for cooperation among federal agencies, state and local governments, and the private sector. The strategy states that the private sector generally remains the first line of defense for its own facilities and should reassess and adjust their planning, assurance, and investment programs to better accommodate the increased risk presented by deliberate acts of violence. In addition, the Office of Homeland Security will continue to act as the President's principal policy adviser staff and coordinating body for major interagency policy issues related to homeland security.

Executive Order 13286 Reflected Establishment of DHS

On February 28, 2003, Executive Order (EO) 13231 was amended in its entirety by Executive Order 13286.[46] Although EO 13286 maintained the same national policy statement regarding the protection against disruption of information systems for critical infrastructures, it dissolved the President's Critical Infrastructure Board that was to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures, and the board's chair— the Special Advisor to the President for Cyberspace Security—and related staff, along with the 10 standing committees established to support the board's work on a wide range of critical information infrastructure efforts. According to EO 13286, the NIAC is to continue to provide the President with advice on the security of information systems for critical infrastructures supporting other sectors of the economy. However, NIAC will provide its advice through the Secretary of Homeland Security. Regarding the functions of the standing committees, an OMB official stated that OMB will continue to oversee the federal information security committee functions. Further, recent media reports state that efforts are underway to ensure the transition of certain other functions to DHS.

Other Developments

On March 1, 2003, DHS assumed certain essential information and analysis and infrastructure protection functions and organizations, including NIPC (other than the Computer Investigation and Operations Section) and the CIAO. Currently, according a Department of Homeland Security official, the department is continuing to carry out the activities previously performed by NIPC and the other transferred functions and organizations. Further, the official stated that the department is enhancing those activities as they are integrated within the new department and are developing a business plan. The DHS official stated that the department is continuing previously established efforts to maintain and build relationships with other federal entities, including the FBI and other NIPC partners, and with the private sector. In addition, the department plans to provide staff to work at the proposed Terrorist Threat Integration Center. Although NIPC experienced the loss of certain senior leadership prior to transition to the new department and have identified some staffing needs, the DHS official stated that the department is able to provide the functions previously performed by NIPC.

[46] *The White House*, Executive Order 13286—Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security *(Washington, D.C.: Feb. 28, 2003)*.

The Nation Faces Ongoing CIP Challenges

Although the actions taken to date are major steps to more effectively protect our nation's critical infrastructures, we have made numerous recommendations over the last several years concerning CIP challenges that still need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in progress. However, even greater efforts are needed to address them. These challenges include developing a comprehensive and coordinated national CIP plan, improving information sharing on threats and vulnerabilities, improving analysis and warning capabilities, and ensuring appropriate incentives to encourage entities outside of the federal government to increase their CIP efforts. It is also important that CIP efforts be appropriately integrated with DHS.

A Comprehensive and Coordinated National CIP Plan Needs to Be Developed

An underlying issue in the implementation of CIP is that no national plan yet exists that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures. Such a clearly defined plan is essential for defining the relationships among all CIP organizations to ensure that the approach is comprehensive and well coordinated. Since 1998, we have reported on the need for such a plan and made numerous related recommendations.

In September 1998, we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of federal entities was important to ensure governmentwide cooperation and support for PDD 63.[46] At that time, we recommended that OMB and the Assistant to the President for National Security Affairs ensure such coordination.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public/private partnership to defend our national infrastructures. However, this plan focused largely on federal cyber CIP efforts, saying little about the private-sector role.

[46] *U.S. General Accounting Office*, Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk, *GAO/AIMD-98-92 (Washington, D.C.: September 23, 1998).*

In September 2001, we reported that agency questions had surfaced regarding specific roles and responsibilities of entities involved in cyber CIP and the timeframes within which CIP objectives were to be met, as well as guidelines for measuring progress.[47] Accordingly, we made several recommendations to supplement those we had made in the past. Specifically, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government's strategy to address computer-based threats define

- specific roles and responsibilities of organizations involved in CIP and related information security activities;
- interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementing vulnerability assessments and related remedial plans; and
- performance measures for which entities can be held accountable.

In July 2002 we issued a report identifying at least 50 organizations that were involved in national or multinational cyber CIP efforts, including 5 advisory committees, 6 Executive Office of the President organizations, 38 executive branch organizations associated with departments, agencies, or intelligence organizations, and 3 other organizations.[48] Although our review did not cover organizations with national physical CIP responsibilities, the large number of organizations that we did identify as involved in CIP efforts presents a need to clarify how these entities coordinate their activities with each other. Our report also stated that PDD 63 did not specifically address other possible critical sectors and their respective federal agency counterparts. Accordingly, we recommended that the federal government's strategy also

- include all relevant sectors and define the key federal agencies' roles and responsibilities associated with each of these sectors, and
- define the relationships among the key CIP organizations.

In July 2002, the *National Strategy for Homeland Security* called for interim cyber and physical infrastructure protection plans that DHS would use to build a comprehensive national infrastructure plan. According to the *National Strategy for Homeland Security*, the national plan is to provide a methodology for identifying and prioritizing critical assets, systems, and functions, and for sharing protection responsibility with state and local government and the private sector. The plan is to establish

[47] U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations, GAO-01-822* (Washington, D.C.: September 20, 2001).

[48] U.S. General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GAO-02-474 (Washington, D.C.: July 15, 2002).

standards and benchmarks for infrastructure protection and provide a means to measure performance. The strategy also states that DHS is to unify the currently divided responsibilities for cyber and physical security. In November 2002, as mentioned previously, the Homeland Security Act of 2002 created DHS and, among other things, required it to develop a comprehensive national plan.

In February 2003, the President issued the interim strategies—*The National Strategy to Secure Cyberspace* and *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (hereafter referred to in this testimony as the cyberspace security strategy and the physical protection strategy). Both define strategic objectives for protecting our nation's critical assets. These strategies identify priorities, actions, and responsibilities for the federal government, including federal lead departments and agencies and DHS, as well as for state and local governments and the private sector. The two do not (1) clearly indicate how the physical and cyber efforts will be coordinated; (2) define the roles, responsibilities, and relationships among the key CIP organizations, including state and local governments and the private sector; (3) indicate time frames or milestones for their overall implementation or for accomplishing specific actions or initiatives; or (4) establish performance measures for which entities can be held responsible. Until a comprehensive and coordinated plan is completed that unifies the responsibilities for cyber and physical infrastructures; identifies roles, responsibilities, and relationships for all CIP efforts; establish time frames or milestones for implementation; and establishes performance measures, our nation risks not having a consistent and appropriate framework to deal with growing threats to its critical infrastructure.

Better Information Sharing on Threats and Vulnerabilities Must Be Implemented

Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber attacks, which could threaten the national welfare. Information on threats, vulnerabilities, and incidents experienced by others can help identify trends, better understand the risks faced, and determine what preventive measures should be implemented. However, as we have reported in recent years, establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult. In addition, the private sector has expressed concerns about sharing information with the government and the difficulty of obtaining security clearances.

In October 2001, we reported on information sharing practices that could benefit CIP.[49] These practices include

[49] *U.S. General Accounting Office,* Information Sharing: Practices That Can Benefit Critical Infrastructure Protection; *GAO-02-24 (Washington, D.C.: Oct. 15, 2001).*

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- developing standards and agreements on how shared information will be used and protected;
- establishing effective and appropriately secure communications mechanisms; and
- taking steps to ensure that sensitive information is not inappropriately disseminated, which may require statutory changes.

A number of activities have been undertaken to build relationships between the federal government and the private sector, such as InfraGard, the Partnership for Critical Infrastructure Security, efforts by the CIAO, and efforts by lead agencies to establish ISACs. For example, the InfraGard Program, which provides the FBI and NIPC with a means of securely sharing information with individual companies, has expanded substantially. By early January 2001, 518 entities were InfraGard members—up from 277 members in October 2000. Members include representatives from private industry, other government agencies, state and local law enforcement, and the academic community. As of February 2003, InfraGard members totaled over 6,700.

As stated above, PDD 63 encouraged the voluntary creation of ISACs to serve as the mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information between the private sector and the federal government through NIPC. ISACs are critical since private-sector entities control over 80 percent of our nation's critical infrastructures. Their activities could improve the security posture of the individual sectors, as well as provide an improved level of communication within and across sectors and all levels of government.

While PDD 63 encouraged the creation of ISACs, it left the actual design and functions of the ISACs, along with their relationship with NIPC, to be determined by the private sector in consultation with the federal government. PDD 63 did provide suggested activities which the ISACs could undertake, including:

- establishing baseline statistics and patterns on the various infrastructures;
- serving as a clearinghouse for information within and among the various sectors;
- providing a library for historical data for use by the private sector and government; and
- reporting private-sector incidents to NIPC.

In April 2001, we reported that NIPC and other government entities had not developed fully productive information-sharing relationships but that NIPC had undertaken a range of initiatives to foster information sharing relationships with ISACs, as well as with government and international entities. We recommended that NIPC formalize relationships with ISACs and develop a plan to foster a two-way exchange of information between them.

In response to our recommendations, NIPC officials told us in July 2002 that an ISAC development and support unit had been created, whose mission was to enhance private-sector cooperation and trust so that it would result in a two-way sharing of information. DHS now reports that there are currently 16 ISACs, including ISACs established for sectors not identified as critical infrastructure sectors. Table 3 lists the current ISACs identified by DHS and the lead agencies. DHS officials stated that they have formal agreements with most of the current ISACs.

Table 3: Lead Agencies and ISAC Status by CIP Sector

Sectors	Designated lead agency	ISAC established
Sectors Identified by PDD 63		
Information and Telecommunications	Homeland Security*	
Information technology		✓
Telecommunications		✓
Banking and finance	Treasury	✓
Water	Environmental Protection Agency	✓
Transportation	Homeland Security*	
Aviation		
Surface Transportation		✓
Maritime		prospective
Trucking		✓
Emergency Services**	Homeland Security*	
Emergency law enforcement		✓
Emergency fire services		✓
*Government***		
Interstate		✓
Energy	Energy	
Electric power		✓
Oil and gas		✓
Public health	Health and Human Services	
Sectors identified by *The National Strategy for Homeland Security*		
Food		✓
Meat and poultry	Agriculture	
All other food products	Health and Human Services	
Agriculture	Agriculture	
Chemical industry and Hazardous materials	Environmental Protection Agency	
Chemicals		✓
Defense industrial base	Defense	
Postal and shipping	Homeland Security	
National monuments and icons	Interior	
Other Sectors that have established ISACs		
Research and Education Networks		✓
Real estate		✓

*The lead agencies previously designated by PDD 63 were (from top to bottom) the Department of Commerce, Department of Transportation, Department of Justice/Federal Bureau of Investigation, and the Federal Emergency Management Agency.

**PDD 63 identified as critical sectors (1) emergency law enforcement and (2) emergency fire services and continuity of government. In the new *National Strategy for Homeland Security*, emergency law enforcement and emergency fire services are both included in an emergency services sector. Also, continuity of government, along with continuity of operations, is listed as a subcomponent under the government sector.

In spite of progress made in establishing ISACs, additional efforts are needed. All sectors do not have a fully established ISAC, and of those sectors that do, there is mixed participation. The amount of information being shared between the federal government and private-sector organizations also varies. Specifically, the five ISACs we recently reviewed[60] showed different levels of progress in implementing the PDD 63 suggested activities. Specifically, four of the five reported that efforts to establish baseline statistics were still in progress. Also, while all five reported that they serve as the clearinghouse for their own sectors, only three of the five reported that they are also coordinating with other sectors. Only one of the five ISACs reported that it provides a library of incidents and historical data that is available to both the private sector and the federal government, and although three additional ISACs do maintain a library, it is available only to the private sector. The one remaining ISAC reported that they had yet to develop a library but have plans to do so. Finally, four of the five stated that they report incidents to NIPC on a regular basis.

Some in the private sector have expressed concerns about voluntarily sharing information with the government. Specifically, concerns have been raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith. For example, neither the information technology nor the energy or the water ISACs share their libraries with the federal government because of concerns that information could be released under FOIA. And, officials of the energy ISAC stated that they have not reported incidents to NIPC because of FOIA and antitrust concerns.

Other obstacles to information sharing, previously mentioned in congressional testimony, include difficulty obtaining security clearances for ISAC personnel and the reluctance to disclose corporate information. In July 2002 congressional testimony, the Director of Information Technology for the North American Electric Reliability Council stated that the owners of critical infrastructures need access to more specific threat information and analysis from the public sector and that this may require either more security clearances or declassifying information.[61]

There will be continuing debate as to whether adequate protection is being provided to the private sector as these entities are encouraged to disclose and exchange information on both physical and cyber security problems

[60] *U.S. General Accounting Office*, Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors; *GAO-03-233 (Washington, D.C.: Feb. 28, 2003).*

[61] *Testimony of Lynn P. Constantini, Director, Information Technology, North American Electric Reliability Council, before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerc U.S. House of Representatives, July 9, 2002.*

and solutions that are essential to protecting our nation's critical infrastructures. The *National Strategy for Homeland Security*, which outlines 12 major legislative initiatives, includes "enabling critical infrastructure information sharing." It states that the nation must meet this need by narrowly limiting public disclosure of information relevant to protecting our physical and cyber critical infrastructures in order to facilitate its voluntary submission. It further states that the Attorney General will convene a panel to propose any legal changes necessary to enable sharing of essential homeland security related information between the federal government and the private sector.

Actions have already been taken by the Congress and the administration to strengthen information sharing. For example, the USA PATRIOT Act promotes information sharing among federal agencies, and numerous terrorism task forces have been established to coordinate investigations and improve communications among federal and local law enforcement.[52] Moreover, the Homeland Security Act of 2002 includes provisions that restrict federal, state, and local government use and disclosure of critical infrastructure information that has been voluntarily submitted to the DHS. These restrictions include exemption from disclosure under FOIA, a general limitation on use to CIP purposes, and limitations on use in civil actions and by state or local governments. The act also provides penalties for any federal employee who improperly discloses any protected critical infrastructure information. At this time, it is too early to tell what impact the new law will have on the willingness of the private sector to share critical infrastructure information.

Information sharing within the government also remains a challenge. In April 2001, we reported that NIPC and other government entities had not developed fully productive information sharing and cooperative relationships.[53] For example, federal agencies had not routinely reported incident information to NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to report such information to the General Services Administration's FedCIRC. Further, NIPC and DOD officials agreed that their information-sharing procedures needed improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts. The NIPC director stated in July 2002 that the relationship between NIPC and other government entities had significantly improved since our review, and the quarterly meetings with senior government leaders were instrumental in improving information sharing. In addition, in

[52] *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), Public Law No. 107-56, October 26, 2001.*

[53] *U.S. General Accounting Office,* Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities, *GAO-01-323 (Washington, D.C.: April. 24, 2001).*

testimony subsequent to our work, officials from the FedCIRC and the U.S. Secret Service discussed the collaborative and cooperative relationships that had since been formed between their agencies and NIPC.

The private sector has also expressed its concerns about the value of information being provided by the government. For example, in July 2002 the President for the Partnership for Critical Infrastructure Security stated in congressional testimony that information sharing between the government and private sector needs work, specifically, in the quality and timeliness of cyber security information coming from the government.[54]

The cyberspace security strategy reiterates that the federal government encourages the private sector to continue to establish ISACs and to enhance the analytical capabilities of existing ISACs. It states that ISACs will play an increasingly important role in the national cyberspace security response system and the overall missions of homeland security. In addition, the physical protection strategy states that the overall management of information sharing activities among government agencies and between public and private sectors has lacked proper coordination and facilitation. The physical protection strategy also establishes specific initiatives for creating more effective and efficient information sharing, including defining protection-related information sharing requirements and promoting the development and operation of critical sector ISACs, and implementing the statutory authorities and powers of the Homeland Security Act of 2002.

Analysis and Warning Capabilities Need to Be Improved

Another key CIP challenge is to develop more robust analysis and warning capabilities to identify threats and provide timely warnings, including an effective methodology for strategic analysis and a framework for collecting needed threat and vulnerability information. Such capabilities need to address both cyber and physical threats.

NIPC was established in PDD 63 as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. Specifically, the directive assigned NIPC the responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to computer-based incidents; providing law enforcement investigation and response, monitoring reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing. This responsibility requires obtaining and analyzing intelligence, law

[54] *Testimony of Kenneth C. Watson, President, Partnership for Critical Infrastructure Security, before the Subcommittee on Oversight and Investigation of the Energy and Commerce Committee, U.S. House of Representatives, July 9, 2002.*

enforcement, and other information to identify patterns that may signal that an attack is under way or imminent. Similar activities are also called for in DHS's Information Analysis and Infrastructure Protection Directorate, which has absorbed NIPC.

In April 2001, we reported on NIPC's progress in developing national capabilities for analyzing threat and vulnerability data, issuing warnings, and responding to attacks, among other issues.[55] Overall, we found that while progress in developing these capabilities was mixed, NIPC had initiated a variety of CIP efforts that had laid a foundation for future governmentwide efforts. In addition, NIPC had provided valuable support and coordination related to investigating and otherwise responding to attacks on computers. However, at the close of our review, the analytical capabilities that PDD 63 asserted were needed to protect the nation's critical infrastructures had not yet been achieved, and NIPC had developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

At the time of our review, NIPC had issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. In addition, it had issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis. We reported that the use of strategic analysis to determine the potential broader implications of individual incidents had been limited. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. Identifying such threats assists in proactively managing risk, including evaluating the risks associated with possible future incidents and effectively mitigating the impact of such incidents.

We also reported that three factors hindered NIPC's ability to develop strategic analytical capabilities:[56]

- First, there was no generally accepted methodology for analyzing strategic cyber-based threats. For example, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.
- Second, NIPC had sustained prolonged leadership vacancies and did not have adequate staff expertise, in part because other federal

[55] *U.S. General Accounting Office,* Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities, *GAO-01-323 (Washington, D.C.: Apr. 25, 2001).*

[56] *GAO-01-323, April 25, 2001.*

agencies had not provided the originally anticipated number of detailees. For example, at the close of our review in February 2001, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of NIPC's 3-year existence. In addition, NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimated were needed to develop analytical capabilities.

- Third, NIPC did not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work, only three industry assessments had been partially completed, and none had been provided to NIPC. In September 2001, we reported that although outreach efforts had raised awareness and improved information sharing, substantive, comprehensive analysis of infrastructure sector interdependencies and vulnerabilities had been limited.

To provide a warning capability, NIPC had established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. While some warnings were issued in time to avert damage, most of the warnings, especially those related to viruses, pertained to attacks under way. We reported that NIPC's ability to issue warnings promptly was impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks; (2) a shortage of skilled staff; (3) the need to ensure that NIPC does not raise undue alarm for insignificant incidents; and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations under way.

In addition, NIPC's own plans for further developing its analysis and warning capabilities were fragmented and incomplete. The relationships between the Center, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council were unclear regarding who had direct authority for setting NIPC priorities and procedures and providing NIPC oversight. As a result, no specific priorities, milestones, or program performance measures existed to guide NIPC's actions or provide a basis for evaluating its progress.

In our report, we recognized that the administration was reviewing the government's infrastructure protection strategy and recommended that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategically analyzing computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data;
- require the development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and
- clearly define the role of NIPC in relation to other government and private-sector entities.

In July 2002, NIPC's director stated that, in response to our report's recommendations, NIPC had developed a plan with goals and objectives to improve its analysis and warning capabilities and had made considerable progress in this area. The plan establishes and describes performance measures both for its analysis and warning section and for other issues relating to staffing, training, investigations, outreach, and warning. In addition, the plan describes the resources needed to reach the specific goals and objectives for the analysis and warning section. The director also stated that the analysis and warning section had created two additional teams to bolster its analytical capabilities: (1) the critical infrastructure assessment team to focus efforts on learning about particular infrastructures and coordinating with respective infrastructure efforts and (2) the collection operations intelligence liaison team to coordinate with various entities within the intelligence community. The director added that NIPC (1) started holding a quarterly meeting with senior government leaders of entities that it regularly works with to better coordinate its analysis and warning capabilities; (2) had developed close working relationships with other CIP entities involved in analysis and warning activities, such as FedCIRC, DOD's Joint Task Force for Computer Network Operations, Carnegie Mellon's CERT Coordination Center, and the intelligence and anti-virus communities; and (3) had developed and implemented procedures to more quickly share relevant CIP information, while separately continuing any related law enforcement investigation.

The director also stated in July 2002 that NIPC had received sustained leadership commitment from key entities, such as the CIA and the National Security Agency, and that it continued to increase its staff primarily through reservists and contractors. However, the director acknowledged that our recommendations were not fully implemented and that despite the accomplishments to date, much more had to be done to create the robust analysis and warning capabilities needed to adequately address cyberthreats.

Another challenge confronting the analysis and warning capabilities of our nation is that, historically, our national CIP attention and efforts have been

focused on cyber threats. In April 2001, we reported that while PDD 63 covers both physical and computer-based threats, federal efforts to meet the directive's requirements have pertained primarily to computer-based threats, since this was an area that the leaders of the administration's CIP strategy view as needing attention. In July 2002, NIPC reported that the potential for concurrent cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure. In July 2002, the director of NIPC told us that NIPC had begun to develop some capabilities for identifying physical CIP threats. For example, NIPC had developed thresholds with several ISACs for reporting physical incidents and, since January 2002, has issued several information bulletins concerning physical CIP threats. However, NIPC's director acknowledged that fully developing this capability will be a significant challenge. The physical protection strategy states that DHS will maintain a comprehensive, up to date assessment of vulnerabilities across sectors and improve processes for domestic threat data collection, analysis, and dissemination to state and local government and private industry.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, is received from the intelligence and law enforcement communities. For example, there has been considerable public debate regarding the quality and timeliness of intelligence data shared between and among relevant intelligence, law enforcement, and other agencies. Also, as the transfer of NIPC to DHS organizationally separated NIPC from the FBI's law enforcement activities, including the Counterterrorism Division and NIPC field agents, it will be critical to establish mechanisms for continued communication to occur. Further, it will be important that the relationships between the law enforcement and intelligence communities and the new DHS are effective and that appropriate information is exchanged on a timely basis.

In January 2003, the President announced the creation of a multi-agency Terrorist Threat Integration Center (TTIC) to merge and analyze terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture. The center will be formed from elements of the Department of Homeland Security, the FBI's Counterterrorism Division, the Director of Central Intelligence's Counterterrorist Center, and the Department of Defense.[57] Specifically, the President stated that it would:

- optimize the use of terrorist threat-related information, expertise, and capabilities to conduct threat analysis and inform collection strategies;

[57] *The White House*, Fact Sheet: Strengthening Intelligence to Better Protect America *(Washington, D.C.: Jan. 28, 2003)*.

- create a structure that ensures information sharing across agency lines in a way consistent with our national values of privacy and civil liberties;
- integrate terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture; and
- be responsible and accountable for providing terrorist threat assessments for our national leadership.

The TTIC is scheduled to begin operations within the CIA's facilities on May 1, 2003, but will eventually move to a new, independent facility. The center is to receive $50 million in fiscal year 2004. The TTIC will fuse international threat-related information from the CIA with domestic threat-related information collected by the FBI's Joint Terrorism Task Forces and analyzed by a separate FBI information-analysis center.

In addition, according to NIPC's director, as of July 2002, a significant challenge in developing a robust analysis and warning function is the development of the technology and human capital capacities to collect and analyze substantial amounts of information. Similarly, the Director of the FBI testified in June 2002 that implementing a more proactive approach to preventing terrorist acts and denying terrorist groups the ability to operate and raise funds require a centralized and robust analytical capacity that did not exist in the FBI's Counterterrorism Division.[68] He also stated that processing and exploiting information gathered domestically and abroad during the course of investigations requires an enhanced analytical and data mining capacity that was not then available. Furthermore, NIPC's director stated that multiagency staffing, similar to NIPC, is a critical success factor in establishing an effective analysis and warning function and that appropriate funding for such staff is important.

The *National Strategy for Homeland Security* identified intelligence and warning as one of six critical mission areas and called for major initiatives to improve our nation's analysis and warning capabilities. The strategy also stated that no government entity was then responsible for analyzing terrorist threats to the homeland, mapping these threats to our vulnerabilities, and taking protective action. The Homeland Security Act gives such responsibility to the new DHS. Further, the Act gives DHS broad statutory authority to access intelligence information, as well as other information, relevant to the terrorist threat and to turn this information into useful warnings. For example, according to a White House fact sheet, DHS's Information Analysis and Infrastructure

[68] *Testimony of Robert S. Mueller, III, Director Federal Bureau of Investigation, before the Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, Committee on Appropriations, U.S. House of Representatives, June 21, 2002.*

Protection Directorate is to receive and analyze terrorism-related information from the TTIC.[59]

An important aspect of improving our nation's analysis and warning capabilities is having comprehensive vulnerability assessments. The President's *National Strategy for Homeland Security* also stated that comprehensive vulnerability assessments of all of our nation's critical infrastructures are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given sector and then invest accordingly to protect it. The strategy stated that the U.S. government does not perform vulnerability assessments of the nation's entire critical infrastructure. The Homeland Security Act of 2002 stated DHS's Under Secretary for Information Analysis and Infrastructure Protection is to carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructures of the United States.

Additional Incentives Are Needed to Encourage Increased Nonfederal Efforts

The President's fiscal year 2004 budget request for the new DHS includes $829 million for information analysis and infrastructure protection, a significant increase from the estimated $177 million for fiscal year 2003. In particular, the requested funding for protection includes about $500 million to identify key critical infrastructure vulnerabilities and support the necessary steps to ensure that security is improved at these sites. Although it also includes almost $300 million for warning advisories, threat assessments, a communications system, and outreach efforts to state and local governments and the private sector, additional incentives may still be needed to encourage nonfederal entities to increase their CIP efforts.

PDD 63 also stated that sector liaisons should identify and assess economic incentives to encourage the desired sector behavior in CIP. Further, to facilitate private-sector participation, it encouraged the voluntary creation of information sharing and analysis centers (ISACs) that could serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. Consistent with the original intent of PDD 63, the *National Strategy for Homeland Security* states that, in many cases, sufficient incentives exist in the private market for addressing the problems of CIP. However, the strategy also discusses the need to use policy tools to protect the health, safety, or well-being of the American people. It mentions federal grants programs to assist state and local efforts, legislation to create incentives for the private sector, and, in some cases, regulation. The physical security strategy reiterates that

[59] *The White House*, Fact Sheet: Strengthening Intelligence to Better Protect America *(Washington, D.C.: Jan. 28, 2003)*.

additional regulatory directives and mandates should only be necessary in instances where the market forces are insufficient to prompt the necessary investments to protect critical infrastructures and key assets. The cyberspace security strategy also states that the market is to provide the major impetus to improve cyber security and that regulation will not become a primary means of securing cyberspace.

Last year, the Comptroller General testified on the need for strong partnerships with those outside the federal government and that the new department would need to design and manage tools of public policy to engage and work constructively with third parties.[60] We have previously testified on the choice and design of public policy tools that are available to governments.[61] These public policy tools include grants, regulations, tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address security concerns. Some of these tools are already being used. For example, as the lead agency for the water sector, the EPA reported providing approximately 449 grants totaling $51 million to assist large drinking water utilities in developing vulnerability assessments, emergency response/operating plans, security enhancement plans and designs, or a combination of these efforts.

In a different approach, the American Chemistry Council, the ISAC for the chemical sector, requires as a condition for membership that its members perform enhanced security activities, including vulnerability assessments. However, because a significant percentage of companies that operate major hazardous chemical facilities do not perform these voluntary security activities, the physical security strategy recognized that mandatory measures may be required. The strategy stated that EPA, in consultation with DHS and other federal, state, and local agencies, will review current laws and regulations pertaining to the sale and distribution of highly toxic substances to determine whether additional measures are necessary. Moreover, the strategy also stated that DHS, in concert with EPA, will work with Congress to enact legislation requiring certain facilities, particularly those that maintain large quantities of hazardous chemicals in close proximity to large populations, to enhance site security.

Without appropriate consideration of public policy tools, private sector participation in sector-related CIP efforts may not reach its full potential. For example, we reported in January 2003 on the efforts of the financial services sector to address cyber threats, including industry efforts to share information and to better foster and facilitate sectorwide efforts. We also reported on the efforts of federal entities and regulators to partner with

[60]U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will Be Pivotal to Success*, GAO-02-886T (Washington, D.C.: June 25, 2002).

[61]U.S. General Accounting Office, *Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy*, GAO-02-549T (Washington, D.C.: Mar. 28, 2002).

the financial services industry to protect critical infrastructures and to address information security. We found that although federal entities had a number of efforts ongoing, Treasury, in its role as sector liaison, had not undertaken a comprehensive assessment of the potential public policy tools to encourage the financial services sector in implementing CIP-related efforts. Because of the importance of considering public policy tools to encourage private sector participation, we recommended that Treasury assess the need for public policy tools to assist the industry in meeting the sector's goals. In addition, in February 2003, we reported on the mixed progress five ISACs had made in accomplishing the activities suggested by PDD 63. We recommended that the responsible lead agencies assess of the need for public policy tools to encourage increased private-sector CIP activities and greater sharing of intelligence and incident information between the sectors and the federal government.

In summary, through audit and evaluation results and the management review and reporting requirements implemented through GISRA and now FISMA, agencies have increased management attention to information security and begun to show progress in correcting identified weaknesses. In addition, continued guidance and OMB and congressional oversight have emphasized the ongoing commitment to improving the federal government's information security. Such efforts must be sustained to help ensure that federal agencies are responding to and providing appropriate protections against the growing threat to the systems that support their missions and provide vital services to the American people. Further, we believe that a comprehensive strategy addressing certain key issues would help to guide these efforts and ensure that they are coordinated and consistently implemented governmentwide.

Over the last several years, we have also identified various challenges to the implementation of CIP that need to be addressed. Although improvements have been made and continuing efforts are in progress, greater efforts are still needed to effectively address them. These challenges include developing a comprehensive and coordinated national plan, improving information sharing on threats and vulnerabilities between the private sector and the federal government as well as within the government itself, improving analysis and warning capabilities, and encouraging entities outside the federal government to increase CIP efforts. It is also important to emphasize that much of the success of ensuring the security of our nation's critical infrastructure will depend on appropriately integrating all CIP efforts with the implementation of the new DHS.

Mr. Chairman, this concludes my written testimony. I would be pleased to answer any questions that you or other members of the Subcommittee

may have at this time. If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by e-mail at dacevr@gao.gov.

(310189)

Mr. PUTNAM. Thank you very much, Mr. Dacey. We appreciate all of the remarks of the panel.

I will recognize Mr. Clay for his questions.

Mr. CLAY. Thank you, Mr. Chairman. Mr. Dacey, Mr. Clarke suggested that GAO should develop the capacity to give Congress real-time security reports on all executive agencies' computer systems. Is GAO prepared to undertake this responsibility?

Mr. DACEY. Not as of today. I would say that we have been doing reviews, and, in fact, while Mr. Pyke did not say prior to his appointment as CIO, we had done a review of Commerce and I am very pleased to hear of the progress they have made in the last 2 years since that. We certainly have a suite of tools, and there are tools available commercially, that can be used to assess security in systems, to scan them, so to speak. We use them, other people in the commercial sector use them to do testing of networks. So in terms of technologies, those types of systems are available. Now, what we run into routinely when we go to agencies is we have to figure out how to run them on their systems and how to interface, and how to use them on their networks and how their networks are configured, which actually takes a large amount of our time to do that.

So I guess the question of active monitoring, GAO has and continues to support that agencies should be regularly monitoring their systems for these kinds of vulnerabilities, and there are thousands, I heard a number before but there are literally thousands of these vulnerabilities. I do know that NASA has undertaken for the last year or so a project to actually assess all of their networks for a subset of vulnerabilities, 20 or 30 odd vulnerabilities, I forget the exact number, that they actively report on to agency management in terms of whether those vulnerabilities exist. They have metrics and measurements performance measures against that.

So, at least with respect to a subset, I think it has been demonstrated that agencies can do that. I will leave it to Congress and others to decide who will do that. But certainly it is very possible to be done.

Mr. CLAY. OK. It is my understanding that the National Institute of Standards and Technology is about to release a draft of security standards required under FISMA. Have you reviewed those standards? And if not, what are your plans for reviewing them?

Mr. DACEY. FISMA required NIST to develop basically risk levels and minimum security standards for each risk level. Separately, as part of the Cyber Research and Development Act, NIST is required to develop checklists for settings on technologies that are widely used or will be widely used in the Federal Government. FISMA made as one of its requirements that NIST consult with GAO on this issue, and they have consulted with us thus far. They are still actively developing those standards. What we have done is to basically look at what we use in terms of our audit process, what do we audit against and trying to ensure that their standards would at least include at a minimum the kind of things that we look for when we do our audits. So that process is taking place. I cannot say exactly when those standards will be developed, but they are intended I understand to be developed for public exposure and comment.

Mr. CLAY. Thank you. Mr. Pyke, in the last panel, Mr. Clarke suggested that IT security be contracted to private firms with penalties on the contractor for breaches. I would like to hear your thoughts on that suggestion.

Mr. PYKE. Mr. Clay, I respectfully disagree with that particular recommendation, although I think that there is plenty of room for us to outsource many of the capabilities we need to have a complete and effective IT security program. As we have done in Commerce from the Secretary on down, I think it is very important to have personal accountability of our managers for the management of IT security. I also think it is important to have a high level individual or individuals responsible for IT security within the organization. When I was the CIO of the National Oceanic and Atmospheric Administration, I raised IT security to the top level within the CIO office. At the Commerce Department, we have IT security and critical infrastructure protection at the top level within the Commerce CIO office. I should add that we have full-time individuals responsible for each of these important functions.

So I do not think the responsibility for IT security within any Federal agency can be delegated by outsourcing. But I do think, especially since we all face a shortfall of the scarce resources necessary to keep on top of IT security, I do think that it is an excellent idea to take advantage of outsourcing to get the job done.

Mr. CLAY. Mr. Pyke, let me also ask you about the Census Bureau. Do they have an enterprise architecture for the modernization of its geographic system, and has your office reviewed that architecture?

Mr. PYKE. Yes. The Census Bureau does have an architecture, and their overall architecture for the agency as a whole and for moving ahead toward the next decennial census is a part of the overall enterprise architecture that we have for the entire Department of Commerce.

Mr. CLAY. What is the cost of this modernization project?

Mr. PYKE. Are you talking about the census modernization?

Mr. CLAY. Yes.

Mr. PYKE. If I may, sir, I would like to provide that number for you for the record.

Mr. CLAY. That will be fine. Thank you.

Ms. MacLean, the last question. Has the banking industry been concerned about sharing information with the Federal Government? And does the FOIA exclusion passed as part of Homeland Security address those concerns?

Ms. MACLEAN. That is a very great question. The financial services sector as a whole believes strongly that FOIA protection is critical to our ability to share information with the Federal Government. Being able to share that information without fear of disclosure of specifics I think is very, very important. So, keeping with that FOIA protection another aspect of that, if we go back to Y2K and the way that Y2K protection was handled with the FOIA; also, liability protection is another aspect that we feel is important.

Mr. CLAY. Thank you. Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Clay. I would like to followup on that question with Ms. MacLean. What would be the threshold of breach or the threshold of cyber threat or cyber attack that would

trigger the need for a public disclosure to the customer or client whose information is jeopardized?

Ms. MACLEAN. I would like to say it somewhere happens naturally. We do share information today as part of our Information Sharing and Analysis Center. We have an FSISAC where today we share information among institutions. We also are required by law and by regulation to notify the Government of any major breach through our SAR program at the financial institution level.

I think making things public really just depends on whether or not there is that need that would assist us in helping resolve the issue. I do not think that it is conducive to make that public every time there is a breach. I think one of the metrics, and I heard you say earlier in the very beginning about the increased numbers of incidents, I actually think that is a positive metric. I think we should be looking for those reports to go up. But I do not think you necessarily need to make those public in order to work the issues and determine what vulnerabilities need to be addressed.

Mr. PUTNAM. Is there a current Federal law or regulation that requires a customer or client whose information may have been breached to be notified? If there is not, what is your company's policy?

Ms. MACLEAN. Yes, from a privacy perspective. And in the State of California, I think it was mentioned earlier, that if there is a breach where public or private information is compromised, you are required to notify that customer. That is different than going on CNN and making that public. It is also for the protection of those customers that I do believe the customer should be notified but not necessarily make all that information public because it does violate their privacy from another aspect.

Mr. PUTNAM. Mr. Pyke, your role as CIO of Commerce, you have oversight for critical infrastructure protection, is that correct?

Mr. PYKE. That is correct.

Mr. PUTNAM. Not just within the Department itself but within the infrastructures that are within the jurisdiction of the Department?

Mr. PYKE. I have responsibility for critical infrastructure within the Department. I am the Critical Infrastructure Assurance Officer.

Mr. PUTNAM. OK. So if there is a substantial cyber threat on an industry within the regulation of the Department of Commerce, are you the first one notified or is someone in Homeland Security the first one notified?

Mr. PYKE. I am notified only when there is a threat or possible threat to our systems and data, not to the sectors of industry that we relate to or interact with. My understanding is that is where the Department of Homeland Security comes in. They are one of the sources of alerts to us about a possible threat, and, as Mr. Forman mentioned, we received three very helpful alerts fairly recently that we and the other agencies across Government have been able to react to. I would hope that those kinds of alerts are made available to the private sector as well.

Mr. PUTNAM. Ms. MacLean, one of the recurring themes today has been that there is a high level of reluctance to compel the private sector to report and there is also some tremendous concern about increasing the regulatory role in setting minimum standards.

What are your feelings on the minimum standards and the approach of regulation? How do we incent that in the private sector so that we have the information that we need and we are getting the results that we need without an over-reaching from the regulatory approach?

Ms. MACLEAN. Today, our particular sector, the financial services sector is highly regulated. So, in some ways, we are already the beneficiary of having some of those guidelines in place. There are a number of regulations today. I think it was mentioned, the Graham-Leach-Bliley Act is one of those regulations which incent or require you to put in additional controls.

The second part of that question on how do we make that process, should we make that process and do more of that, I really do not think additional regulation is conducive to actually getting companies to put those controls in place. Risk management, in most companies, especially in the financial sector, is in the business of selling trust. So it is to our advantage to really provide secure services to our customers. The customers demand that. And so there is a market force that really is at the heart of everything we do. We do it because it makes good business sense. And the checks and balances are in place, if you will, through the regulatory agencies who oversee us.

Mr. PUTNAM. Did you agree with the recommendation of the first panel that perhaps the way to get at publicly traded corporations is to have a certified audit process that is reflected in a report to the SEC?

Ms. MACLEAN. I do agree with that. And we do that to an extent today within the financial services sector. I think that would be an effective means. And you are looking more at an effective program versus regulating that program.

Mr. PUTNAM. One of the challenges that has come up is that a number of the issues we deal with are not as much technological challenges as they are human challenges or cultural challenges. How are you or others in the private sector held accountable for protecting your infrastructure from security breaches?

Ms. MACLEAN. My whole job at Bank of America is to provide that leadership, that vision, and I mentioned execution and accountability. I think those are four core things that have to be in place for any effective program. I think within the financial services sector, the way that we have organized with the associations is to provide that leadership and guidance to all of the financial services sector so that we are consistent in our approach.

The other key to this I think is the outreach opportunities, because we are very interdependent on other sectors, such as telecommunications and energy and our government partners, the Federal Reserve Bank, other people with whom we have interdependencies. Making sure that everyone within each link of the chain, if you will, those chains, the links in the chains are all doing the right things. I think the leadership around those best practices and expectations that we have are really critical to having a cohesive integrated program.

Mr. PUTNAM. Let me give you a version of what I asked Mr. Pyke. If you get a report that there is something very suspicious going on, something that is raising red flags in your infrastructure

protection systems, is your first instinct to call the Comptroller General or the Federal Reserve or Homeland Security?

Ms. MACLEAN. My first instinct is to call our crisis management hotline together which includes all of our institutions, and includes our regulators who are a part of that process. And that is part of what the council has put into place. Having that blast message, if you will, which goes out to multiple avenues so that we ensure that we get everybody on the phone, would be the first thing that we would do.

Mr. PUTNAM. And I would assume that would probably be replicated throughout the different sectors—the power company's first response would be to notify FERC or DOE; telecommunications, their equivalent agency or department of jurisdiction. It makes you wonder at what point it finally gets to the people who are in charge of that, which would be Homeland Security.

Mr. Dacey, what is the biggest obstacle that you have found in the failure of the Federal Government to have adequate information security, and is it a human challenge or a technological challenge?

Mr. DACEY. Most of the issue really relates I think to a human challenge. We have many technologies to monitor and manage these systems and I think it is a matter of getting the right amount of attention, focus, responsibility, and accountability in place. What we have now is a situation where some agencies have done better than others. If you look at our written testimony, there are a lot of charts that summarize some of the GISRA reporting for the second year and some agencies are reporting statistics, such as Mr. Pyke, that are quite high and others that are low. And I think the issue is really focusing in on what are the reasons why some of these agencies are doing better than others.

There is no silver bullet to any of this. But one of the things that Mr. Pyke referred to earlier is the fact that he has responsibility for establishing information security standards and monitoring those and maintaining accountability for people to implement those throughout the agency. In many of the agencies that we have looked at, that has not always been the case. The CIO at the agency level has certain responsibilities but oftentimes the component parts of the agency have autonomy to develop and establish their networks and their security. And in those environments, if you have a situation where one component has weak security, that can jeopardize the rest of the agency considering that in most cases their systems are interlinked and oftentimes trusted, so that getting access to one can readily get you access to another.

So I think those are the primary issues. I think OMB laid those out in their first year GISRA report and are continuing to work those issues. If you look at the numbers, again, there is definitely progress being shown. But if you look at some of them, you will see that there is a lot of information we do not have yet. We talk about a process for managing vulnerabilities, but in many cases systems have not really been fully tested or analyzed to identify the vulnerabilities that exist so that it can be fixed. So there is a process here that needs to take place. But, certainly, the GISRA and now FISMA I think have been landmark changes in the way in which information security has been viewed by the agencies.

The last part, which was referred to a little earlier, is research and development. I think it is key that continue in a cohesive fashion so that we can make sure that we are developing the best technologies we have to defend against cyber threats.

Mr. PUTNAM. Certainly, the current in IT management and procurement has been away from the traditional stovepipe system and the inherent redundancies and duplication. But presumably a positive benefit of those stovepipes and of those redundancies is some limited protection from a cyber security threat. For all the consequences of not being able to communicate with one another, the benefits have been that you had some kind of a firewall there. Would you comment on that a little bit. As we press these agencies to tear down stovepipes, what consequence does that have for cyber security?

Mr. DACEY. I think many, if not all, of the agencies have really gotten to a point where they are highly internetworked within themselves. I think, based upon the studies we have done where we have actually gone in and assessed security, we have generally found that, again, the systems are fairly trusted. One of the concerns that we have expressed is not only the impact of an external party coming in, but also internal parties are a threat to security as well. When you have got tens of thousands of users in some of these systems, you really have to be careful to manage that.

What we have not seen in many systems is once we are able to get in, we do try as part of our audits to break into systems both internally and externally, and are generally successful, but when we do that, we typically find that we can use that access to gain privileges throughout the entire network and other places. So to some extent, I think removing the stovepipes in terms of information security is critical or you are going to continue to have that. What we have not seen is really an effective segmenting of networks so that if one is broken into, you cannot get access to other parts. That is certainly technologically possible. And if you follow through FISMA and the idea that there will be different risk level systems, you are going to have to come up with a strategy on segmenting them so you have one high level risk system that does not connect to a low level risk system without appropriate protections.

Mr. PUTNAM. Mr. Pyke, we have heard from Ms. MacLean on the accountability measures that are in place in the private sector to ensure an appropriate commitment to cyber security. What has Secretary Evans empowered you to do that has made the Department of Commerce a model for success in a situation where everyone else is pretty well mired in failure?

Mr. PYKE. Mr. Chairman, one of the things he has done has been not just to empower me as CIO to do my job and do it in a full way, but he has empowered and mandated that the Commerce agency heads, the under secretaries, assistant secretaries, and directors of the individual bureaus or operating units within the Department, that they give their time and attention to computer security, to protecting the infrastructure. And this has opened the way for my staff and me to be able to provide policy guidance, to provide direction, and have it received well. It has opened the way for us to work with the Commerce agencies and have them be responsive when we have an incident that we need to handle.

I might mention with regard to something you asked me earlier in terms of incident handling, we have had at least one incident that I am aware of where we had an intrusion that we reported. When we have an intrusion that we detect we report the incident to FedCIRC, to the Federal Computer Incident Response Center which is now part of the Department of Homeland Security. That particular incident resulted in a Government-wide alert and I believe an alert that went out to the private sector as well with regard to the appropriate measures to take to respond to that particular threat.

Mr. PUTNAM. Thank you, Mr. Pyke.

I want to thank all of our witnesses from both panels for their outstanding testimony and their ability to help us understand what is a very complex issue. It is clear that the time to act is now. We have not made the progress that we need to make to be as prepared as we should be as a Nation. We must all work together to protect our Nation from what could certainly be a digital disaster.

I want to thank Mr. Clay for his input and his support of our efforts on the subcommittee. And recognizing that we were not able to answer all the questions that people had, I will keep the record open for 2 weeks for submitted questions and answers.

Mr. Dacey, Mr. Pyke, Ms. MacLean, we appreciate what you do. We appreciate your service to the subcommittee.

And with that, we stand adjourned.

[Whereupon, at 11:30 a.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]