AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

LESSONS LEARNED FROM THE GOVERNMENT INFORMATION SECURITY REFORM ACT OF 2000

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

MARCH 6, 2002

Serial No. 107–124

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

82–355 PDF WASHINGTON : 2002

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

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

STEPHEN HORN, California, *Chairman*

RON LEWIS, Kentucky
DAN MILLER, Florida
DOUG OSE, California
ADAM H. PUTNAM, Florida

JANICE D. SCHAKOWSKY, Illinois
MAJOR R. OWENS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
CLAIRE BUCKLES, *Professional Staff Member*
JUSTIN PAULHAMUS, *Clerk*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on March 6, 2002	1
Statement of:	
Dacey, Robert F., Director, Information Security, U.S. General Accounting Office; Mark A. Forman, Associate Director, Office of Information Technology and e-Government, Office of Management and Budget; Arden L. Bement, Jr., director, National Institute of Standards and Technology; Roberta L. Gross, former Inspector General, National Aeronautics and Space Administration; Robert G. Gorrie, Deputy Staff Director, Defense-wide Information Assurance Program Office, Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence; and Karen S. Evans, Chief Information Officer, Department of Energy	17
Davis, Hon. Thomas M., a Representative in Congress from the Commonwealth of Virginia	6
Letters, statements, etc., submitted for the record by:	
Bement, Arden L., Jr., director, National Institute of Standards and Technology:	
Followup questions and responses	120
Prepared statement of	73
Dacey, Robert F., Director, Information Security, U.S. General Accounting Office, prepared statement of	20
Davis, Hon. Thomas M., a Representative in Congress from the Commonwealth of Virginia, prepared statement of	10
Evans, Karen S., Chief Information Officer, Department of Energy, prepared statement of	109
Forman, Mark A., Associate Director, Office of Information Technology and e-Government, Office of Management and Budget, prepared statement of	54
Gorrie, Robert G., Deputy Staff Director, Defense-wide Information Assurance Program Office, Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, prepared statement of	98
Gross, Roberta L., former Inspector General, National Aeronautics and Space Administration, prepared statement of	86
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of	3
Schakowsky, Hon. Janice D., a Representative in Congress from the State of Illinois, prepared statement of	69

LESSONS LEARNED FROM THE GOVERNMENT INFORMATION SECURITY REFORM ACT OF 2000

WEDNESDAY, MARCH 6, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Schakowsky, and Maloney.

Staff Present: J. Russell George, staff director and chief counsel; Bonnie Heald, deputy staff director; Claire Buckles, professional staff member; Justin Paulhamus, clerk; Michael Sazonoff, intern; David McMillen, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. HORN. A quorum being present, the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

The Federal Government relies on computer systems to provide essential services to the Nation and its people. These large, complex systems help regulate the economy, collect taxes, pay benefits, and defend the Nation. The speed and accessibility of the technology have greatly enhanced government operations and have provided citizens with nearly instant access to their government.

Yet, those operations are at risk. Computers at the White House, the Department of Defense, the Department of the Treasury, and the Department of the Interior have all been successfully attacked. The security vulnerabilities at the Department of the Interior are so severe that a U.S. District Court judge in Washington has ordered the Department to disconnect its Trust Asset and Accounting Management System from the Internet. This system handles about $500 million a year in royalty and lease payments to Native Americans.

These are not the only troubled agencies, however. In November 2001, the subcommittee issued its second annual report card grading computer security efforts at 24 major executive branch agencies. Overall, the executive branch earned an abysmal grade of "F." That grade was the same during the Clinton administration and now the Bush administration.

We have known for more than a decade that the government's information systems are vulnerable, yet little has changed. In a report issued last month, the Office of Management and Budget concluded that a significant part of the problem falls to senior managers who have failed to focus sufficient attention on computer security. I agree. The various bureaucracies need to be pushed by the political appointees, so we can have a better record.

Since 1987, Congress has passed legislation to address Federal computer security weaknesses. The most recent law, the Government Information Security Reform Act, was enacted in the year 2000. This law requires Federal agencies to assess the nature and sensitivity of the information stored in their computers and then develop appropriate security plans to protect that information. In addition, it requires that, for the first time, agencies conduct annual computer security evaluations and report the results to the Office of Management and Budget.

Agencies filed their first reports in September 2001. Clearly, the full benefits of the law have not been realized. Agencies have not yet developed security plans that balance protection and risk. However, they are beginning to focus on the problem. The act is scheduled to sunset next year.

Today's hearing will explore how Federal agencies have implemented the act and what additional steps might be taken to ensure that effective safeguards are in place. We must identify the weaknesses in order to correct them. We must use the "lessons learned" from the Government Information Security Reform Act to take effective, urgently needed action to ensure that it is reauthorized and improved.

I welcome today's witnesses, and I look forward to working with each of you to ensure the security of the government's information technology resources.

I will enter into the record at this point as an exhibit after my opening remarks the Computer Security Report Card of November 9, 2001.

[The prepared statement of Hon. Stephen Horn follows:]

DAN BURTON, INDIANA,
CHAIRMAN
BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
[illegible] MICA, FLORIDA
[illegible] M. DAVIS III, VIRGINIA
[illegible] A. McINTOSH, INDIANA
MARK E. SOUDER, INDIANA
JOE SCARBOROUGH, FLORIDA
STEVEN C. LATOURETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
ASA HUTCHINSON, ARKANSAS
LEE TERRY, NEBRASKA
JUDY BIGGERT, ILLINOIS
GREG WALDEN, OREGON
DOUG OSE, CALIFORNIA
PAUL RYAN, WISCONSIN
JOHN T. DOOLITTLE, CALIFORNIA
HELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
TTY (202) 225–6852

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER
TOM LANTOS, CALIFORNIA
ROBERT E. WISE, Jr., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
GARY A. CONDIT, CALIFORNIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, Jr., TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

Opening Statement
Representative Steve Horn, R-CA
Chairman, Government Efficiency, Financial Management and Governmental Relations
March 6, 2002

A quorum being present, the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

The federal government relies on computer systems to provide essential services to the nation and its people. These large, complex systems help regulate the economy, collect taxes, pay benefits and defend the nation. The speed and accessibility of the technology have greatly enhanced government operations and have provided citizens with nearly instant access to their government.

Yet, those operations are at risk. Computers at the White House, the Department of Defense, the Department of the Treasury and the Department of the Interior have all been successfully attacked. The security vulnerabilities at the Department of the Interior are so severe that a U.S. District Court judge in Washington has ordered the department to disconnect its Trust Asset and Accounting Management System from the Internet. This system handles about $500 million a year in royalty and lease payments to Native Americans.

These are not the only troubled agencies, however. In November 2001, the subcommittee issued its second annual report card, grading computer security efforts at 24 major executive branch agencies. Overall, the executive branch earned an abysmal grade of "F."

We have known for more than a decade that the government's information systems are vulnerable, yet little has changed. In a report, issued last month, the Office of Management and Budget concluded that a significant part of the problem falls to senior managers who have failed to focus sufficient attention on computer security.

Since 1987, Congress has passed legislation to address federal computer security weaknesses. The most recent law, the Government Information Security Reform Act, was enacted in 2000. This law requires federal agencies to assess the nature and sensitivity of the information stored in their computers and then develop appropriate security plans to protect that information. In addition, it requires that -- for the first time -- agencies conduct annual computer security evaluations and report the results to the Office of Management and Budget.

Agencies filed their first reports in September 2001. Clearly, the full benefits of the law have not been realized. Agencies have not yet developed security plans that balance protection and risk. However, they are beginning to focus on the problem. The Act is scheduled to sunset next year.

Today's hearing will explore how federal agencies have implemented the Act and what additional steps must be taken to ensure that effective safeguards are in place. We must identify the weaknesses in order to correct them. We must use the "lessons learned" from the Government Information Security Reform Act to take effective, urgently needed action to ensure that it is reauthorized and improved.

I welcome today's witnesses. And I look forward to working with each of you to ensure the security of the Government's information technology resources.

Computer Security Report Card

November 9, 2001

Departments and Agencies	Grade
NSF National Science Foundation	B+
SSA Social Security Administration	C+
NASA National Aeronautics & Space Administration	C-
EPA Environmental Protection Agency	D+
STATE Department of State	D+
FEMA Federal Emergency Management Agency	D
GSA General Services Administration	D
HUD Department of Housing and Urban Development	D
Agriculture Department of Agriculture	F
AID Agency for International Development	F
Commerce Department of Commerce	F
Defense Department of Defense	F

Departments and Agencies	Grade
Education Department of Education	F
Energy Department of Energy	F
HHS Department of Health & Human Services	F
Interior Department of the Interior	F
Justice Department of Justice	F
Labor Department of Labor	F
NRC Nuclear Regulatory Commission	F
OPM Office of Personnel Management	F
SBA Small Business Administration	F
Transportation Department of Transportation	F
Treasury Department of the Treasury	F
VA Department of Veterans Affairs	F
Governmentwide Grade	F

Prepared for Chairman Stephen Horn, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. Based on agency reports required by the Security Act of 2000, and GAO and Inspectors General audit reports issued from July 2000 through September 2001.
Subcommittee Home Page: http://www.house.gov/reform/gefmir.htm

Mr. HORN. The ranking member is coming, and I see that my colleague, Mr. Davis, has been here now as panel one, and we're delighted to have you here. You have been a major force in the work of e-government and the work of technology generally. So the gentleman from Virginia, Mr. Davis.

STATEMENT OF HON. THOMAS M. DAVIS, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF VIRGINIA

Mr. DAVIS. Let me first commend you and your staff for the tremendous work you have done on Federal information security during your tenure as chairman of this subcommittee and your previous chairmanship of the Government Management, Information, and Technology Subcommittee. It's a privilege working with you on this critical topic.

I want to thank you for giving me the opportunity to speak on this issue in the context of today's hearing, examining the lessons learned from the implementation of the Government Information Security Reform Act of 2000 [GISRA].

Unquestionably, the events of September 11th and the ensuing war on terrorism have produced a variety of responses throughout the world. Nowhere has the response been so fervent as here in our Nation's Capital. From the creation of the new Office of Homeland Security to security-related legislation, there is an unprecedented awareness of the vulnerabilities we face.

This new awareness has naturally focused more attention on security matters, particularly with respect to information security. Yet, this issue and the fact that Federal information systems continue to be woefully unprotected from both malevolent acts and benign interruptions have presented a grave concern to me for a number of years. I know that you and the members of this subcommittee share that concern as well.

From our work in the Government Reform Committee, it is clear that the state of Federal information security suffers from a lack of coordinated, uniform management. Resolving this problem becomes even more imperative when you consider the many objectives we hope to achieve through the efficient and cost-effective use of information technology and the advancement of electronic government. These objectives include electronic procurement, telecommuting, a comprehensive information-sharing network, and improved provision of services to citizens and businesses. The common element of these goals is the interconnectivity that they each require to facilitate communications between different public and private entities.

Poor information security management has persisted in both the public and private sectors long before IT became the ubiquitous engine driving governmental, business, and even home activities. After all, the information security implicates both the physical and the cyber-environment.

A decade ago, technology stood as one of many factors important to the mission and performance objectives of the Federal Government. But no longer is technology "one of many." Instead, the Information Revolution and the ever-evolving technologies that support its collection, assimilation, and communications have become integral to the functioning of our government.

As our reliance on technology and our desire for interconnectivity have grown over the past decade, intensifying with the advent of the Internet, our vulnerability to attacks has grown exponentially. The high degree of interdependence between information systems, both internally and externally, exposes the Federal Government's computer networks to benign and destructive disruptions. This fact is tremendously important in understanding how we devise a comprehensive and yet flexible strategy for coordinating, implementing, and maintaining Federal information security practices throughout the Federal Government as the threat of electronic terrorism increases.

Yet, Federal information security management continues to falter. Despite consistent evaluations since 1997 showing that Federal information security is a government-wide, high-risk issue, GAO continues to find "pervasive and continuing weaknesses." And, of course, as this subcommittee found last November, 16 of the 24 Federal agencies evaluated in 2001 each received a disappointing grade of "F," with only one agency receiving a grade higher than a "C+."

Of course, while these grades are disappointing, they reflect the difficulty of implementing effective security management without sufficient commitment and guidance from an accountable entity within each agency, and for the Federal Government as a whole.

In July 2000, I introduced legislation that would have created, among other things, a new Federal Chief Information Officer in the Executive Office of the President. One of the primary components of that bill expanded upon the then yet-to-be-enacted Government Information Security Reform Act [GISRA], introduced by Senators Fred Thompson and Joe Lieberman.

My legislation, entitled, "the Federal Information Policy Act" [FIPA], reflected my firm belief that there needs to be an executive branch office that holds both the prestige and the accountability for strategically modernizing our stovepipe IT structure. At the same time, that office must have the authority to prioritize cross-jurisdictional e-government initiatives and networked information and telecommunications networks, in order to achieve efficiencies and secure Federal information systems.

With the establishment of a new office of Associate Director of IT and Electronic Government within the OMB, I have opted to withhold the reintroduction of Federal CIO legislation until I have had an opportunity to evaluate the progress that OMB has been able to achieve in carrying out the administration's Enterprise Information Management and Integration initiative.

That said, my concerns regarding the pervasive and persistent weaknesses in Federal information security management, infrastructure, and accountability remain strong. These are concerns I know you also share, Mr. Chairman, and I applaud your subcommittee's steady work in bringing to the forefront the critical need for immediate and focused attention on this issue.

Yet, I would add that, to the extent that increased security concerns rely on the ability of the public and private sectors to share information securely, it is even more critical that the Federal Government put its own house in order with respect to the security of its own Federal information and telecommunications systems. It is

for this reason that I have just introduced legislation similar to the information security provisions in FIPA, and I am very pleased that you have agreed to co-sponsor this measure with me, Mr. Chairman.

The overall purpose of these efforts is to strengthen the information security management infrastructure of the Federal Government. The bill, entitled, "the Federal Information Security Management Act" [FISMA], undertakes this objective by building on the foundations laid out by GISRA. As you know, GISRA requires every Federal agency to develop and implement security policies that include risk assessment, risk-based policies, security awareness training, and periodic reviews.

With GISRA set to expire on November 29th of this year, the Federal Information Security Management Act permanently reauthorizes this legislation and implements additional measures designed to enable the Federal Government to become a reliable public partner for protecting America's information highways. In general, FISMA streamlines GISRA's provisions and requires that agencies utilize information security best practices that will ensure the integrity, confidentiality, and availability of Federal information systems.

Moreover, the bill seeks to strengthen the role played by the National Institute of Standards and Technology in developing and maintaining standards and guidelines for minimum information security controls. Agencies would be required to identify the risk levels associated with their systems and implement the appropriate level of protections accordingly. This latter objective is especially important in light of the interconnectivity of information systems. We need to implement a framework that ensures that when systems interconnect with each other, there is a uniform management infrastructure and universal benchmark for measuring the risks and vulnerabilities of Federal information systems.

We cannot afford to delay enactment of this legislation. At a time when uncertainty threatens confidence in our Nation's preparedness, the Federal Government must make information security a priority. I am heartened by the President's bold commitment to tying the budget process to individual agency performance, and to using information security as one measurement of that performance. However, the information security cannot go the way of any other "issue du jour." It is a constant management requirement that requires eternal vigilance, and the ranking of its importance to Federal operations cannot fluctuate from one administration to the next.

It is my hope that we take this opportunity, in the context of extending GISRA, to signal Congress' deep concerns that information security is not being taken seriously by every agency and department. We must demand that in our networked era, where technology is the driver, every Federal information system must be managed in a way that minimizes both the risk that a breach or disruption will occur and the harm that would result should such a disruption take place.

We will learn a lot today as we determine the impact that GISRA has had on the information security practices throughout the Federal Government. I very much look forward to working with you,

Mr. Chairman, the members of this subcommittee, and other concerned Members of the House and Senate as we move forward on strengthening GISRA and improving our government's overall information security management. Thank you.

[The prepared statement of Hon. Thomas M. Davis follows:]

STATEMENT OF REPRESENTATIVE TOM DAVIS

BEFORE THE SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT, AND INTERGOVERNMENTAL RELATIONS OF THE HOUSE COMMITTEE ON GOVERNMENT REFORM

"Lessons Learned from the Government Information Security Reform Act of 2000"

Wednesday, March 6, 2002
10 a.m.

Mr. Chairman, allow me to first commend you and your staff for the tremendous work you have done on Federal information security during your tenure as Chairman of this Subcommittee and your previous chairmanship on the Government Management, Information and Technology Subcommittee. It is a privilege working with you on this critical topic. I want to thank you for giving me the opportunity to speak on this issue in the context of today's hearing examining the lessons learned from the implementation of the Government Information Security Reform Act of 2000.

Unquestionably, the events of September 11th and the ensuing war on terrorism have produced a variety of responses throughout the world. Nowhere has the response been so fervent as here in our nation's Capital. From the creation of the new Office of Homeland Security to security-related legislation, there is an unprecedented awareness of the vulnerabilities we face.

This new awareness has naturally focused more attention on security matters, particularly with respect to information security. Yet this issue and the fact that Federal information systems continue to be woefully unprotected from both malevolent attacks and benign interruptions, have presented a grave concern to me for a number of years. I know that you and the other Members of the Subcommittee share that concern as well.

From our work in the Government Reform Committee, it is clear that the state of Federal information security suffers from a lack of coordinated, uniform management. Resolving this problem becomes even more imperative when you consider the many objectives we hope to achieve through the efficient and cost-effective use of information technology and the advancement of electronic government. These objectives include electronic procurement, telecommuting, a comprehensive information-sharing network, and improved provision of services to citizens and businesses.

The common element of these goals is the interconnectivity that they each require to facilitate communications between different public and private entities.

Poor information security management has persisted in both the public and private sectors long before IT became the ubiquitous engine driving governmental, business, and even home activities. After all, information security implicates both the physical and cyber environment.

A decade ago, technology stood as one of many factors important to the mission and performance objectives of the Federal Government. But no longer is technology "one of many"; instead, the Information Revolution and the ever-evolving technologies that support its collection, assimilation, and communication, have become integral to the functioning of our government.

As our reliance on technology and our desire for interconnectivity have grown over the past decade--intensifying with the advent of the Internet, our vulnerability to attacks has grown exponentially. The high degree of interdependence between information systems, both internally and externally, exposes the Federal government's

computer networks to benign and destructive disruptions. This fact is tremendously important to understanding how we devise a comprehensive and yet flexible strategy for coordinating, implementing and maintaining Federal information security practices throughout the Federal Government as the threat of electronic terrorism increases.

Yet Federal information security management continues to falter. Despite consistent evaluations since 1997 showing that Federal information security is a government-wide high-risk issue, GAO continues to find "pervasive and continuing weaknesses." And of course, as this Subcommittee found last November, 16 of the 24 federal agencies evaluated in 2001 each received a disappointing grade of "F", with only one agency receiving a grade higher than a C+.

Of course, while these grades are disappointing, they reflect the difficulty of implementing effective security management without sufficient commitment and guidance from an accountable entity within each agency, and for the Federal government as a whole.

In July 2000, I introduced legislation that would have created, among other things, a new Federal Chief Information Officer (CIO) in the Executive Office of the President. One of the primary components of that bill expanded upon the then yet-to-be-enacted Government Information Security Reform Act (GISRA), introduced by Senators Fred Thompson and Joe Lieberman.

My legislation, entitled the Federal Information Policy Act or "FIPA," reflected my firm belief that there needs to be an Executive Branch office that holds both the prestige and the accountability for strategically modernizing our stovepipe IT structure.

At the same time, that office must have the authority to prioritize cross-jurisdictional e-government initiatives, and networked information and telecommunications networks, in order to achieve efficiencies and secure Federal information systems.

With the establishment of a new office of Associate Director of IT and Electronic Government within the Office of Management and Budget (OMB), I have opted to withhold the reintroduction of Federal CIO legislation until I have had an opportunity to evaluate the progress that OMB has been able to achieve in carrying out the Administration's Enterprise Information Management and Integration initiative.

That said, my concerns regarding the pervasive and persistent weaknesses in Federal information security management, infrastructure, and accountability remain strong. These are concerns that I know you also share, Mr. Chairman. And I applaud your Subcommittee's steady work in bringing to the forefront, the critical need for immediate and focused attention on this issue.

Yet I would add that to the extent that increased security concerns rely on the ability of the public and private sectors to share information securely, it is even more critical that the Federal government put its own house in order with respect to the security of its own Federal information and telecommunications systems. It is for this reason that I have just introduced legislation similar to the information security provisions in FIPA, and I am very pleased that you have agreed to co-sponsor this measure with me, Mr. Chairman.

The overall purpose of these efforts is to strengthen the information security management infrastructure of the Federal government. The bill, entitled the Federal

Information Security Management Act or "FISMA," undertakes this objective by building on the foundation laid out by GISRA (pronounced "giz-ruh"). As you know, GISRA requires every Federal agency to develop and implement security policies that include risk assessment, risk-based policies, security awareness training, and periodic reviews.

With GISRA set to expire on November 29, 2002, the Federal Information Security Management Act permanently reauthorizes this legislation and implements additional measures designed to enable the Federal government to become a reliable public partner for protecting America's information highways. In general, FISMA streamlines GISRA's provisions and requires that agencies utilize information security best practices that will ensure the integrity, confidentiality, and availability of Federal information systems.

Moreover, this bill seeks to strengthen the role played by the National Institute of Standards and Technology (NIST) in developing and maintaining standards and guidelines for minimum information security controls. Agencies would be required to identify the risk levels associated with their systems and implement the appropriate level of protections accordingly. This latter objective is especially important in light of the interconnectivity of information systems. We need to implement a framework that ensures that when systems interconnect with each other, there is a uniform management infrastructure and universal benchmark for measuring the risks and vulnerabilities of Federal information systems.

We cannot afford to delay enactment of this legislation. At a time when uncertainty threatens confidence in our nation's preparedness, the Federal government

must make information security a priority. I am heartened by the President's bold commitment to tying the budget process to individual agency performance, and to using information security as one measurement of that performance. However, information security cannot go the way of any other "issue du jour." It is a constant management requirement that requires eternal vigilance, and the ranking of its importance to Federal operations cannot fluctuate from one Administration to the next.

It is my hope that we take this opportunity, in the context of extending GISRA, to signal Congress' deep concerns that information security is not being taken seriously by *every* agency and department. We must demand that in our networked era, where technology is the driver, every Federal information system must be managed in a way that minimizes both the risk that a breach or disruption will occur and the harm that would result should such a disruption take place.

We will learn a lot today as we determine the impact that GISRA has had on the information security practices throughout the Federal government. I very much look forward to working with you, Mr. Chairman, the Members of this Subcommittee, and other concerned Members of the House and Senate as we move forward on strengthening GISRA and improving our government's overall information security management.

Mr. HORN. I thank you for all the work you have done. Could you translate those two things, like "FISMA", was it, or something?

Mr. DAVIS. Right, it's the Federal Information Security Management Act. Of course, GISRA was the previous act.

Mr. HORN. Now is it true that Mr. Richard Clark is really fulfilling the office that you and some of our friends in the Senate wanted to do?

Mr. DAVIS. Part of it. I think that is as close as we can come to it, yes, sir.

Mr. HORN. Yes. Well, my understanding is that he is a pretty tough-minded person.

Mr. DAVIS. He is a tough-minded guy.

Mr. HORN. So that is what we want.

Mr. DAVIS. Exactly.

Mr. HORN. OK. So, in a sense, part of that which everybody has wanted is now underway. So we just have to wait to see what OMB and he do to get the thing done.

Mr. DAVIS. Mr. Chairman, the question always is you have a tough-minded person, but how much authority do they actually have, when push comes to shove? When they get on the phone, who are they calling from, how seriously are they taken at the other end of the line? That is what really remains to be seen.

Mr. HORN. Yes, well, you are certainly right on that. If the President backs him up, the Cabinet Secretaries I am sure will listen, and if it becomes part of a Cabinet agenda, that will help on this.

Mr. DAVIS. Mr. Chairman, as you know, we went through this with the Y2K issues——

Mr. HORN. Right.

Mr. DAVIS. [continuing]. Where they went through two or three czars.

Mr. HORN. Right.

Mr. DAVIS. Most of them having two or three other jobs and not having the clout until the administration finally brought in the appropriate person who had the clout and put it together at the end.

Mr. HORN. And had the ear of the President.

Mr. DAVIS. Yes, had the ear of the President.

Mr. HORN. Knew him before he was here.

Mr. DAVIS. Exactly, and, more importantly, when they called, the people on the other end of the phone knew that he was speaking for the President.

Mr. HORN. Yes.

Mr. DAVIS. And John Koskinen turned that around.

Mr. HORN. Right. Well, thank you very much——

Mr. DAVIS. Thank you.

Mr. HORN [continuing]. For your presentation. If you would like to stay with us, we are delighted to have you, if you wish.

Mr. DAVIS. I will stay for a few minutes. Thank you, Mr. Chairman.

Mr. HORN. OK. We will now swear in panel two, and that is Robert F. Dacey, Director, Information Security, U.S. General Accounting Office; Mark A. Forman, Associate Director, Office of Information Technology and E-Government, Office of Management and Budget; the Honorable Arden L. Bement, Jr., Ph.D., Director, National Institute of Standards and Technology; the Honorable Ro-

berta L. Gross, Former Inspector General, National Aeronautics and Space Administration; Robert G. Gorrie, Deputy Staff Director, Defense-wide Information Assurance Program Office, Assistant Secretary of Defense for Command, Control, Communications and Intelligence, and our last presenter on this panel will be Karen S. Evans, Chief Information Officer, Department of Energy.

As you know, since this is an investigating subcommittee, you raise your right hands to accept the oath.

[Witnesses sworn.]

Mr. HORN. The clerk will note that all six witnesses affirmed.

Please be seated. We will start with Mr. Dacey, the Director of Information Security, U.S. General Accounting Office, which is Congress' right arm in terms of getting things done. GAO is presided over by the Comptroller General of the United States. We have a first-rate person in that role right now in General Walker. So we are always glad to hear what the General Accounting Office has to say on these areas.

STATEMENTS OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY, U.S. GENERAL ACCOUNTING OFFICE; MARK A. FORMAN, ASSOCIATE DIRECTOR, OFFICE OF INFORMATION TECHNOLOGY AND E-GOVERNMENT, OFFICE OF MANAGEMENT AND BUDGET; ARDEN L. BEMENT, JR., DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; ROBERTA L. GROSS, FORMER INSPECTOR GENERAL, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION; ROBERT G. GORRIE, DEPUTY STAFF DIRECTOR, DEFENSE-WIDE INFORMATION ASSURANCE PROGRAM OFFICE, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE; AND KAREN S. EVANS, CHIEF INFORMATION OFFICER, DEPARTMENT OF ENERGY

Mr. DACEY. Mr. Chairman and members of the subcommittee, I am pleased to be here today to discuss the Federal Government's first-year implementation of government information security reform provisions. As you requested, I will briefly summarize our written statement.

Federal agencies rely extensively on computerized systems and electronic data to support their missions and critical operations. Concerned with reports that continuing pervasive computer security weaknesses place Federal operations at significant risk of disruption, tampering, fraud, and inappropriate disclosures of sensitive information, the Congress enacted the reform provisions to reduce these risks and provide for more effective oversight of Federal information security.

Mr. Chairman, as you know, we have been conducting a review of the implementation of the reform provisions for you and the Ranking Member. Today I will provide a preliminary result of our review.

The initial implementation of reform provisions is a significant step in improving Federal agencies' information security programs and addressing their information security weaknesses. The legislation consolidates information security requirements into an overall management framework covering all agency systems. It adds new

statutory evaluation and reporting requirements and OMB and congressional oversight.

Agencies have noted a number of benefits of this first-year implementation, including increased management attention to, and accountability for, information security. In addition, the legislation has resulted in other important actions by the administration, such as plans to integrate information security into the President's management agenda scorecard. Also, agencies have taken steps to redesign and strengthen their information security.

OMB oversight, which included formal guidance, review and analysis of agency-reported material, agency discussion and feedback, and monitoring of corrective actions, has helped agency implementation and reporting efforts. Although agencies generally considered OMB guidance beneficial, the initial implementation of reform provisions highlighted the need for further guidance in several areas.

Last month OMB released its first required annual report to the Congress on the results of agency implementation efforts. As a result, in this report OMB commended agency improvement efforts, but noted that many agencies have significant deficiencies in every important area of security. OMB also identified a number of common agency security weaknesses, including lack of senior management attention, inadequate accountability for job and program performance, and a limited capability to detect vulnerabilities or intrusions.

We agree that OMB's report to the Congress and the agency reports are a valuable baseline and believe that OMB's report provides a useful overview of OMB and agency efforts to comply with the reform provisions. I would like to personally commend the OMB staff for their efforts in this endeavor.

Nonetheless, certain additional information, including the adequacy of agency corrective action plans and the results of audits of evaluations for national security systems, is needed by Congress to fully assess and oversee these efforts and deliberate over agency budgets.

OMB has not authorized agencies to release some agency material, such as agency corrective action plans, to the Congress or GAO. We plan to continue working with OMB in an effort to find workable solutions to obtain this information.

Agency reports to OMB show that agencies have not established information security programs consistent with the provisions of the legislation and that significant weaknesses exist. Although agency actions are now underway to strengthen information security and implement these requirements, significant improvements will require sustained management attention, as well as OMB and congressional oversight.

The IG's independent evaluations of agency implementation efforts also played a key role in the implementation process. The IG's first-year efforts were largely based on existing or ongoing audit work that had been planned to evaluate agency information security, which in a number of instances consisted primarily of audits of financial systems.

While their future efforts should expand to include more systems, the IG's first-year evaluations helped to identify significant weak-

nesses in all 24 agencies, weaknesses that were not always identified by agencies in their reports.

Given the recent events and reports that critical operations and assets are highly vulnerable to cyber-attack, it is essential that Congress have adequate information to oversee and fund the Federal information security efforts, and that these efforts be guided by a comprehensive strategy for improvement. In addition, there are a number of important steps that the administration and the agencies should take, including delineating the roles and responsibilities of the numerous entities involved in Federal information security and the related aspects of critical infrastructure protection, providing more specific guidance to agencies on the security controls they need to implement, and allocating sufficient agency resources for information security.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the subcommittee may have.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m. EST
Wednesday,
March 6, 2002

INFORMATION SECURITY

Additional Actions Needed to Fully Implement Reform Legislation

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-02-470T

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss efforts by the federal government to implement provisions for Government Information Security Reform (the reform provisions) that were enacted as part of the National Defense Authorization Act for Fiscal Year 2001.[1] Federal agencies rely extensively on computerized systems and electronic data to support their missions and critical operations. Concerned with reports that continuing, pervasive security weaknesses place federal operations at significant risk of disruption, tampering, fraud, and inappropriate disclosures of sensitive information, the Congress enacted the reform provisions to reduce these risks and provide more effective oversight of federal information security.

In my testimony today, I will first describe some of the improvement efforts and benefits that have resulted from this first year implementation of the reform provisions. Next, I will describe the results of our evaluation of actions by the Office of Management and Budget (OMB), 24 of the largest federal agencies, and these agencies' inspectors general (IGs) to implement the reform provisions. As part of this discussion, I will also summarize the overall results of these actions and, in particular, note any challenges to effective implementation or oversight of the reform provisions.

Mr. Chairman, as you know we have been conducting a review of the implementation of the reform provisions for you and the ranking member. Today, I will provide the preliminary results of our review. In conducting this review, we interviewed officials and staff in the offices of the chief information officer (CIO) and the IGs for 24 of the largest federal agencies. We reviewed OMB guidance and instructions related to the reform provisions and, for the 24 agencies, analyzed summaries of their management reviews of their information security programs. Further, we analyzed the IGs' summaries and reports on their independent evaluations of the agencies' information security programs. We also analyzed OMB's fiscal year 2001 report to the Congress on the results of these reviews and evaluations.[2]

We performed this review from May 2001 to March 2002 in accordance with generally accepted government auditing standards.

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

Background

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. However, this widespread interconnectivity also poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support, such as telecommunications, power distribution, public health, national defense (including the military's warfighting capability), law enforcement, government, and emergency services. Likewise, the speed and accessibility that create the enormous benefits of the computer age, 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.

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, the likelihood increases that information attacks will threaten vital national interests. Further, the events of September 11, 2001, underscored the need to protect America's cyberspace against potentially disastrous cyber attacks—attacks that could also be coordinated to coincide with physical terrorist attacks to maximize the impact of both.

Since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.[3] 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. In addition, in both 1998 and 2000, we analyzed audit results for 24 of the largest federal agencies and found that all 24 had significant information security weaknesses.[4] As a result of these analyses, we have

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

[4]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; *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*. GAO/AIMD-00-295. Washington, D.C.: September 6, 2000.

identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[5]

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 or 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.

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 Government Information Security Reform provisions as part of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001. These provisions became effective November 29, 2000, and are in effect for 2 years after this date. The reform provisions supplement 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 are consistent with existing information

[5]U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*. GAO/HR-97-9. Washington, D.C.: February 1, 1997; *High-Risk Series: An Update*. GAO/HR-99-1. Washington, D.C.: January 1999; *High Risk Series: An Update*. GAO-01-263. Washington, D.C.: January 2001.

security guidance issued by OMB[6] and the National Institute of Standards and Technology (NIST),[7] as well as audit and best practice guidance issued by GAO.[8] Most importantly, however, the provisions consolidate these separate requirements and guidance into an overall framework for managing information security and establish new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight.

The legislation assigned specific responsibilities to OMB, agency heads and CIOs, and the IGs. OMB is responsible for establishing and overseeing policies, standards and guidelines for information security. This includes the authority to approve agency information security programs, but delegates OMB's responsibilities with regard to national security systems to national security agencies. OMB is also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs. The reform provisions do not specify a date for this report.

Each agency, including national security agencies, is 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 is 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;

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

[7]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.

[8]U.S. General Accounting Office, *Federal Information System Controls Manual, Volume 1—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.

- 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, the reform provisions require 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 are to be performed by the agency IG or an independent evaluator, and the results of these evaluations are to be reported to OMB. For the evaluation of national security systems, special provisions include designation of evaluators by national security agencies, restricted reporting of evaluation results, and an audit of the independent evaluation performed by the IG or an independent evaluator. For national security systems, only the results of each audit of an evaluation are to be reported to OMB.

Finally, the reform provisions also assign additional responsibilities for information security policies, standards, guidance, training, and other functions to other agencies. These agencies are NIST, the Department of Defense, the Intelligence Community, the Attorney General, the General Services Administration (GSA), and the Office of Personnel Management.

With oversight jurisdiction for information security, this subcommittee has continued to hold hearings on the status of information security in the federal government. Most recently, on November 9, 2001, the subcommittee issued information security "grades" based primarily on the agencies' reform provision review summaries and IG evaluations that were submitted to OMB. The overall grade for the federal government was an "F."

Results in Brief

The initial implementation of the reform provisions is a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. The legislation consolidates information security requirements into an overall management framework covering all agency systems, adds new statutory evaluation and reporting requirements that facilitate implementation of these requirements, and strengthens OMB and congressional oversight. Agencies have noted benefits of this first-year implementation, including increased management attention to and accountability for information security. In addition, the legislation has resulted in other important actions by the administration to address information security,

such as plans to integrate information security into the President's Management Agenda Scorecard.

OMB is using a combination of formal guidance, review and analysis of agency-reported material, agency discussion and feedback, and monitoring of corrective actions to oversee and coordinate agency compliance with the requirements of the reform provisions. This oversight contributed to agency implementation and reporting efforts. However, further guidance is needed to ensure that agencies effectively implement these requirements and can show their progress in these efforts. For example, OMB's reporting guidance required agencies to identify performance measures and actual performance for implementing key security requirements like assessing risk and testing and evaluating security controls, but did not provide guidance on establishing such measures. Thus, agencies were left to independently develop their own measures.

In February 2002, OMB released its required annual report to the Congress on the results of agency evaluations. In this report, OMB commended agencies' improvement efforts, but noted that many agencies have significant deficiencies in every important area of security. OMB also identified a number of common agency security weaknesses, including a lack of senior management attention, inadequate accountability for job and program performance, and a limited capability to detect vulnerabilities or intrusions. Although OMB's report provides an overview of agencies' progress and status, the report does not specifically address several requirements of the reform provisions, including the adequacy of agencies' corrective action plans and the results of evaluations for national security systems. Further, OMB considers some agency material, such as agencies' corrective action plans, to contain predecisional budget information and will not authorize agencies to release this material to the Congress or GAO. The lack of such important information limits congressional oversight of agencies' implementation, compliance, and corrective action efforts, as well as for budget deliberations. We plan to continue working with OMB in an effort to find workable solutions to obtain the information needed for congressional oversight.

In response to the reform provisions, agencies reviewed their information security programs, reported the results of these reviews to OMB, and developed plans to correct identified weaknesses. However, their reviews showed that agencies have not established information security programs consistent with the legislative requirements and that significant weaknesses exist. Although agency actions are now underway to strengthen information security and implement these requirements, significant improvement will require sustained management attention and OMB and congressional oversight.

The IGs also played a critical role in this process by independently evaluating the agencies' implementation efforts and verifying the effectiveness of security controls. However, the IGs' first-year efforts to evaluate agency information security were largely based on existing or ongoing audit work to evaluate agency information security, which in a number of instances, consisted primarily of audits of financial systems. While their future evaluations should expand to include more systems supporting nonfinancial operations, the IGs' first-year evaluations helped identify significant weaknesses in all 24 of the largest federal agencies—weaknesses that were not always identified by the agencies in their reports.

Given recent events and reports that critical operations and assets are highly vulnerable to cyber attack, it is essential that the Congress have adequate information to oversee and fund federal information security efforts and that these efforts be guided by a comprehensive strategy for improvement. OMB should, therefore, consider providing the Congress with additional information that the agencies submitted under the reform provisions, such as appropriate information from the agencies' corrective action plans. In addition, 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, including delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection, providing more specific guidance to agencies on the security controls that they need to implement, and allocating sufficient agency resources for information security.

Reform Provisions Increase Management Attention to Information Security

The initial implementation of the reform provisions is a significant step in addressing the serious, pervasive weaknesses in the federal government's information security. The legislation consolidates existing security requirements and adds new statutory requirements designed to improve information security, such as independent evaluations and annual reporting. In addition, implementation of the provisions has improved agency focus on information security and resulted in important actions by the administration.

Although security requirements existed in law and policy before this law, the reform provisions put into law several important additional requirements. First, the provisions require a risk-based security management program covering all operations and assets of the agency and those provided or managed for the agency by others to be implemented by agency program managers and CIOs. Instituting such an approach is important since many agencies had not effectively evaluated their information security risks and implemented appropriate controls. Our studies of public and private best practices have shown that effective security

program management requires implementing a process that provides for a cycle of risk management activities as now included in the reform provisions.[9] Moreover, other efforts to improve agency information security will not be fully effective and lasting unless they are supported by a strong agencywide security management program.

Second, the reform provisions require an annual independent evaluation of each agency's information security program. Individually, as well as collectively, these evaluations can provide much needed information for improved oversight by OMB and the Congress. Our years of auditing agency security programs have shown that independent tests and evaluations are essential to verifying the effectiveness of computer-based controls. Audits can also evaluate agency implementation of management initiatives, thus promoting management accountability. Annual independent evaluations of agency information security programs will help drive reform because they will spotlight both the obstacles and progress toward improving information security and provide a means of measuring progress, much like the financial statement audits required by the Government Management Reform Act of 1994. Further, independent reviews proved to be an important mechanism for monitoring progress and uncovering problems that needed attention in the federal government's efforts to meet the Year 2000 computing challenge.

Third, the reform provisions take a governmentwide approach to information security by accommodating a wide range of information security needs and applying requirements to all agencies, including those engaged in national security. This is important because the information security needs of civilian agency operations and those of national security operations have converged in recent years. In the past, when sensitive information was more likely to be maintained on paper or in stand-alone computers, the main concern was data confidentiality, especially as it pertained to classified national security data. Now, virtually all agencies rely on interconnected computers to maintain information and carry out operations that are essential to their missions. While the confidentiality needs of these data vary, all agencies must be concerned about the integrity and the availability of their systems and data. It is important for all agencies to understand these various types of risks and take appropriate steps to manage them.

[9]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations.* GAO/AIMD-98-68. Washington, D.C.: May 1998; *Information Security Risk Management: Practices of Leading Organizations.* GAO/AIMD-00-33. Washington, D.C.: November 1999.

Fourth, the annual reporting requirements provide a means for both OMB and the Congress to oversee the effectiveness of agency and government-wide information security, measure progress in improving information security, and consider information security in budget deliberations. In addition to management reviews, annual IG reporting of the independent evaluation results to OMB and OMB's reporting of these results to the Congress provide the Congress with an objective assessment of agencies' information security programs on which to base its oversight and budgeting activities. This reporting also facilitates a process to help ensure consistent identification of information security weaknesses by both the IG and agency management.

In addition to new statutory provisions, first-year implementation of the reform provisions has yielded significant benefits in terms of agency focus on information security. A number of agencies stated that as a result of implementing the reform provisions, they are taking significant steps to improve their information security programs. For example, one agency stated that the legislation provided it with the opportunity to identify some systemic program-level weaknesses for which it plans to undertake separate initiatives targeted specifically to improve the weaknesses. Other benefits agencies observed included (1) higher visibility of information security within the agencies, (2) increased awareness of information security requirements among department personnel, (3) recognition that program managers are to be held accountable for the security of their operations, (4) greater agency consideration of security throughout the system life cycle, and (5) justification for additional resources and funding needed to improve security. Agency IGs also viewed the reform provisions as a positive step towards improving information security particularly by increasing agency management's focus on this issue.

Implementation of the reform provisions has also resulted in important actions by the administration, which if properly implemented, should continue to improve information security in the federal government. For example, OMB has issued guidance that information technology investments will not be funded unless security is incorporated into and funded as part of each investment, and NIST has established a Computer Security Expert Assist Team to review agencies' computer security management. The administration also has plans to

- direct all large agencies to undertake a review to identify and prioritize critical assets within the agencies and their interrelationships with other agencies and the private sector, as well as a cross-government review to ensure that all critical government processes and assets have been identified;
- integrate security into the President's Management Agenda Scorecard;
- develop workable measures of performance;

- develop e-training on mandatory topics, including security; and
- explore methods to disseminate vulnerability patches to agencies more effectively.

OMB has Guided and Overseen Agency Implementation

On January 16, 2001, OMB issued guidance to the agencies on implementing the reform provisions that summarized OMB, agency, and IG responsibilities, and provided answers to other specific implementation questions.[10] OMB followed up the implementation guidance with agency reporting instructions first issued in draft form in April and then in final form on June 22.[11] These final reporting instructions directed agencies to transmit copies of the annual agency program reviews, IG independent evaluations, and for national security systems, audits of the independent evaluations to OMB 3 months later, on September 10, 2001—the same time they were to submit their fiscal year 2003 budget materials. In addition to the program reviews and evaluations, agency heads were also to provide a brief executive summary developed by the agency CIO, agency program officials, and the IG based on the results of their work.

The OMB reporting instructions also listed specific topics that the agencies were to address, many of which were referenced back to corresponding requirements of the reform provisions. These topics, which became the basic structure of the executive summaries submitted by the agencies and most IGs, basically asked that agencies identify, describe, or report:

1. Total security funding as found in the agency's fiscal year 2001 budget request, fiscal year 2001 budget enacted, and the fiscal year 2002 budget request.
2. The total number of programs included in the program reviews or independent evaluations.
3. The methods used to conduct the program reviews and independent evaluations.
4. Any material weakness in policies, procedures, or practices as identified and required to be reported under existing law.

[10]"Guidance on Implementing the Government Information Security Reform Act," Memorandum for the Heads of Executive Departments and Agencies, Jack Lew, Director, M-01-08, January 16, 2001.

[11]"Reporting Instructions for the Government Information Security Reform Act," Memorandum for the Heads of Executive Departments and Agencies, Mitchell E. Daniels, Jr., Director, M-01-24, June 22, 2001.

5. The specific measures and actual performance for performance measures that agencies used to ensure that for operations and assets under their control, agency program officials have assessed the risk, determined the appropriate level of security, maintained an up-to-date security plan (that is practiced throughout the life cycle) for each supporting system, and tested and evaluated security controls and techniques.
6. The specific measures and actual performance for performance measures that agencies used to ensure that the agency CIO (a) adequately maintains an agencywide security program, (b) ensures the effective implementation of the program and evaluates the performance of major agency components, and (c) ensures that agency employees with significant security responsibilities are trained.
7. How the agency ensures that employees are sufficiently trained in their security responsibilities to include identifying the total number of agency employees, the types of security training available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training.
8. The agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities.
9. How the agency integrates security into its capital planning and investment control process.
10. The specific methodology and how it has been implemented by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems.
11. The specific measures and actual performance for performance measures that the head of the agency used to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system.
12. How the agency has integrated its information and information technology security program with its critical infrastructure protection responsibilities and other security programs.
13. The specific methods used by the agency to ensure that contractor-provided services or services provided by another agency are adequately secure and meet the requirements of the reform provisions and other governmentwide and agency policy and guidance.

The reporting instructions also included an additional requirement for each agency head to work with the CIO and program officials to provide a strategy to correct security weaknesses identified through the annual program reviews, independent evaluations, other reviews or audits performed throughout the reporting period, as well as any uncompleted actions identified before the reporting period. Due to OMB by October 31, 2001, this information was to

include a "plan of action and milestones" (corrective action plan) that listed the weaknesses; showed required resources, milestones, and completion dates; and described how the agency planned to address these weaknesses. In response to agency requests, on October 17, OMB provided more detailed guidance for preparing and submitting these corrective action plans, which also provided a sample spreadsheet-type format.[12] The guidance also established a requirement for agencies to submit quarterly status updates to OMB with the first update due on January 31, 2002.

OMB's guidance addressed many key information security requirements in the reform provisions, and agencies generally considered the guidance beneficial in summarizing their efforts to implement these requirements. However, with their reports due to OMB on September 10, several agencies questioned the timeliness of the final reporting guidance being issued less than 3 months before this deadline.

Several agencies also noted the need for additional clarification or guidance in some areas. For example, our analysis of agency executive summaries showed that many agencies did not have or were still in the process of developing and implementing security performance measures. Some thought additional guidance on appropriate measures would be helpful and more cost-effective than having each agency develop its own. Other agencies had questions regarding what should be identified and reported as security costs in their budgets.

In addition to providing guidance, OMB also reviewed the results of agencies' program reviews and independent evaluations and consulted with officials in the agencies to clarify information and provide feedback. OMB also sent letters to the agency heads that provided the results of its assessment of the agencies' submissions for the reform provisions and either conditionally approved or disapproved their information security programs. Further, OMB states in its report to the Congress that it will discuss security corrective action plans with each agency and monitor their progress through the quarterly updates that agencies are to submit. These actions should contribute to OMB's effective oversight and help focus agencies' improvement efforts. However, OMB's sustained commitment to both implementing the reform provisions and overseeing agencies will be critical to ensuring that agencies substantially improve their information security programs.

[12]"Guidance for Preparing and Submitting Security Plans of Action and Milestones," Memorandum for the Heads of Executive Departments and Agencies, Mitchell E. Daniels, Jr., Director, M-02-01, October 17, 2001.

Key Information Needed for Congressional Oversight

On February 13, 2002, OMB released its required report to the Congress to summarize the agency independent evaluations. Based on reports from over 50 departments and agencies and focusing on management issues as opposed to technical or operational issues, this report (1) provides an overview of OMB and agencies' implementation efforts; (2) summarizes the overall results of OMB's analyses; (3) includes individual agency summaries for the 24 of the largest federal departments and agencies; and (4) includes brief summary remarks for small and independent agencies. OMB notes that although examples of good security exist in many agencies, and others are working very hard to improve their performance, many agencies have significant deficiencies in every important area of security. In particular, the report highlights six common security weaknesses:

- a lack of senior management attention to information security;
- inadequate accountability for job and program performance related to information technology security;
- limited security training for general users, information technology professionals, and security professionals;
- inadequate integration of security into the capital planning and investment control process;
- poor security for contractor-provided services; and
- limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

Overall, OMB views its report to the Congress and the agency reports to be a valuable baseline to record agency security performance—a baseline captured with more detailed information than previously available that will be useful for oversight by agencies, IGs, OMB, GAO, and the Congress.

While we agree and believe that OMB's report provides a useful overview of OMB and agency efforts to comply with the reform provisions, certain additional information not included in the report is necessary to fully assess and oversee these efforts. The lack of such important information limits congressional oversight for agencies' implementation, compliance, and corrective action efforts, as well as for budget deliberations. Specifically, OMB's report does not address the following:

- The report does not provide any specific analysis or opinion on the adequacy of agency corrective action plans that were submitted to OMB in late October of

last year and included the planned timeframes for correcting security weaknesses. Agency corrective actions are underway, and while OMB indicated that performance in implementing these plans would be reflected in next year's report, information about the adequacy and reasonableness of such plans and the related costs to implement them, as well as an independent review, are important elements in congressional oversight and budget deliberations. In August 2001, OMB sent a memorandum to agency heads stating that it considered all reform provision material prepared by the CIOs for OMB to be predecisional and not releasable the public, the Congress, or GAO. In September, this subcommittee interceded to request that OMB provide the agency executive summaries to you, and OMB complied with this request. Recently, OMB agreed that it would also authorize the agencies to release the more detailed material to us after the agencies redact any sensitive information. However, OMB has continued to restrict access to agency corrective action plans. We plan to continue working with OMB in an effort to find workable solutions to obtain the information needed for congressional oversight. With the president requesting $4.2 billion for information security funding for fiscal year 2003, congressional oversight of future spending on information security will be important to 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. Accordingly, OMB should consider authorizing agencies to release appropriate information from the corrective action plans to the Congress. Also, future IG evaluations need to provide an independent assessment of agency corrective action plans.

- The report discusses review results for national security systems in several individual agency summaries, but does not summarize the overall results of the audits of the evaluations for these systems, which the reform provisions specifically require agencies to provide OMB and OMB to report subsequently to the Congress. This lack of an overall summary was compounded by limited access to information regarding national security systems by the director of Central Intelligence (DCI). The reform provisions assign the DCI and the secretary of defense specific responsibilities for national security systems, including developing and ensuring that information security policies, standards, and guidelines are implemented and designating the entity to perform the independent evaluation of the information security program and practices for these systems. As part of our review, DCI staff declined to meet with us to discuss the guidance and assistance they provided agencies to implement the reform provisions for national security systems. The DCI stated that our inquiry related to matters of intelligence oversight, which are under the purview of the congressional entities charged with overseeing the intelligence community. While evaluations and audits of evaluations for systems under the control of the DCI are available only to the appropriate oversight committees of Congress,

OMB is required to report to the Congress on the results of audits of evaluations that the agencies submit to OMB for other national security systems. We acknowledge the sensitivity of this information. Nevertheless, because the review, evaluation, and reporting requirements of the reform provisions apply to national security systems, as well as non-national-security systems, this lack of high-level summary information on implementation of the provisions and the security for national security systems limits the ability of the Congress to provide governmentwide oversight for information security. Consequently, we believe that OMB should consider providing appropriate information on national security systems to the Congress.

- OMB's report identifies lack of top management attention as a common weakness. It also notes that agencies have not implemented all the requirements of the legislation, and that it either disapproved or only conditionally approved the information security programs of each of the 24 agencies. However, the report does not address the status or effectiveness of the agencies' efforts to implement specific requirements of an agencywide information security program such as conducting risk assessments and testing and evaluating controls. OMB addresses these requirements in its individual agency summaries, but does not provide any overall results. Our analyses showed that most agencies have not fully implemented requirements to assess risk and test and evaluate controls and that this represents systemic weaknesses in the federal government's information security. Such requirements are critical elements of an overall information security program, and the Congress should be fully informed on the status of agency efforts to implement and comply with them. To address this, in its future annual reports to the Congress, OMB should consider explicitly identifying the overall status of agency efforts to implement each of the requirements for agency information security programs.

Reform Provisions Spur Agency Actions and Highlight Continued Weaknesses

To implement the reform provisions, agencies conducted management assessments of their information security programs and systems and followed OMB guidance to report their results. The methodologies that the agencies used varied, but most indicated that they used NIST's *Security Self-Assessment Guide* to assist program officials in reviewing their programs.[13] Provided to help agencies perform self-assessments of their information security programs and to accompany the NIST-developed *Federal IT Security Assessment Framework*,[14] this guide 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. Most agencies considered this questionnaire to be a useful tool and several modified or tailored it for their use. In addition, several agencies used independent contractors to evaluate their systems, and in at least one case, an agency had its program assessed by the NIST Computer Security Expert Assist Team.[15]

In addition to these assessments of their information security programs, agencies also considered the results of audit work performed by their IGs, GAO, and others to help them identify information security weaknesses for reporting to OMB and identifying corrective actions. In particular, a number of agencies worked closely with the IGs to help ensure that they consistently identified weaknesses.

Most agencies structured their executive summaries according to the 13 topics that OMB's reporting instructions indicated they should address. However, these summaries did not always provide all requested data or provide context for determining the significance of their efforts. For example, they did not indicate the extent to which agency programs and systems, contractor-supported operations, or national security system programs were covered by their review.

[13]National Institute of Standards and Technology *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26, November 2001.

[14]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, November 28, 2000.

[15]NIST created the Computer Security Expert Assist Team (CSEAT) to improve federal critical infrastructure protection planning and implementation efforts by assisting governmental entities in improving the security of their information and cyber assets. The CSEAT review of an agency's computer security program is based on a combination of proven techniques and best practices and results in an action plan that provides a federal agency with a business-case-based roadmap to cost-effectively enhance the protection of their information system assets.

In general, our analyses of these summaries showed that although agencies are making progress in addressing information security, much remains to be done. None of the agencies had fully implemented the requirements of the reform provisions and all continue to have significant information security weaknesses. In particular, we identified the following key information security requirements of the reform provisions that were problematic for the 24 agencies reviewed.

Extent that Agencies Assess Risk is Unknown

The reform provisions require agencies to perform periodic threat-based risk assessments for systems and data. However, the agency and IG reports indicated that most agencies could not demonstrate that periodic risk assessments are being conducted. However, none of the 24 agencies had conducted risk assessments for all their systems, and 11, or 46 percent, had not established effective performance measures to show how well program officials met these requirements.

Risk assessments are an essential element of risk management and overall security program management and, as our best practice work has shown,[16] are an integral part of the management processes of leading organizations. 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 based on 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.

OMB reporting guidance addressed this requirement by asking agencies to describe performance measures used to ensure that agency program officials have assessed the risk to operations and assets under their control. In its report to the Congress, OMB identified measuring performance as a common weakness and covered risk assessments in its individual agency summaries. OMB did not, however, identify the pervasive lack of risk assessments as an overall weakness in federal information security.

Policies and Procedures Not Adequate

The reform provisions require agencies to establish information security policies and procedures that are commensurate with risk and that comprehensively address the other reform provisions. OMB's report refers to selected policies and

[16]GAO/AIMD-98-68, May 1998.

procedures, but does not address them comprehensively. Because risks are not adequately assessed, policies and procedures may be inadequate or excessive. Also, our audits have identified instances where agency policies and procedures did not comprehensively address all areas of security, were not sufficiently detailed, were outdated, or were inconsistent across the agency.

Security Training and Awareness Efforts Incomplete

The reform provisions require agencies to provide training on security responsibilities for information security personnel and on security awareness for agency personnel. Agency summaries showed that some agencies provided little or no training, and many could not show to what extent security training was provided. For example, 4 of the 24 agencies (17 percent) reported that they were still developing or implementing their security awareness and training program. Further, 10 of the 24 agencies (42 percent) did not report data to indicate the number of agency employees receiving security training, and 8 (33 percent) did not report the total costs of providing such training.

Our studies of best practices at leading organizations have shown that these organizations took steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed.[17] 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. In addition, 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.

In its report to the Congress, OMB identified security education and awareness as a common weakness and noted that OMB and federal agencies are now working through the new Critical Infrastructure Protection Board's education committee and the CIO Council's Workforce Committee to address this issue. Also, the CIO Council's Best Practices Committee is working with NIST through NIST's Federal Agency Security Practices Website to identify and disseminate best practices involving security training. Finally, OMB notes that one of the administration's electronic government initiatives is to establish and deliver electronic training.

[17]GAO/AIMD-98-68, May 1998.

Security Controls Not Adequately Tested and Evaluated

Under the reform provisions, one of the responsibilities of the agency head is to ensure that appropriate agency officials are responsible for periodically testing and evaluating the effectiveness of policies, procedures, controls, and techniques. Many of the 24 agencies we contacted said that they primarily relied on management self-assessments to review their programs or systems this first year and did not perform any control testing as part of these assessments. Several agencies indicated that control testing was part of their certification and accreditation processes, but also reported that many systems were not certified and accredited.[18]

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.

OMB's report to the Congress also did not specifically identify lack of control testing as a common weakness, but did address it as part of the individual agency summaries.

Remedial Actions May Not be Adequate

The reform provisions require that agencies develop a process for ensuring that remedial action is taken to address significant deficiencies. While we were unable to review the adequacy of corrective action plans submitted to OMB, our audits have identified instances in which items on other agency corrective action plans were not independently verified or considered with respect to other systems that might contain the same or similar weakness. We have also noted instances where agencies had no process to accumulate identified deficiencies across the agency. Given these prior findings, it is important that corrective action plans be carefully reviewed.

[18]Certification is a formal review and test of a system's security safeguards to determine whether or not they meet security needs and applicable requirements. Accreditation is the formal authorization for system operation and is usually supported by certification of the system's security safeguards, including its management, operational, and technical controls.

Incident-Handling and Information-Sharing Procedures Not Implemented

The reform provisions require agencies to implement procedures for detecting, reporting, and responding to security incidents. Of the 24 agencies we reviewed, 18 (75 percent) reported that they had documented incident handling procedures, but had not implemented these procedures agencywide. In addition, 5 agencies (22 percent) reported that their procedures did not cover reporting incidents to the Federal Computer Incident Response Center (FedCIRC)[19] or law enforcement.

Even strong controls may not block all intrusions and misuse, but 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.

In its report to the Congress, OMB identified "detecting, reporting, and sharing information on vulnerabilities" as a common agency weakness. It also noted that ongoing activity to address this issue includes FedCIRC's quarterly reporting to OMB on the federal government's status on security incidents and GSA's, under OMB and Critical Infrastructure Protection Board guidance, exploring of methods to disseminate vulnerability patches to all agencies more effectively.

Critical Assets Identified, But Not Ranked or Updated

The reform provisions require that each agencywide information security program ensure the integrity, confidentiality, and availability of systems and data supporting the agency's critical operations and assets. Of the 24 agencies covered

[19]GSA's FedCIRC provides 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.

by our review, 15 had not implemented an effective methodology such as Project Matrix reviews[20] to identify their critical assets, and 7 had not determined the priority for restoring these assets should a disruption in critical operations occur.

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 are 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.

OMB's report to the Congress does not specifically address the overall extent to which agencies identified and prioritized their critical assets, but does cover this topic in the individual agency summaries. Also, OMB indicates that it will direct all large agencies to undertake a Project Matrix review, and once these reviews are completed, it will identify cross-government activities and lines of business for Matrix reviews.

Agency Efforts to Ensure Security of Contractor-Provided Services are Limited

Under the reform provisions, agencies are required to develop and implement risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained either by the agency or for it by another agency or contractor. Laws and policies have included security requirements for years, but agency reports indicate that although most included security requirements in their service contracts, most not did they have a process to ensure the security of services provided by a contractor or another agency.

OMB reported this as a common weakness in its report to the Congress noting that activities to address this issue include (1) working under the guidance of an OMB-led security committee established under Executive Order 13231 to develop recommendations addressing security in contracts themselves,[21] and (2)

[20]The Department of Commerce's Critical Infrastructure Assurance Office established Project Matrix to provide a standard methodology for identifying all assets, nodes, networks, and associated infrastructure dependencies and interdependencies required for the federal government to fulfill its national security, economic stability, and critical public health and safety responsibilities to the American people.

[21]"Critical Infrastructure Protection in the Information Age," Executive Order 13121, October 16, 2001.

working with the CIO Council and the Procurement Executives Council to establish a training program that ensures appropriate security training for contractors.

Agencies May Not Identify All Significant Security Weaknesses

The reform provisions require agencies to examine the adequacy and effectiveness of information security policies, procedures, and practices, and to report any significant deficiency found as a material weakness under the applicable criteria for other laws, including the Clinger-Cohen Act of 1996, the Chief Financial Officers Act of 1990, and the Federal Managers Financial Integrity Act. Although most agencies reported security weaknesses, several did not identify all weaknesses highlighted in the IGs' independent evaluations. For example, two IGs identified security weaknesses, but the CIOs did not identify any weaknesses in their executive summaries because they were not considered material weaknesses.

As I will illustrate next in my discussion of the results of the IGs' independent evaluations, our latest analyses of audit results for the 24 agencies confirmed that all agencies had significant information security weaknesses. Such weaknesses should be identified and reported in the CIOs' reports consistent with the IGs' independent evaluations to ensure that they are appropriately considered in implementing corrective actions.

IG Role Critical to Agency Implementation and Reporting

The reform provisions assign the agency IGs a critical role in the overall implementation and reporting process. Each agency is to have the IG or other independent evaluator annually evaluate its information security program and practices. This evaluation is to include testing of the effectiveness of information security control techniques for an appropriate subset of the agency's information systems and an assessment of the agency's compliance with the legislation; it may also use existing audits, evaluations, or reports relating to the programs or practices of the agency. For national security systems, the secretary of defense or DCI designates who is to perform the independent evaluation, but the IG is to perform an audit of the evaluation. The results of each evaluation of non-national-security systems and of the audit of the evaluation for national security systems are to be reported to OMB.

Individually, as well as collectively, the annual independent evaluations provide much needed information for improved oversight by OMB and the Congress. Our years of auditing agency security programs have shown that independent tests

and evaluations are essential to verifying the effectiveness of computer-based controls. The independent evaluations can also evaluate agency implementation of management initiatives, thus promoting management accountability. Moreover, an annual independent evaluation of agency information security programs will help drive reform because it will spotlight both the obstacles and progress toward improving information security.

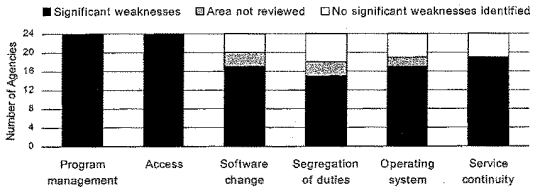
For this first-year evaluation and reporting for the reform provisions, IGs primarily performed the independent evaluations and largely relied on existing or ongoing work to evaluate agency security, most of which was related to their financial statement audits. With the reform provisions applicable to essentially all major systems including national security systems, as well as other types of risk beyond financial statements, future IG independent evaluation efforts will have to expand their coverage to include such additional risks and more nonfinancial systems, particularly for agencies with significant nonfinancial operations such as the departments of Defense and Justice. An important step toward ensuring information security is to fully understand the weaknesses that exist, and as the body of audit evidence expands, it is probable that additional significant deficiencies will be identified. However, this expanded coverage will also place a significant new burden on existing audit capabilities, which will require ensuring that agency IGs have sufficient resources to either perform or contract for the needed work.

While no format was prescribed for their evaluation reports, most IGs prepared an executive summary and report which, at OMB's request, addressed the specific topics identified in OMB's reporting guidance. This made comparison of agency and IG results easier, and better highlighted discrepancies. For the most part and particularly where the CIO and IG offices coordinated their responses, the IG evaluations were consistent with what the agencies reported. However, there were areas where the CIO reviews and the IG evaluations did not agree in their assessments of the agencies' progress in implementing the requirements of the reform provisions. Reasons cited include different interpretations of the law or guidance and the time lag between the audit reports the IG used for its evaluation and the possibly more current status reflected in the CIO's review.

However, perhaps the most important area of the IGs' independent evaluations is their identification of the agency's significant information security weaknesses for which they identified essentially known weaknesses including, but not limited to, those considered material weaknesses under reporting requirements for other legislation. To summarize these identified weaknesses, we also analyzed the results of IG and GAO audit reports published from July 2000 through September 2001, including the results of the IGs' independent evaluations. These

analyses showed significant information security weaknesses in all major areas of the agencies' 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. Figure 1 illustrates the distribution of weaknesses across the 24 agencies for the following six general control areas: (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 1: Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued July 2000 through September 2001.

Our analysis shows that weaknesses were most often identified for security program management, access controls, and service continuity controls. For security program management, we found weaknesses for all 24 agencies in 2001 as compared to 21 agencies (88 percent) in a similar analysis in 2000.[22] For access controls, we also found weaknesses for all 24 agencies in 2001—the same condition we found in 2000. For service continuity controls, we found weaknesses at 19 of the 24 agencies (79 percent) as compared to 20 agencies or 83 percent in 2000.

[22]U.S. General Accounting Office, *Computer Security: Critical Federal Operations and Assets Remain at Risk.* GAO/T-AIMD-00-314. Washington, D.C.: September 11, 2000.

Reform Provisions Create Agency and IG Challenges

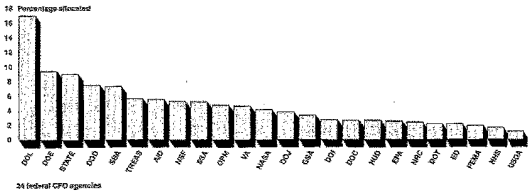
Agencies identified challenges during their first-year implementation of the reform provisions, some of which, according to the agencies, limited the extent of their efforts. Perhaps most significantly, several agencies acknowledged that they had not been reviewing their systems according to existing requirements in OMB Circular A-130. As a result, they did not have system reviews they could use to help respond to review requirements of the reform provisions. In addition, several agencies sought contractor assistance, but said that delays in obtaining this help limited what they could do in time to meet the September 10 deadline for reporting to OMB. For example, one agency was still trying to obtain contractor services as late as July 2001 with the reporting deadline only 2 months away. Also, several agencies noted that late final guidance from OMB on reporting also limited what they could do to gather and report information. Many agencies also had not maintained data that OMB requested be reported, such as training statistics and actual performance measure results that would help them demonstrate the extent to which they had met security requirements.

One final challenge emphasized by many agencies was the need for adequate funding to implement security requirements. Several agencies noted that funding limitations had directly affected their ability to implement existing security requirements and, thus, affected their compliance with the reform provisions. Although, in most instances, this issue involved a lack of funding, in at least one agency, CIO staff pointed to specific security funding the agency received as key to the improvement efforts it has undertaken in recent years.

While citing funding as an implementation challenge, agencies apparently had difficulty identifying how much they spend related to information security. The security costs that OMB requested agencies to report were not provided in some cases. In addition, for costs that were provided, there was no detail as to what these costs consisted of or how they are actually reflected in agency budget submissions. Further, while most of the 24 agencies we reviewed reported that they had integrated security into their capital planning and investment control process, 19 (79 percent) reported that they had not included security requirements and costs on every fiscal year 2002 capital asset plan submitted to OMB.

In addition to incomplete security cost data, costs that were reported to OMB varied widely. On the basis of the final costs shown in OMB's report to the Congress, we present, in figure 2, the 24 agencies' fiscal year 2002 security funding as a percentage of their total information technology spending. These percentages range from a high of 17.0 percent for the Department of Labor to a low of 1.0 percent for the Department of Agriculture.

Figure 2: Percentage of Agency Fiscal Year Information Technology (IT) Budget Allocated to IT



OMB reports that it assessed the agencies' performance against the amount they spent and did not find that increased security spending equals increased security performance. As a result, it concludes that there is no evidence that poor security is a result of lack of money, and that improvements in security performance will come from agencies giving significant attention to the security weaknesses it describes in its report.

While security funding might not always correlate with security performance, information security does involve costs, and OMB acknowledges the importance of this funding by requiring agencies to identify security funding in their budget submissions. We also agree with OMB that much can be done to cost-effectively address common weaknesses, such as security training, across government rather than piecemeal by agency. At the same time, however, agencies have specific weaknesses that they must correct. OMB has required agencies to identify these weaknesses and to indicate the level of resources required to correct them in their corrective action plans.

From the IGs' perspective, several have indicated that the requirement for an annual evaluation will represent a challenge because of their difficulty in obtaining adequate resources in today's competitive market for information security professionals. Further, by conducting an evaluation every year, the IGs believe they will lose the ability to deploy current limited resources in other important areas and may have to limit the scope of their work.

Improvements Efforts are Underway, But Challenges to Federal Information Security Remain

As I discussed previously, a number of improvement efforts have been undertaken in the past few years both at an agency and governmentwide level. Among these efforts and partially in response to the events of September 11, 2001, the president created the Office of Homeland Security, with duties that include coordinating efforts to protect critical public and private information systems within the United States from terrorist attack. The president also (1) appointed a special advisor for cyberspace security to coordinate interagency efforts to secure information systems and (2) created the President's Critical Infrastructure Protection Board to recommend policies and coordinate programs for protecting information for critical infrastructure. The board is to include a standing committee for executive branch information systems security, chaired by an OMB designee.

These actions are laudable. However, given recent events and reports that critical operations and assets continue to be highly vulnerable to computer-based attacks, the government still faces a challenge in ensuring that risks from cyber threats are appropriately addressed in the context of the broader array of risks to the nation's welfare. Accordingly, it is important that federal information security efforts be guided by a comprehensive strategy for improvement. In 1998, shortly after the initial issuance of Presidential Decision Directive (PDD) 63 on protecting the nation's critical infrastructure, we recommended that OMB, which, by law, is responsible for overseeing federal information security, and the assistant to the president for national security affairs work together to ensure that the roles of new and existing federal efforts were coordinated under a comprehensive strategy.[23] Our more recent reviews of the National Infrastructure Protection Center and of broader federal efforts to counter computer-based attacks showed that there was a continuing need to clarify responsibilities and critical infrastructure protection objectives.[24] As the administration refines the strategy that it has begun to lay out in recent months, it is imperative that it takes steps to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed.

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security

[23]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.

[24]U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities.* GAO-01-323. Washington, D.C.: April 25, 2001; *Combating Terrorism: Selected Challenges and Related Recommendations.* GAO-01-822. Washington, D.C.: September 20, 2001.

and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating federal agency security, and NIST, with assistance from the National Security Agency, is responsible for establishing related standards. In addition, interagency bodies—such as the CIO Council and the entities created under PDD 63 on critical infrastructure protection—are attempting to coordinate agency initiatives. Although these organizations have developed fundamentally sound policies and guidance and have undertaken potentially useful initiatives, effective improvements are not yet taking place. Further, it is unclear how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they 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 what computer security controls to implement and the level of rigor with which to enforce these controls. In theory, this discretion is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. 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.[25] 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. Implementing such standards for federal agencies would require developing a single set of information classification categories for use by all agencies to define the criticality and sensitivity of the various types of information they maintain. It would also necessitate establishing minimum mandatory requirements for protecting information in each classification category.

Third, ensuring effective implementation of agency information security and critical infrastructure protection plans will require active monitoring by the agencies to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required by the reform provisions, would allow for more meaningful performance measurement. In addition, the annual evaluation, reporting, and monitoring process established through these provisions, is an important

[25]GAO/AIMD-98-68, May 1998.

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 to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by the 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. 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. 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, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on information security will be important to 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.

Seventh, expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. As the director of the CERT® Coordination Center testified before this subcommittee last September, "It is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches." In addition, in its December 2001 third annual report, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (also known as the Gilmore Commission) recommended that the Office of Homeland Security develop and implement a comprehensive plan for research development, test, and evaluation to enhance cyber security.[26]

[26] *Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction.* December 15, 2001.

In summary, first-year implementation of the reform provisions has resulted in a number of positive initiatives and benefits, and OMB, the agencies, and the IGs all undertook efforts to implement these provisions. However, faced with limited past efforts to implement security and other obstacles, agencies in their reviews did not provide the scope or depth of coverage intended, particularly in testing and evaluating controls. The IGs also had to rely primarily on their existing work for this first-year effort. Consequently, much work remains to be done to achieve the objectives of the reform legislation. In addition, OMB did not report to the Congress on key elements of the provisions, such as the adequacy of agencies' corrective action plans and overall evaluation results for national security systems, or to provide supporting information. We plan to continue to work with OMB in an effort to find workable solutions to obtain the information needed for congressional oversight. These factors limit congressional insight into the status of information security for the federal government, as well as its ability to perform its responsibilities for oversight and budget deliberations. In addition, with the increasing threat to critical federal operations and assets and poor federal information security as indicated by reform provision reviews and evaluations, it is imperative that the administration and the agencies implement a comprehensive strategy for improvement that emphasizes information security and addresses known weaknesses.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

Contact

If you should have any questions about the testimony, please contact me at (202) 512-3317. I can be reached by e-mail at *daceyr@gao.gov.*

(310151)

Mr. HORN. Thank you very much for that succinct opening.

Mark A. Forman is the Associate Director, Office of Information Technology and e-Government, Office of Management and Budget. Welcome.

Mr. FORMAN. Thank you, Mr. Chairman, and thank you, Congressman Davis, both for your leadership and your vision as it relates to e-government and computer security. Having your focus and the oversight on this issue is critically important to the success of the initiatives that we are trying to accomplish for government-wide security. We understand not only the need for this, but we appreciate your having the hearing and the focus on this.

I would like to say good morning and thank you for inviting me here to discuss the lessons learned from the implementation of the Government Information Security Reform Act. I, too, have submitted the prepared testimony, and I will take a synopsis of that in my oral presentation.

As you know, the President has given a high-priority to security of government assets, and this includes government information systems and protection of the Nation's critical information assets from cyber threats and physical attack. We believe that protecting the information and the information systems on which the Federal Government depends requires agencies, first, to identify and resolve the current weaknesses and risks, as well as to then protect against the future vulnerabilities and threats.

Last October the President issued Executive Order 13231, the Critical Infrastructure Protection in the Information Age. That established the Critical Infrastructure Protection Board and created the chair as a special advisor to the President for Cyberspace Security.

Now the President has made OMB a critical member of this board. Our presence reflects our statutory role regarding security of Federal information systems. In addition, there are several committees under the board, and we chair the Standing Committee on Executive Branch Information Systems Security.

The administration has been proactive in implementation of the Government Information Security Reform Act, and I will refer to this from now on as the Security Act. This includes expanding the reporting requirements to include the Chief Information Officer and senior agencies' officials' input with the Inspectors General.

We have moved beyond simply reporting security weaknesses and are focusing on agency work to remediate the security weaknesses. The basic push behind our continuing work is a strong focus on management implementation of security.

We have recently taken the following two steps to help ensure a strong focus on maintaining senior management attention to security: First, in January, OMB Director Mitch Daniels sent letters to the heads of agencies and departments communicating our concerns regarding their fiscal year 2001 security performance. In general, agency heads responded back in writing with a commitment to resolve their past flaws. OMB will soon meet with all of the 24 large agencies and departments to discuss the work in implementing their corrective action plans.

Second, the President has charged Director Daniels with overseeing implementation of the management agenda through the use

of an executive branch management scorecard. This scorecard tracks agency improvement in five governmentwide areas and assigns a red, yellow, or green score.

One of these areas is expanding electronic government, and we are incorporating IT as a core criterion within that. This means that if an agency does not meet IT security criteria, it will not achieve a green score, regardless of the agency's performance under the other e-government criteria.

I would now like to talk a little bit about our report to Congress, the findings, some of the next steps. As you know, one of OMB's responsibilities under the Security Act is to submit each year a report to Congress that summarizes the results of security evaluations conducted by agencies and reported to OMB. On February 13th of this year, Director Daniels transmitted this report to the Congress.

At this time I would like to recognize the tremendous amount of work of agency program officials, CIOs, IGs, my staff, and all of their staffs in conducting the reviews and evaluations upon which the report is based. This was a large effort for all involved, and the report illustrates this work, as well as the ongoing efforts of agencies to remediate their weaknesses.

Additionally, the National Institutes of Standards of Technology continue to play their critical role in promoting IT security requirements among agencies. OMB policy requires that each agency's program implement policy standards and procedures consistent with NIST guidance. NIST has developed a security questionnaire, and most agencies use this document as the basis for conducting their annual reviews under the Security Act.

The OMB report represents a first year of implementation. It is a valuable baseline that has recorded the security agency performance. Even though the Security Act only required us to summarize the results, we expanded the report. We included the results of CIO and program official reviews in the recent activities we have undertaken in preparing the fiscal year 2003 budget decisions, OMB findings, and next steps, as well as additional efforts that we have undertaken and the agencies have taken to improve Federal information technology security.

From our assessment of agency performance, we have both validated the earlier positions on what the problems were and identified at a high-level important lessons learned. I would like to briefly sum those up.

First, security is primarily a management problem, not a technical or funding problem. Are you willing to support us if we push to get someone fired because they will not implement a security plan? Second, increased spending does not necessarily translate into increased security performance. Third, high-quality IG audits are necessary. The IGs provide an important, independent validation function. Fourth, agency employees with specific security responsibilities must have the authority to fulfill their responsibilities and at the same time have to be held accountable for their performance.

There are a number of additional actions I have described. A key part of the written testimony I would ask you to look at are the actions under the OMB Security Committee of the Critical Infra-

structure Protection Board. Therein we have laid out a process to focus more rapidly on actions needing to be addressed, because this is an ever-changing issue both in terms of vulnerability and threats.

I would also ask you to take a look at the decisions that we have made in the budget, and would ask your support in the appropriations decisions that ultimately will have to make these into reality.

Finally, I would like to focus on the governmentwide initiatives that we have underway leveraging the project matrix work and the enterprise architecture work. The development of the governmentwide enterprise architecture assessment is critical and a central part of not only our e-government efforts, but our cyber-security efforts. Basically, to more clearly identify and prioritize the security needs for government assets, OMB is going to direct all large agencies to undertake a project matrix review, and that was a key element of the 2003 budget.

Again, I would like to thank you for the opportunity to testify. We have a summary in the testimony of the six government problems that we identified in the report, and I would be willing to answer any questions in that regard at the appropriate time.

[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 GOVERNMENT EFFICIENCY,
FINANCIAL MANAGEMENT, AND INTERGOVERNMENTAL RELATIONS
U.S. HOUSE OF REPRESENTATIVES
March 6, 2002

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me here to discuss the lessons learned from implementation of the Government Information Security Reform Act (Security Act). Additionally, I would like to talk with you about the recent OMB report to Congress on Federal government information security reform, our findings in the report, and the next steps we are taking with agencies to improve IT security.

Before I get to the substance of my testimony, I need to make sure the Subcommittee understands that I do not serve in a confirmed position within the Office of Management and Budget (OMB). As a general policy, OMB does not usually send officials in non-confirmed political positions to testify before Congress. However, because of the importance of the issue and the fact that OMB does not yet have a Deputy Director for Management, the OMB Director decided it was in the best interest of the Administration to have me appear on his behalf as a witness for this hearing.

As you know, the President has given a high priority to the security of government assets including government information systems and the protection of our nation's critical information assets from cyber threats and physical attacks. We believe that protecting the information and information systems on which the Federal government depends, requires agencies to identify and resolve current security weaknesses and risks, as well as protect against future vulnerabilities and threats.

Last October, the President issued Executive Order 13231, "Critical Infrastructure Protection in the

Information Age." This Executive Order establishes the Critical Infrastructure Protection Board and creates a Chair who serves as the Special Advisor to the President for Cyberspace Security. This Board will promote greater coordination and consistency among the Federal agencies. The Board will oversee work to ensure that: Federal policies and processes are appropriate so that critical commercial and government IT assets are adequately secure; emergency preparedness communications are operating adequately; and government and industry work closely together to address increasing interconnections and shared risk. Richard Clarke serves as Chair of the Board and Special Advisor to the President for Cyberspace Security, and reports both to Governor Ridge on issues that affect homeland security and to National Security Advisor Condolezza Rice on issues that affect national security.

The President has made OMB a member of the Critical Infrastructure Protection Board. OMB's presence reflects our statutory role regarding the security of Federal information systems. Additionally, OMB chairs the Board's standing committee on Executive Branch Information Systems Security.

Government Information Security Reform

The Administration has been proactive in implementation of the Government Information Security Reform Act (Security Act). This includes expansion of its reporting requirements to include CIO and senior agency officials' input with IGs, and moving beyond simply reporting security weaknesses and instead focusing on agency work to remediate their security weaknesses. The basic push behind our continuing work is a strong focus on management implementation of security.

Senior Management Attention to Security

In January, OMB Director Mitch Daniels sent letters to the heads of agencies communicating our concerns regarding their FY01 security programs. The primary purpose of these letters was to capture senior management attention. In general, agency heads responded in writing with a commitment to resolve their past flaws. As follow-on from these letters, the OMB summary report, and agency

corrective action plans, OMB will soon meet with all 24 large agencies.

As you know, the President has charged Director Daniels with overseeing the implementation of his Management Agenda through the use of an Executive Branch Management Scorecard. This Scorecard tracks agency improvement in five government-wide problem areas and assigns a red, yellow, or green score. Under one of these areas, expanding electronic government, we are incorporating IT security as a core criteria. This means that if an agency does not meet the IT security criteria it will not achieve a green score regardless of their performance under the other e-gov criteria. Additionally, IT security is a key component of the other Management Agenda items.

OMB Guidance on Remediating Security Weaknesses

Last fall, OMB issued guidance to agencies on the development and submission of security plans to correct weaknesses. These plans require agencies to identify, assess, prioritize, allocate resources, and monitor the progress of corrective efforts for their security weaknesses. They are important because they bring a discipline to the process, are a valuable management and oversight tool, and make tracking progress much easier for all involved.

Additionally, Federal agencies are required to provide quarterly updates to OMB. The information provided to OMB in the initial plans of action and milestones (POA&Ms) were used during the FY03 budget process to prioritize agency funding for security and define remediation activities.

Successful implementation of corrective action plans that appropriately address all weaknesses will bring agencies a long way toward positive overall security performance, progress that we expect to document in next year's report to the Congress.

I would also like to point out that while we all tend to focus largely on the 24 Chief Financial Officers Act agencies, these action plans are also being developed by over 30 small and independent agencies, such as FDIC, SEC, and NEH. We plan on meeting with the small and independent agencies as well.

OMB Report to Congress - Findings and Next Steps

As you know, one of OMB's responsibilities under the Security Act is to submit annually a summary report to Congress summarizing the results of security evaluations conducted by agencies and reported to OMB. On February 13th, Director Daniels transmitted this report to Congress.

At this time I would like to recognize the tremendous amount of work of agency program officials, CIOs, IGs, and all of their staffs in conducting the reviews and evaluations. This was a large effort for all involved and the report illustrates this work as well as the ongoing efforts of agencies to remediate their weaknesses.

Additionally, the National Institute of Standards and Technology (NIST) continues to play a critical role in promoting IT security requirements among agencies. Among their activities they have recently issued security guidance on telework, security webservers, and cryptography. OMB policy requires that each agency's program shall implement policy standards and procedures, which are consistent with NIST guidance. Also, NIST has developed a security questionnaire, based on the Federal CIO Council and NIST Security Framework. This security questionnaire assists agencies in performing self-assessments of their IT systems. It is based primarily on NIST technical guidance and GAO's Federal Information System Controls Audit Manual and allows agencies to assess the management, operational, and technical controls of their systems. Indeed, most agencies used this document as the basis for conducting their annual reviews under the Security Act. We are currently working with NIST on the automation of this tool for agency use.

This report represents the first year of implementation of the Security Act. It is a valuable baseline that has recorded agency security performance. The findings in the report are based solely on work performed by agencies during the FY01 reporting period. Our report briefly describes recent Administration activities involving IT security -- namely the President's Executive Orders on Homeland Security and Cyber Security. The report discusses the steps taken by OMB and Federal agencies to implement the Security Act as well as

additional efforts OMB and the agencies have taken to improve Federal information technology security.

From our assessment of agency performance under the Security Act, we have both validated our earlier positions on the problems with IT security and identified important lessons learned:

1. Security is primarily a management problem, not a technical or funding problem;

2. Increased security spending does not necessarily translate into increased security performance;

3. High quality IG audits are necessary. Prior to the Security Act IG involvement in IT security was largely through their work in financial management. IGs provide an important independent validation function; and

4. Agency employees with specific security responsibilities must have the authority to fulfill their responsibilities and be held accountable for their performance.

Our report also identifies six common government-wide security weaknesses we found in our review of agency submissions, along with activities underway by OMB and the agencies to resolve them. Where agencies are performing well, we identified their actions as examples of effective practices.

For the most part these weaknesses are not new or surprising. We, along with GAO, and agency IGs, have found them to be problems for at least six years. This time, the evaluation and reporting requirements of the Security Act have given OMB and Federal agencies an opportunity to develop a comprehensive cross government baseline of agency IT security performance that has not previously been available. As I mentioned earlier, OMB has taken steps to maximize this opportunity through additional guidance requiring agencies to develop and submit initial corrective action plans.

I will briefly discuss these weaknesses and the next steps the Administration is taking to assist agencies in resolving them.

1. Senior management attention. Senior leaders must consistently establish and maintain control over the security of the operations and assets for which they are responsible. As the Security Act recognizes, security is a management function which must be embraced by each Federal agency and agency head.

   Next Steps: OMB is working through the President's Management Council to promote sustained attention to security as part of OMB's work on the President's Management Agenda and the integration of security into the Scorecard that I spoke of earlier.

2. Measuring performance. Agencies must be able to evaluate the performance of officials charged with implementing specific requirements of the Security Act. To evaluate agency actions, OMB requested data in the FY01 Security Act reports that agencies measure job and program performance, i.e., how senior leaders evaluate whether responsible officials at all levels are doing their job. They must be able to evaluate the performance of officials charged with securing agency operations and assets. Virtually every agency response regarding performance implies that there is inadequate accountability for job and program performance related to IT security.

   Next Steps: OMB has drafted quantifiable management level performance measures for agencies to identify the performance gaps in their IT security work. Our guidance for last year's report required agencies to respond to 13 topic areas, which represented the requirements of the Security Act and OMB budget guidance. They range from questions on agency security training and incident response capabilities to the integration of security into their capital planning processes. Our FY02 guidance will still contain these questions, but will move beyond the baseline and focus on progress. We will require agencies to report the results of their security evaluations and their progress implementing their corrective action plans according to these performance measures. To ensure that accountability follows authority, the measures are organized according to the Federal employee responsible. These measures are mandatory and represent the minimum metrics against which agencies must track against to ensure performance and measure progress. We encourage

agencies to develop additional measures that address their needs.

Additionally, NIST is developing technical security metrics that will assist agencies in measuring the security performance of their programs and systems and help them implement appropriate security controls to protect their programs and systems.

3. Security education and awareness. Agencies must improve security education and awareness. General users, IT professionals, and security professionals need to have the knowledge to do their jobs effectively prior to be held accountable.

   Next Steps: OMB and Federal agencies are now working through the new Critical Infrastructure Protection Board's education committee and the CIO Council's Workforce Committee to address this issue. Additionally, the CIO Council's Best Practices Committee is working with NIST through NIST's Federal Agency Security Practices website to identify and disseminate best practices involving security training. Finally, one of the Administration's electronic government initiatives is to establish and deliver electronic-training. This initiative will provide e-training on a number of mandatory topics, including security, for use by all Federal agencies, along with State and local governments.

4. Funding and integrating security into capital planning and investment control. Security must be built into and funded within each system and program through effective capital planning and investment control. As OMB has done for the past two years in budget guidance, Federal agencies were instructed to report on security funding to underscore this fundamental point. Systems that do not integrate security into their IT capital asset plans will not be funded.

   Next Steps: OMB continues to aggressively apply this approach 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. The IT investment justification and documentation process is key to sound program and financial management. Security must not be viewed differently. This process demonstrates explicitly

how much agencies are spending on security and associates that spending with a given level of performance. Thereafter, Federal agencies will be far better equipped to determine what funding is necessary to achieve improved performance. This is the security component of the business case.

5. Ensuring that contractor services are adequately secure. Agencies must ensure that contractor services are adequately secure as most Federal IT projects are developed and many operated by contractors. Therefore, IT contracts need to include adequate security requirements. Many agencies reported no security controls in contracts or no verification that contractors fulfill any requirements that may be in place.

   Next Steps: Under the guidance of the OMB-led security committee established by E.O. 13231, an issue group will develop recommendations, to include addressing how security is handled in contracts themselves. We are working with the Federal Acquisition Regulatory Council to develop for government-wide use a clause to ensure security is addressed as appropriate in contracts.

6. Detecting, reporting, and sharing information on vulnerabilities. Far too many agencies have virtually no meaningful system to test or monitor system activity and therefore are unable to detect intrusions, suspected intrusions, or virus infections. This places individual agency systems and operations at great risk since response depends on detection. Perhaps most significant, not detecting and reporting IT security problems could cause cascading harm. Our vastly inter-networked environment also means an environment of shared risk with the best security being only as strong as the weakest security.

   Early warning for the entire Federal community starts first with detection by individual agencies, not incident response centers at the FBI, GSA, DOD, or elsewhere. The latter can only know what is reported to them, reporting can only come from detection, and guidance for corrective action depends upon both. This need is thus not a technical one, but a management one. Additionally, it is critical that agencies and their components report all incidents in a timely manner to GSA's Federal Computer Incident Response Center and appropriate law enforcement

authorities such as the FBI's National Infrastructure Protection Center as required by the Security Act.

Next Steps: GSA's Federal Computer Incident Response Center reports on a quarterly basis to OMB on the Federal government's status on IT security incidents. Additionally, under OMB and Critical Infrastructure Protection Board guidance, GSA is exploring methods to disseminate patches to all agencies more effectively. Additionally, I plan on issuing updated guidance to agencies on reporting to FedCIRC, stressing the necessity for accurate and timely reporting.

While not addressed in our report, we also found that agencies have not implemented a disciplined process for systems security planning, accreditation, and review. The first such review is comprehensive and complex, but subsequent ones are simply maintenance; NIST is completing its automation of their tool for agency use to conduct these reviews.

While OMB can and will continue to assist agencies with their efforts in addressing their security weaknesses, both the responsibility and ability to fix these weaknesses and others, ultimately lie with agencies. IGs, OMB, and GAO cannot do it for them.

Additional OMB Actions

Finally, I would like to provide you with more detail on three other items that we continue to work on.

1. OMB Security Committee. In our report we mentioned the formation of a security committee on Executive Branch Information Systems Security. OMB will chair this standing committee under the President's Critical Infrastructure Protection Board. The CIP Board was created by the President in Executive Order 13231, "Critical Infrastructure Protection in the Information Age." This Executive Order establishes the Critical Infrastructure Protection Board and creates a Chair who serves as the Special Advisor to the President for Cyberspace Security. The goal of the Board is to promote greater coordination and consistency among the Federal agencies. Members of the committee will be representatives from all the key

communities in the Federal government that have a role in IT security. This includes CIOs, CFOs, PEs, IGs, agency program officials, agency security managers, and HR folks. Most of the Committee's work will be performed by individual issue groups. These issue groups will form to address a discrete issue such as security and acquisition as designated by the Committee (including issues referred by other organizations, committees, and individual agencies). Upon completion of an issue, the issue group will dissolve. The work of the Committee will occur under existing policy and guidance setting authorities. Neither the Committee nor the issue groups have any policy or guidance setting authority and thus shall not issue guidance or other documents.

2. IT Security and the Budget. OMB will continue to engage the agencies in a variety of ways to address the problems that have been identified, continuing to emphasize both the responsibilities and performance of agency employees in addition to accountability for exercising those responsibilities and consequences for poor performance. We will continue to rely on traditional budget and management processes to ensure that IT security needs are being addressed. OMB has made it a policy to stop funding projects that do not adequately address security requirements and neglect to document how security planning and funding is integrated into the project's life cycle.

   To ensure that security is addressed throughout the budget process OMB established the following four criteria:

   -- Agencies must report security costs for each major and significant IT investment. In the long run, it will greatly help agencies demonstrate explicitly how much they are spending on security and associates that spending with a given level of performance. Thereafter, Federal agencies will be far better equipped to determine what funding is necessary to achieve improved performance. This is the security component of the business case. We do this to ensure that security is included and funded for each IT investment throughout the life of the investment. We do not use security funding as an indicator of

good security. It is an indicator of good security management -- that the agency has integrated security and views security as a critical component of the entire investment and not as an add-on.

-- Agencies must document in their business cases that adequate security controls have been incorporated into the life cycle planning and funding of each IT investment.

-- Agency security reports and corrective action plans are presumed to reflect the agency's security priorities and thus will be a central tool for OMB in prioritizing funding for systems.

-- Agencies must tie their corrective action plans for a system directly to the business case for that IT investment.

Additionally, we developed through the budget process, a process for tracking projects that are at risk due to poor business cases. We are currently tracking nearly 400 major IT projects which amount to approximately $10B of both the Federal government's $48B FY02 IT spending and $52B FY03 IT spending. Of the 400 projects roughly half are at risk in part to poor demonstration of security planning, procedures, and controls. Poor security in projects amount to just over $6B (full IT investment costs) of the $10B at risk. We are working with agencies to address these concerns and many of them are currently revising their plans to address the problems.

3. Enterprise Architecture and Project Matrix. The development of a government-wide enterprise architecture is a central part of the Administration's electronic government efforts. Establishment of an architecture for the Federal government will greatly facilitate information sharing based on the lines of business of each agency. Additionally, this architecture will identify redundant capabilities and provide ample opportunities to increase efficiencies while reducing costs, and duplicative programs. Accordingly, OMB will also be able to better prioritize and fund the Federal government's security needs.

To more clearly identify and prioritize the security needs for government assets, OMB will direct all large agencies to undertake a Project Matrix review. Project Matrix was developed by the Critical Infrastructure Assurance Office of the Department of Commerce. A Matrix review identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector. This is largely a vertical view of agency functions. To ensure that all critical government processes and assets have been identified, once reviews have been completed at each large agency, OMB will identify cross-government activities and lines of business for Matrix reviews. In this way OMB will have identified both vertically and horizontally the critical operations and assets of the Federal government's critical enterprise architecture and its relationship beyond government.

Conclusion

In discharging OMB responsibilities under the Security Act, OMB has communicated with the appropriate agency heads to impress upon them that true improvements in security performance comes not due to external oversight from OMB, IGs, the General Accounting Office (GAO), or Congressional committees, but from within - holding agency employees, including CIOs and program officials, accountable for fulfilling their responsibilities. I cannot stress this point enough - Security is the responsibility of every employee in the agency. There must be consequences for inadequate performance. OMB has also underscored the essential companion to accountability -- the need for clear and unambiguous authority to exercise responsibilities.

The first year of the Security Act has brought us all a better and more detailed understanding of the Federal government's IT security status than ever before. The reporting requirements of the Security Act have afforded agencies, IGs, GAO, OMB, and Congress the ability to capture a performance baseline. This baseline clearly illustrates significant and pervasive security weaknesses across every department and agency. We have considerable problems in IT security that requires serious attention. Now that we are better informed of our security weaknesses, and agencies have developed plans on how to remediate those

weaknesses, the next step is continuing the implementation of those plans and determine our success through measuring performance.

Mr. HORN. Well, thank you very much. I want to emphasize what you just did now, the President's Executive order, which was Critical Infrastructure Protection in the Information Age, and he established a board, as you suggested. The chair, who serves as a special advisor to the President for Cyberspace Security, and that, of course, is Richard Clark, who serves as the Board and he is the Special Advisor to the President for Cyberspace Security. He reports both to Governor Ridge on issues that affect homeland security and to the National Security Advisor, Condoleezza Rice, on the issues that affect national security.

The President has made OMB a member of the Critical Infrastructure Protection Board. Are you on that board as part of it?

Mr. FORMAN. Yes, I am.

Mr. HORN. I think it shows the President has taken some real action with people that did have his ear.

I am going to have to recess now. When I come back, the ranking member, Ms. Schakowsky, will have her statement in, and we will then go down the line. We have a Journal vote before us.

Ms. SCHAKOWSKY. Is there an opportunity for me to do that now?

Mr. HORN. Sure, sure. She will put it in now, and once she finishes, we are in recess.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. I appreciate that.

I want to thank the chairman for holding this hearing and for his leadership on computer security issues in the House. I look forward to working with him to improve government information security reform language that was passed in the Congress.

It was passed in the last Congress as a part of the Defense Authorization Act, and as such, really didn't get, in my view, adequate review in the House. No hearings were held, and we had very little opportunity to affect the content.

Consequently, under Representative Waxman's leadership, we sought and received a 2-year sunset on this legislation. Our experience over the past year has substantiated the wisdom of that approach.

There are a number of problems in this legislation that have already come to our attention. I am hopeful that today's hearing will help us put together a more complete picture of the actions to make this legislation more effective.

One problem has already come to our attention. One of the problems is the reports prepared by the agencies. We asked the GAO to use agency information security reports to develop the scorecards for our hearing last fall. It came as a surprise when the administration refused to allow access to those reports, claiming that they were predecisional and part of the budget process. After much negotiation, we were finally given access to executive summaries, hardly a satisfactory outcome.

A more serious shortcoming of this legislation is the absence of any system to assure that all agency systems are checked and protected. Today few, if any, agencies have a complete inventory of its computer systems, even though just such an inventory was required for Y2K compliance just 2 years ago. Without a complete inventory, it is impossible to know if all systems have had the risks assessed and the protections tested. We must make sure that every agency maintains a current inventory of systems and has in place

a systematic process to assess risk for those systems and to test the protections in place.

I am sorry that I was late. I do look forward to hearing today's witnesses, if not reading the testimony, and hope that each of you will understand that we share the common goal of assuring the public that our systems have adequate protection. So I thank you all for coming today.

We will be back.

[The prepared statement of Hon. Janice D. Schakowsky follows:]

**STATEMENT OF THE HONORABLE JAN SCHAKOWSKY
AT THE HEARING ON
GOVERNMENT INFORMATION SECURITY REFORM**

MARCH 6, 2002

Thank you Mr. Chairman for holding this hearing, and for your leadership on computer security issues in the House. I look forward to working with you to improve the government information security reform language passed in the last congress.

The government information security language was passed in the last Congress as a part of the Defense Authorization Act. Consequently, it did not get adequate review in the House. No hearings were held, and we had little opportunity to affect the content. Consequently, under Representative Waxman's leadership, we sought and recieved a two year sunset on this legislation. Our experience over the past year has substantiated the wisdom of that approach.

There are a number of problems in this legislation that have already come to our attention. I hope that today's hearing will help us put together a more complete picture of the actions needed to make this legislation more effective.

One problem that has already come to our attention is the reports prepared by the agencies. We asked GAO to use agency information security reports to develop the score cards for our hearing last fall. It came as a surprise when the Administration refused to allow access to those reports claiming that they were predecisional and a part of the budget process. After much negotiation, we were finally given access to the executive summaries. Hardly a satisfactory outcome.

A more serious shortcoming of this legislation is the absence of any system to assure that all agency systems are checked and protected. Today, few if any agencies have a complete inventory of its computer systems, even though just such an inventory was required for Y2K compliance just two years ago. Without a complete inventory, it is impossible to know if all systems have had the risks assessed and the protections tested. We must make sure that every agency maintains a current inventory of systems, and has in place a systematic process to assess risk for those systems and to test the protections in place.

I look forward to today's witnesses, and I hope that each of you will understand that we share the common goal of assuring the public that our systems have adequate protection

[Recess.]

Mr. HORN. Recess has ended, and we will begin next with Mr. Bement, who is the Director of the National Institute of Standards and Technology [NIST]—not in the mist, but NIST. [Laughter.]

Dr. BEMENT. Right. Thank you, Mr. Chairman.

Mr. HORN. As a little kid, I remembered well the standards and your beautiful campus out there.

Dr. BEMENT. You are more than welcome anytime, Mr. Chairman.

Thank you very much for giving me the opportunity to speak to you about NIST's role in cyber-security. NIST's Computer Security Program supports the vision of strong cyber-security and its critical role both in homeland security and e-government. Our agency has specific statutory responsibilities under both GISRA and the Computer Security Act of 1987 for developing standards and guidances that help Federal agencies to protect sensitive, unclassified information.

Specifically, NIST has published a guidance for firewalls, intrusion detection, cryptography, public Web servers, and risk management. We also conduct computer security research in close cooperation with industry and academia. We work to find ways to apply new technologies in a secure manner.

The solutions that we develop are made available to both public and private users. This research helps us to find more cost-effective ways to implement and address security requirements.

I would now like to highlight a few of our more important recent contributions to improve cyber-security in Federal agencies. In December the Secretary of Commerce approved the Advanced Encryption Standard [AES], as a Federal security standard. Within days, commercial firms were announcing products that incorporated the AES. It is clear that AES soon will be used extensively internationally and be available in a wide array of commercial products to protect sensitive Federal information. We expect AES will be used daily to secure trillions of dollars in electronic transactions and to protect sensitive personal business and government information.

The Chief Information Officers' Council and NIST developed a security assessment framework to assist agencies with a very high-level review of their security status. The framework established the groundwork for standardizing on five levels of security and defined the criteria agencies could use to determine if the levels were adequately implemented. By using the framework levels, an agency can prioritize agency efforts as well as to evaluate progress.

Building from the framework, NIST issued a more detailed security questionnaire that most agencies use to conduct their programmed system reviews. This document provided guidance on applying the framework. In addition, the guide provides control objectives and techniques that can be measured for each area. Many agencies use this to prepare their GISRA responses to OMB.

NIST also recently formed a team that specializes in helping Federal agencies navigate through the dangers of cyberspace. The Computer Security Expert Assist Team [CSEAT], helps agencies understand how to protect their computer systems, how to identify

and fix existing vulnerabilities, and how to anticipate and prepare for future security threats.

The CSEAT reviews are also valuable to NIST. They give us a firsthand look at how NIST guidance is implemented, helping us to improve our products and processes.

Our new information-sharing Web site for Federal agency security practices covers a host of topics ranging from contingency planning to network security. Computer security professionals from various Federal agencies have contributed much of the material on the site. The site also contains the best practices for critical infrastructure protection and computer security identified by the Federal Chief Information Officers' Council. The site is one of the latest additions to NIST's Computer Security Resource Center and is one of the busiest and most popular spots on the entire NIST Web site.

Another aspect of our work involves security testing which complements security standards by giving users confidence that the security standards and specifications are implemented correctly in the products they buy. NIST and our Canadian counterpart have set up a joint program to help ensure correct and secure implementation of unclassified cryptographic algorithms and products. Statistics show that 48 percent of the modules tested voluntarily under this program have security flaws that were corrected during testing. So, without our program, the Federal Government would have only a 50/50 chance of buying products that correctly implemented cryptography.

I would like to point out that in carrying out our responsibilities under GISRA and the Computer Security Act, we consult frequency with other agencies. In particular, we work very closely with the Office of Management and Budget. We consult with OMB representatives on the Federal Chief Information Officers' Council, the Federal Computer Security Program Managers' Forum, and the Committee on National Security Systems. We soon will serve on the newly formed Committee on Executive Branch Information Systems Security. I would like to take this opportunity to commend my OMB colleagues for their steadfast support in promoting our security standards and guidelines with Federal agencies.

Let me close by emphasizing that our national commitment to improved cyber-security must be increased in Federal agencies and elsewhere. NIST has a proven track record of success and stands ready to play key roles in this and other facets of homeland security.

Thank you very much, Mr. Chairman. I will be pleased to answer any of your questions.

[The prepared statement of Dr. Bement follows:]

Statement of

Dr. Arden L. Bement, Jr.

Director
National Institute of Standards and Technology
U.S. Department of Commerce

Before the

Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

House of Representatives
United States Congress

"Lessons Learned from the Government Information Security Reform Act of 2000"

March 6, 2002

Good morning Chairman Horn and Members of the Subcommittee. On behalf of the National Institute of Standards and Technology (NIST), thank you for the invitation to speak to you today about cybersecurity issues. I am Arden Bement, Director of the National Institute of Standards and Technology (NIST), which is part of the Department of Commerce's Technology Administration.

Let me commend the Subcommittee for focusing on the critical issue of cybersecurity in Federal departments and agencies. As evidenced by the recent OMB report to the Congress on Federal Government Information Security Reform, cybersecurity is a continuing challenge that demands the attention of the Congress, the Executive Branch, industry, academia, and the public. It is also vital to our homeland defense efforts. The NIST security program supports the vision of strong cybersecurity and its crucial role both in homeland defense as well as in E-Government by enabling improvements in service to our citizens through secure electronic programs.

In the area of cybersecurity, NIST has specific statutory responsibilities for developing standards and guidelines to assist Federal agencies in the protection of sensitive unclassified systems. This is in addition to our broad mission of strengthening the U.S. economy – including improving the competitiveness of America's information technology (IT) industry. In support of this mission, we conduct standards and technology work to help industry produce more secure, yet cost-effective, products, which we believe will be more competitive in the marketplace. Having more secure products available in the marketplace will, of course, also benefit Federal agencies, since they will be using commercial products to secure their systems.

NIST's Computer Security Division in our Information Technology Laboratory (ITL) is the focal point of our security program. Our program focuses on a few key areas: cyrptographic standards and guidelines; public key infrastructure; security research; agency assistance and the National Information Assurance Partnership (NIAP), which is jointly managed by NIST and the National Security Agency (NSA) to focus on increasing the number and quality of IT security products. NSA, as you may know, has IT security responsibilities for many of the classified government systems.

To put our program in perspective, please keep in mind that approximately $10 million of direct Congressional appropriations, funding a NIST staff of about 45, supports both our Federal and industry computer security responsibilities. This is a very small program when compared with NSA's recently released Information Assurance budget of $755M for FY 2002. However, NIST's small program does provide a significant return on investment. A new independent economic impact study conducted by the Research Triangle Institute (RTI) conservatively estimates that NIST's security research into "role based access control (RBAC)" has saved U.S. industry $295 million and accelerated industry's adoption of this advanced access control method by a year. ITL's research cost taxpayers only $2.3 million. RTI estimated that RBAC technology has saved U.S. industry a total of $671 million, and that our work was responsible for 44 percent of the savings.

NIST's Statutory Responsibilities

Before expanding on some of NIST contributions to cybersecurity, I would like to briefly review the IT responsibilities that Congress assigned to NIST under two key statues -- the Government Information Security Reform Act (GISRA) and the Computer Security Act.

NIST was specifically tasked under GISRA to:

- Develop, issue, review and update standards and guidance for security of Federal information systems;
- Develop, issue, review and update guidelines for training in computer security awareness and accepted computer security practices;
- Provide agencies with guidance for security planning to assist in development of applications and system security plans;
- Provide guidance and assistance to agencies on cost-effective controls for interconnecting systems; and
- Evaluate information technologies to assess security vulnerabilities in Federal systems.

The GISRA-assigned responsibilities build upon the long-standing responsibilities of NIST under the Computer Security Act and other statutes. The Computer Security Act was established to improve security and privacy of sensitive information in federal computer systems. It gave statutory authority to NIST to:

- Develop uniform security standards and guidelines for the protection of sensitive information in non-classified federal computer systems;
- Develop technical, management, physical and administrative standards and guidelines for cost-effective security and privacy of sensitive information in non-classified federal computer systems;
- Develop guidelines for use by operators of federal computer systems containing sensitive information in training their employees in security awareness and good security practices;
- Develop validation procedures to evaluate the effectiveness of the security standards and guidelines developed;
- Assist the private sector, upon request, in using and applying NIST standards and guidelines;
- Provide technical assistance to operators of federal computer systems in implementing these standards and guidelines; and
- Coordinate closely with other agencies such as the Departments of Energy and Defense, the Office of Management and Budget, and others as appropriate, to assure to the maximum extent feasible that standards and guidelines developed are consistent and compatible across the entire federal sector (classified and non-classified).

We work very closely with the Office of Management and Budget (OMB) in carrying out our security responsibilities under GISRA and the Computer Security Act. We work with OMB representatives on the Federal Chief Information Officers Council, the Federal Computer Security Program Managers' Forum, and the Committee on National Security Systems. We will soon also serve on the newly formed Committee on Executive Branch Information Systems Security. We have had security personnel on detail to OMB. All of our Federal Information Processing Standards are formally coordinated with OMB prior to promulgation by the Secretary of Commerce. We also solicit comments on draft guidance and standards from Federal agencies and departments via the CIO Council, the Federal Computer Security Program Managers' Forum, and our Computer System Security and Privacy Advisory Board (on which Federal agencies are represented). We also distribute our final guidelines and standards to these groups, and others, and make them widely available via our popular Computer Security Resource Center (http://csrc.nist.gov/) web site. While on the subject of our Federal agencies, let me take this opportunity to commend my OMB colleague for OMB's steadfast support in promoting our security standards and guidelines with Federal departments and agencies.

Let me highlight some of the recent NIST contributions in meeting these important responsibilities.

Security Guidelines and Standards

In 2001-2002, NIST published the following guidance:

- Firewalls and Firewall Policy,
- Recommendation for Block Cipher Modes of Operation - Methods and Techniques,
- Underlying Technical Models for Information Technology Security,
- Introduction to Public Key Technology and the Federal Public Key Infrastructure,
- Intrusion Detection Systems,
- Risk Management Guide for Information Technology Systems,
- A Comparison of the Security Requirements for Cryptographic Modules in Federal Information Processing Standards 140-1 and FIPS 140-2,
- Guidelines on Active Content and Mobile Code,
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security), and
- Security Self-Assessment Guide for Information Technology Systems.

We also published draft guidelines currently under review by Federal departments and agencies as well as other interested organizations and individuals concerning:

- Guideline on Network Security Testing,
- System Administration Guidance for Windows 2000 Professional,
- Use of the Common Vulnerabilities and Exposure (CVE) Naming Scheme,
- Contingency Planning Guide,
- Security for Telecommuting and Broadband Communications, and

- Security Guide for Interconnecting Information Technology Systems.

In addition, during the same timeframe, we completed the following Federal Information Processing Standards (FIPS):

- Advanced Encryption Standard (FIPS 197);
- Security Requirements for Cryptographic Modules (FIPS 140-2)

Late last year, the Secretary of Commerce approved the Advanced Encryption Standard, (or AES) as a federal security standard. Within days of the AES announcement, commercial firms were announcing products that incorporated the AES, making it clear that the AES will soon be used extensively internationally -- and be available in a wide array of commercial products to protect sensitive Federal information. As AES is deployed, we expect that it will be used daily to secure trillions of dollars in electronic transactions and protect sensitive personal, business, and government information.

We also have prepared updates to the Secure Hash Standard (FIPS 180) and are producing the final standard in response to public comments we have received. In addition we have issued numerous ITL Bulletins during the last year to provide guidance to agencies and others on a broad list of topics.

Reducing Vulnerabilities Through Research and Security Testing

Both research and security testing can help reduce vulnerabilities in the commercial IT products used to support the nation's critical infrastructures.

Research on information technology vulnerabilities and the development of techniques for cost-effective security are urgently needed. When we identify new technologies that could potentially influence our customers' security practices, we research the technologies and their potential vulnerabilities. We also work to find ways to apply new technologies in a secure manner. The solutions that we develop are made available to both public and private users. Some examples are methods for authorization management and policy management, ways to detect intrusions to systems, and demonstrations of mobile agents. Research helps us find more cost-effective ways to implement and address security requirements.

Security testing complements security standards by providing consumers with confidence that security standards and specifications are correctly implemented in the products they buy. Implementing cryptography correctly and securely can be complicated. However, unless it is correctly implemented, it may provide no protection. Therefore, in conjunction with the Government of Canada's Communication Security Establishment we operate the Cryptographic Module Validation Program, which helps ensure correct and secure implementation of the particular cryptography. The Cryptographic Module Validation Program has now validated over 200 modules with another 75 or more expected this year. This successful program utilizes private sector

accredited laboratories to conduct security conformance testing of cryptographic modules against the cryptographic Federal standards NIST develops and maintains. The testing by the laboratories and our work with Canada involves access to unclassified public algorithms and test suites, and not to any Federal government operational cryptographic keys or classified information.

Statistics from the testing laboratories show that 48% of the modules brought in for voluntary testing had security flaws that were corrected during testing. In other words, without our program, the Federal government would have had only a 50/50 chance of buying correctly implemented cryptography!

In addition, in recent years we have worked to develop the "Common Criteria" (ISO/IEC 15408), which can be used to specify security requirements. These requirements are then used by private-sector laboratories, accredited by NIST, for the voluntary evaluation of commercial products needed for the protection of government systems and networks. This work is undertaken in cooperation with the Defense Department's National Security Agency in our National Information Assurance Partnership.

We have developed a web-based tool known as ICAT that allows users to identify known vulnerabilities for their specific software. NIST's ICAT then provides links to vendor sites at which the users can obtain patches to address these vulnerabilities. This is important because many computer break-ins exploit known vulnerabilities.

Training and Awareness

Timely, relevant, and easily accessible information to raise awareness about the risks, vulnerabilities and requirements for protection of information systems is urgently needed. This is particularly true for new and rapidly emerging technologies, which are being delivered with such alacrity by our industry.

We also host and sponsor information sharing among security educators, the Federal Computer Security Program Managers' Forum, and industry. We sponsor the web-based Computer Security Resource Center to provide a wide-range of security materials and information to the community and link to the Federal Computer Incident Response Center at GSA and other emergency response centers. We actively support information sharing through our conferences, workshops, web pages, publications, and bulletins. Finally, we also have a guideline available to assist agencies with their training activities and are an active supporter of the Federal Information Systems Security Educators' Association.

Security Assessment Framework and Self-Assessment Guideline

The Chief Information Officers Council and NIST developed a security assessment Framework to assist agencies with a very high level review of their security status. The Framework established the groundwork for standardizing on five levels of

security and defined criteria agencies could use to determine if the levels were adequately implemented. By using the Framework levels, an agency can prioritize agency efforts as well as to evaluate progress.

Building from this Framework, NIST issued a more detailed security questionnaire that most agencies used to conduct their program and system reviews. This document (NIST Special Publication 800-26) provides guidance on applying the Framework by identifying 17 control areas, such as those pertaining to identification and authentication and contingency planning. In addition, the guide provides control objectives and techniques that can be measured for each area. Many agencies used this to prepare their GISRA responses to OMB.

Federal Agency Security Practices Web Site

NIST recently inaugurated the Federal Agency Security Practices (FASP) website (http://csrc.nist.gov/fasp/), building upon past successful work of the Federal CIO Council's Best Security Practices pilot effort to identify, evaluate, and disseminate best practices for CIP and security. NIST was asked to undertake the transition of this pilot effort to an operational program. As a result, NIST developed the FASP site, which contains agency policies, procedures and practices; the CIO pilot best practices; and, a Frequently-Asked-Questions section. Agencies are encouraged to share their IT security information and IT security practices and submit them for posting on the FASP site. Over 60 practices are now available via the site. Some practices have been modified so as not to identify the specific submitting agencies.

Establishment of the NIST Computer Security Expert Assist Team

To assist agencies in securing their IT through improved management, Congress appropriated $3M in new funding in FY 2001 for NIST to establish the Computer Security Expert Assist Team (CSEAT). This team performs a review of an agency's computer security program from a management, not a technical, perspective. The team's efforts help improve federal cybersecurity planning and implementation efforts by assisting governmental entities in improving the security of their information and cyber assets. The CSEAT accomplishes this by performing a review of an agency's computer security program. The review is based on a combination of proven techniques and best practices and results in an action plan that provides a Federal agency with a business case-based roadmap to cost-effectively enhance the protection of their information system assets.

The CSEAT has three primary purposes:

1. to assist agencies in improving the security of Federal IT systems,
2. to help reduce disruption of critical Federal systems/services, and
3. to improve Federal agency CIP planning and implementation efforts.

The CSEAT also helps Federal agencies understand how to protect information systems, identify and fix existing vulnerabilities, and prepare for future security threats.

The CSEAT also facilitates exchange of best security practices among government agencies and between the government and private sector.

These reviews are important not only to the specific agencies, but also to NIST. One of the key objectives in implementing the CSEAT initiative was to assist NIST in identifying systemic security issues and challenges specific to distinct agency environments in order to support development of needed computer security guidance. The CSEAT visits and subsequent reviews of agency's processes help NIST obtain a "first hand" understanding of how NIST guidance is implemented at the working level in diverse federal organizations. This is invaluable to NIST in meeting its statutory requirements for deployment of effective security standards and guidelines. The CSEAT reviews provide critical information for NIST strategic planning in support of technical assistance for Federal agencies.

No funding was provided for this team in FY 2002. The Executive Order on Critical Infrastructure Protection states that the heads of Executive Branch departments and agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems. The President's FY 2003 budget proposes funding CSEAT as a cost-reimbursable program where Federal agencies pay for CSEAT reviews. The requested funding of $1 million will cover administrative costs to maintain a small staff to oversee and administer CSEAT activities, review methodology, and ensure currency of information and approach.

Conclusion

Let me close by emphasizing that our national commitment to improve cybersecurity must be increased -- in Federal agencies and elsewhere. There is still much more to be done to address the continuing challenges of IT security. NIST has a proven track record of success and stands ready to play a key role in this and other facets of homeland defense. While we have a small effort in terms of funding NIST has a very critical role in Federal IT security. We will continue to work to meet our statutory responsibilities in protecting sensitive systems of Federal departments and agencies, leading our security research, standards development, and testing programs, running the Computer Security Resource Center, and raising awareness and demand for security products and services. Thank you, Mr. Chairman. I will be pleased to answer any questions.

Mr. HORN. Thank you, and we are delighted to have your paper in particular.

We now turn to the Honorable Roberta L. Gross, former Inspector General, National Aeronautics and Space Administration. I lost track of you. You have been a witness here before. When did you leave the Inspector General's position?

Ms. GROSS. Saturday.

Mr. HORN. Saturday? OK.

Ms. GROSS. But your staffer had asked me prior to the time, and I had told her that I would be leaving, but we talked about I would still come. So here I am.

Mr. HORN. Great. Well, welcome. So if we could summarize your testimony?

Ms. GROSS. Absolutely. I thank you for inviting me to testify today on GISRA, and my testimony is obviously based on my recent experience as NASA's Inspector General. I served in that post from August 1995 through March 2, 2002. I am also basing it on my experience as being the former Chair of the IGs' IT Roundtable, where we discuss cross-cutting issues across the government.

Last year I, along with a representative of the GAO, testified before the Senate Committee on Governmental Affairs on a precursor of GISRA, Senate bill 1993. The then-chair of the committee, the Honorable Senator Thompson, began his opening statement by recounting how time after time the GAO kept writing reports, Inspectors General kept writing reports, about serious lapses in IT security, deficiencies in IT capital, in human resources planning. He observed that over the years law after law was passed, regulation after regulation, and the issues seemed to reoccur and nothing seemed to get better, and it was no wonder, with so many laws and regulations, that this Senator rhetorically asked, "Why are we enacting GISRA?" The answer is that GISRA was needed, GISRA has had success, and it can be improved.

My remarks are going to be divided into three sections: bad news—I couldn't be an Inspector General, or former Inspector General, without that, right? Good news, next steps, and lessons learned.

During our GISRA reviews and audits at NASA, we found problems in each of the six areas highlighted by OMB. I am only going to address three of them, using NASA as an illustration, and I incorporate by reference my written testimony.

The three that I would like to use as illustration are, one, lack of senior management attention; two, limited programs for security awareness and education, and, three, failure to exercise oversight of contractor security services.

While some of the agency's IT practices are more mature than those at many agencies, and I notice that NASA got a "C-," and they are above one of the yellow lines, NASA management has historically been unwilling to recognize and/or fully acknowledge the significance of the IT weaknesses and deal with them in a timely manner. There are various interrelated reasons for that.

They were engaged, since I have been there, in downsizing, funding problems, but also, seriously, an unwillingness of middle management or IT security officials to tell senior management the extent of the problem, as well as lack of reception by senior manage-

ment to hear about the extent of the problem. So that is a good segueway into the first problem: senior management attention.

Leaderships of all the agencies occupy bully pulpits by virtue of their positions. They can regularly remind staff of their IT responsibilities and obligations. No cost; talk is cheap. What should they be doing?

They should be addressing their employees in as many forums as possible and reinforce that IT security is everybody's responsibility. For example, we saw that the former Administrator used his office—this is at NASA again—used his office as a bully pulpit for safety. Safety was NASA's No. 1 core value. At senior staff meetings, leadership reiterated this value, discussed lessons learned, and tracked programs related to safety.

However, no similar attention to ITS, other than during the Y2 crisis. Y2 came and went, and senior management attention came and went. I hope the new Administrator will use his office as a bully pulpit on IT issues.

Let's talk about the CIO. The CIO also did not utilize the bully pulpit to communicate IG findings, and we had the same findings over and over again, and NASA agreed to implement our recommendations over and over again. They didn't monitor these recommendations that they agreed to implement.

Instead of using the bully pulpit and communicating to the staff and saying, "Don't wait for the IG. Why don't you look to see if your systems have similar problems? And here are some suggestions that the agency IG recommended. Maybe these will be fixes for you." This really didn't happen.

But I do want to point out the good news. Since the GISRA report, the CIO has shown improvement in communicating and sharing his communications with the OIG about IT vulnerabilities we identified in the IT reviews. I used lack of communication as one of the reasons why we found material weakness for purposes of the GISRA report; the CIO failed to use a very low-cost/no-cost forum.

No. 2, another problem highlighted by OMB, as well as the IGs, is insufficient security awareness and training. Civil servants and contractors, they all need to have the training before being given access to systems. If personnel have more responsibilities and higher-level sensitivities to systems, they need to have different kind of training.

But NASA did not establish 100 percent training participation for the targeted groups for all its measures, despite the age-old adage: "You're only as good as your weakest link." The point is not that you are going to make 100 percent of your goal, but shouldn't that be your goal? How could you have less than 100 percent for people to be trained as your goal? Otherwise, you're going to allow and accept weak links.

Our biggest complaint on this training issue was that NASA did not have all of its civil servant system administrators trained, but even more significant is that they excluded, as their performance measure, contractor personnel. Guess what? Seventy-nine percent of NASA's systems administrators are contractors. Their training is not even measured; they are not even tracked in terms of whether they have the appropriate training. This is an obvious risk for which NASA did not implement compensating controls.

Oversight of contractor responsibility. Over and beyond incorporating IT clauses into contracts, which OMB addressed and we address, you still have to make sure that you know who these contractors are with who you are working with. They have wide-range responsibilities. Think about it. They are your systems administrators. They purchase and provide desktops. They are the ones that safeguard sensitive information. They maintain your systems. They put the patches in your system.

Who are these people? What are they doing? And are you oversighting them? Contractor oversight is an area where the government needs to be attentive, and certainly NASA does.

OK, good news. OMB focuses greater cooperation between OIGs and CIOs. I do want to say and give credit to two individuals who are here. Never say IGs don't say good things about people. Glen Schlarman and Kamela White are both here. There's Glen, and Kamela, she's hiding over there.

Mr. HORN. Why don't you speak that back into the mike? They didn't quite catch it.

Ms. GROSS. OK. Both Kamela and Glen are here. In forwarding their summary report to Congress, they did not try to paint a rosy picture, but tried to present an accurate picture, and this wasn't always easy because sometimes it looked like the IGs and the agencies were reporting on two different worlds.

I also want to commend them for their steadfast insistence that management work with IGs in developing corrective action plans. This has been a welcomed increase in cooperation between IGs and CIOs. IG after IG report this.

Equally important, GISRA brought accountability to the heads of the agencies. They had to forward the report. They had to forward an IG report as well as the agency report and put their name on it. It was their report. No more plausible deniability. They couldn't claim they didn't know what the IT issues were at their agencies. That was real good.

OK, next steps, and I'm going quickly—GISRA I think should be extended in some form for 2 to 5 years, so that agencies will implement agreed-upon changes. In subsequent legislation, Congress should consider to allow the IGs to have more flexibility in their reporting responsibilities. This year it will still be the same, but if you still have to do this kind of level of intensity without having additional funding from the agency and OMB, you are not going to be able to move into other high-risk areas. Unlike when Congress passed the CFO audit and most IGs got more resources, that didn't happen for GISRA.

Another suggestion is that there should be a sunset provision maybe in the 3 to 5 years, so you can evaluate is what you want to do. Are the means overtaking the end? So I think a sunset provision is good.

Another way to ensure greater uniformity is to eliminate the act's bifurcation of responsibilities for national security programs. Under the act, the agency head asks an outside evaluator to come in, look at national security systems, which the IG later reviews. NASA's IG's office never got that security report in time to review it for the GISRA Act.

The IGs use at the least, a uniform evaluation methodology. They will either use government standards, PCIE-wide standards for reviews, or GAGAS, government auditing standards for their audits. This is not always the case. Agency heads bring in different people. Who knows what standards they are using? So this should be eliminated, and it should be having the IGs do 100 percent of that.

These next steps require a focus on agencies' infrastructure for reporting intrusions, and also the agencies' first-responders. Are they training first-responders? When you have a program manager they want to fix the problem. Often their fixes may increase the problem. Maybe the intruder is still in the network trojanizing the systems. Program managers don't always know what they are doing when they fix problems, partly because they are not coordinating with law enforcement. IGs must look at, and I think this should be an area of Congress could look at to see if they are actually, the agencies, are implementing law enforecement coordination. The Congress passed the USA Patriot's Act of 2001 to help law enforcement with the cyber war. One section allows victims of computer attacks to authorize persons acting in color of law to monitor trespassers on their computer systems. This provides law enforcement with the same authority in the cyber world that a police officer has in the normal world if there is a burglary in progress. This had to be amended so the monitoring wouldn't be considered wiretapping. This is important. I want to commend Howard Schmidt, vice chair, President's Critical Infrastructure Board. He is working with Richard Clark. He has initiated contacts with NASA's Inspector General's office to help frame a OIG-wide response for the victim agencies. NASA, under my term, established the first Inspector General's Computer Crimes Unit, and Howard was turning to our unit in part because we were recognized both nationally and internationally for our expertise. It is crucial that OIGs help their victim agencies and those agencies look to this monitoring provision. Let's not wait for the cyber-attack, the law has already passed.

Nobody has procedures. I know, because I put a request for monitoring into the agency, and it is under review. We need to have more sense of urgency for something like this. The law was passed because there was an urgent situation. That urgency cannot wait for the next attack, and if that is a cyber attack——

Mr. HORN. Let me ask you a minute about this particular aspect on the follow up and getting that. Did they use the Carnegie-Mellon operation in part or did they use the FBI one?

Ms. GROSS. Carnegie-Mellon is not a law enforcement entity. They get information from both the private sector, and government agencies. Part of the way Carnegie-Mellon works, is sharing of information. Although it is not a law enforcement entity, they do have a member of the FBI on the Cert. They do share information with law enforcement. It goes back and forth, but it is not a law enforcement entity.

The FBI also wanted this Computer Security Act passed. They, like any other law enforcement entity needed that in order to do the monitoring; consensual monitoring by the owners of systems when you know there is a burglary, a cyber burglary in process,

they can monitor. They needed that provision. There's no nationwide or agencywide practices on how to use that authority though.

But, again, remember with the FBI, the FBI has to look at the private sector, universities and international entities. The group that really looks for their victim agencies is the OIGs. Many of them know the agency people; they know the systems; they know the programs. You might have a shot at figuring out the intent and motive of intruders if IGs are involved.

They have fully qualified law enforcement special agents. This is a way of ensuring those much needed protections.

Right now, you have a focus of the FBI looking at physical terrorism. The role of the IGs becomes even more paramount because of that. They need to step-up to the plate. I would be glad to speak more on that. I can wax eloquent on that issue.

Mr. HORN. We will get to that again, but we will move on to Mr. Gorrie.

Ms. GROSS. Yes.

[The prepared statement of Ms. Gross follows:]

Statement of Roberta L. Gross
Before the
House of Representatives Committee on Government Reform
March 6, 20002

I thank you for the opportunity to be here today to discuss "Lessons Learned From the Government Information Security Reform Act (GISRA) of 2000". My testimony is based primarily on my recent experience as NASA's Inspector General[1] and Chair of the Information Technology (IT) Roundtable, a committee of the President's and Executive Councils on Integrity and Efficiency (PCIE/ECIE).[2]

My remarks are divided into three sections: 1) The Bad News, 2) The Good News, and 3) Next Steps.

THE BAD NEWS

Along with Jack Brock, formerly the Director of Governmentwide Defense Information Systems with the United States General Accounting Office (GAO), I testified before the Senate Committee on Governmental Affairs on March 2, 2000, on S. 1993, the Government Information Security Act of 1999, a precursor proposal to the current GISRA Act. When the then Chair of the Committee, the Honorable Senator Thompson, began his opening remarks, he turned to Mr. Brock and me and stated rhetorically, "We get report after report . . . If I were you guys, I would wonder why you are even in business and whether or not we pay any attention. . . . This last [GAO] report still points out serious deficiencies. . . and it makes you wonder what in the world it takes to get anybody's attention." Senator Thompson went on to recount how time after time the GAO and Inspectors General (IGs) reported serious lapses in IT security and deficiencies in IT capital and human resources planning. He observed that over the years, law after law were passed to address these issues and nothing seemed to get better.

We knew to what he was referring:

For instance, we knew that the IGs have identified IT related issues as among the top management concerns in the Federal Government. The PCIE/ECIE reviews found that "OIGs across government report a remarkably consistent series of top management challenges confronting their agencies: information technology resources, data, integrity

[1] I served as NASA's Inspector General from August 1995 to March 2, 2002.
[2] Executive Order No. 12805, Integrity and Efficiency in Federal Programs, May 11, 1992, established the PCIE and ECIE. These Councils are chaired by the Deputy Director for Management of the Office of Management and Budget (OMB) and are comprised of Federal agency Inspectors General (IGs). IGs meet regularly to identify and discuss governmentwide areas of weaknesses and vulnerabilities of crime, fraud, waste and abuse in Federal programs. The IT Roundtable, one of the PCIE/ECIE committees, focuses on governmentwide issues associated with IT. For example, the IT Roundtable is sponsoring a session in April 2002 with Mark Forman, Associate Director for Information Technology and E-Government, OMB, as part of a PCIE/ECIE review of the President's e-government initiative. IGs will focus, among other issues, on whether agencies are implementing appropriate internal controls to ensure the integrity, availability, and security of government records generated by these initiatives.

and security, financial management, GPRA accountability, procurement and grants management, and human capital staffing" [emphasis supplied].[3]

We also knew that GAO identified continuing IT challenges as part of its High Risk reports. These challenges include: strengthening Agency information security; improving the collection, use, and dissemination of government information; pursuing opportunities for electronic government; constructing sound enterprise architectures; fostering mature systems acquisition, development and operational practices; ensuring effective Agency IT investment practices; and developing IT human capital strategies.[4]

We knew about the laws and regulations to which Senator Thompson was referring, which agencies are required to follow, and which, if implemented, would result in good IT practices. For example, key guidance is provided by OMB Circular A-130 "Management of Federal Information Resources." That circular directs that users of Federal information resources have the skills, knowledge, and training to manage information resources. One of the circular's premises is that the application of up-to-date IT presents opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies. [5]

Other legal authorities governing IT referred to by Senator Thompson include the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35); the Clinger-Cohen Act (also known as "Information Technology Management Reform Act of 1996") (Pub. L. 104-106, Division E); the Privacy Act, as amended (5 U.S.C. 552a); the Chief Financial Officers Act (CFO Act) (31 U.S.C. 3512 et seq.); the Federal Property and Administrative Services Act, as amended (40 U.S.C. 487); and the Computer Security Act of 1987 (Pub. L. 100-235).

It is no wonder with so many laws and regulations that the Senator rhetorically asked, "Why enact GISRA?" To answer that question, I will briefly summarize the GISRA results and refer to the OIG findings at NASA, for purposes of illustrating general points. However, first I will summarize my overall perception of GISRA – it has had success. It can be improved.

---

[3]The top management challenges are set forth in "A Progress Report to the President: President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE)-Fiscal Year 2000." Excerpts from Office of Inspector General (OIG) reports show a range of IT problems: "DOE OIG Finds That Contractor Did Not Clear Sensitive Information From Surplus Computers"; "NASA OIG Assessment of International Space Station Communications Systems Identifies Needed Improvements"; "HUD OIG Documents Continuing Problems with Information Technology"; SSA OIG Questions Reliability of Codes in SSA Databases"; "Treasury OIG Documents Deficiencies in Customs' Automated Systems"; "TIGTA Identifies Security Weaknesses in Key IRS Programs"; "USPS OIG Aids in Investigation of Computer Hacker".

[4]See GAO publication, Major Challenges and Program Risks: A Governmentwide Perspective, page 18 (GAO 01-241, January 2001).

[5]OMB Circular A-130 is directed to the Federal government, which is the largest single producer, collector, consumer, and disseminator of information in the United States.

GISRA Results

OMB recently submitted to Congress the summary GISRA report entitled, "FY 2001 Report to Congress on Federal Government Information Security Reform." The report highlighted six common governmentwide security weaknesses:

1) lack of senior management attention;
2) little or no performance measures for officials with IT security responsibilities;
3) limited programs for security awareness and education;
4) inadequate integration of security into capital planning and investment control process;
5) failure to exercise oversight of contractor security services; and
6) inadequate attention to detecting, reporting, and sharing information on vulnerabilities.

Results of NASA GISRA Review

During our GISRA audits and reviews at NASA, the OIG found problems in each of the areas highlighted by OMB. While some of the agency's IT practices are more mature than those at many other agencies, NASA management has historically been unwilling to recognize and/or fully acknowledge the significance of the weaknesses and deal with them in a timely manner.

- Senior Management Attention

The leadership of the Agency - the Administrator, the CIO, and the Center Directors - occupy "bully pulpits" by virtue of their positions. They can regularly remind staff of their ITS obligations at virtually no cost. What should they do? They should address their employees in as many forums as possible and reinforce that ITS is everyone's responsibility. They should provide adequate funding for and, thereafter, mandate training and awareness programs and ensure such programs are actually implemented. Does that happen?

Consider the situation at NASA. The OIG has identified ITS as a material weakness for purpose of the Federal Managers Financial Integrity Act (FMFIA),[6] in part, because of the lack of communication by the CIO of the vulnerabilities and weaknesses the OIG identifies in audits and reviews. Throughout Fiscal Years 2000 and 2001, we identified time and time again the same weaknesses. Specifically, we identified weaknesses in NASA's ability to apply adequate host-based [7]security, including password management; control over privileged system capabilities; critical system directory and file protection;

[6]Based on the recommendation of the NASA Internal Control Council, the Administrator reported ITS as a significant area of concern for purposes of FMFIA. NASA OIG contracts with Pricewaterhouse Coopers (PWC) for the annual financial audit. PWC found ITS a reportable condition as related to financial systems.

[7]Host-based security controls protect the availability, integrity, and confidentiality of systems and are designed to prevent unauthorized access from within the organization and from outside intruders who can circumvent network or perimeter controls.

configuration of security capabilities provided by the operating system; and security monitoring and reporting activities. Also, we found and still find problems in how NASA implements firewall capabilities to protect NASA networks from unauthorized access or compromise from external networks, such as the Internet.

We have seen the former Administrator use his office as a "bully pulpit". During his last several years, he reiterated at every meeting that safety was NASA's number one core value. At senior staff meetings he and his leadership reiterated this value, discussed lessons learned and tracked programs related to safety. However, he did not devote similar attention to ITS (other than during the Y2K crises).[8] I hope the new Administrator will use his office as a "bully pulpit" on IT issues.

The CIO did not utilize the "bully pulpit" to communicate the findings of the IG ITS reviews and audits. We found no documented evidence that the CIO used IG reports to motivate the ITS community to minimize security vulnerabilities by examining their systems for similar problems. The CIO also did not effectively track agreed-upon recommendations stemming from IG audits and reviews to ensure managers took appropriate action. Because of this lack of communication (a cost/low cost tool to address ITS problems), the CIO did not utilize an opportunity to better understand resource requirements, funding shortfalls, and priorities. Moreover, agreed-upon corrective actions have been slow and incomplete. Since the GISRA report, however, the CIO has shown improvement in communicating (and sharing with the OIG his communications) about IT vulnerabilities we have identified in our reviews.

- Performance Measures for Officials With IT Responsibilities:

To its credit, NASA uses commercial software to scan its IT systems for vulnerabilities. While this is a good first step, the OIG has been concerned that NASA did not inform decision makers about the limitations of the scanning program[9] and, as a result, may have understated NASA's IT vulnerabilities and provided undue assurance about the integrity, availability and confidentiality of NASA's information. NASA did agree to refine their vulnerability testing. OMB acknowledged NASA efforts in this area noting that it "does find it healthy, however, that the Agency has developed measures that are worthy of substantive discussion. Many agencies have not progressed this far."

---

[8]The Year 2000 (Y2K) date conversion problem involved computer systems and applications that used a two-digit format (mm/dd/yy) to generate a date. These systems needed to be updated so that they would continue to function properly once the year 2000 began.

[9]NASA initially identified a fixed-set of 57 vulnerabilities. However, the vendor classified 389 vulnerabilities as high risk. Moreover, the scanning software vendor issues monthly updates with additional scanning capabilities. Admittedly, NASA would not want to scan even for all the high-risk vulnerabilities because of problems with "false positive" results. Nevertheless, NASA's metrics were too focused on reporting progress against fixed vulnerabilities, rather than adequately reflecting the changing risk environment.

- Security Awareness and Training:

A key component of NASA's IT program is that all users, both civil servant and contractor, must complete training before given access to any of NASA's systems. However, only 5 of the 10 IT training awareness performance measures established in FY 2001 required all individuals in the targeted group to complete the required training. Similarly, only 5 (42%) of the 12 FY 2002 IT training and awareness performance measures were set at 100% participation for the targeted group despite the well-known ITS adage that an entity is only as safe as its weakest link. The OIG was particularly concerned that NASA did not set 100 % training participation for its civil servant system administrators. (System administrators have the primary responsibility for implementing the security policies on the IT systems they manage). It is even more significant that the system administrator training measure completely excluded contractor personnel, who comprised about 79% of NASA's system administrators. This is an obvious risk for which NASA did not implement compensating controls.

- Integration of ITS into capital planning and investment:

The OIG reported that the Agency did not include security requirements and costs in its capital asset plans, and did not plan to submit all plans for FY 2002 as requested by OMB. The reviews further found that the Agency had not calculated IT security costs on a system-by-system basis as required by OMB budget guidance. OMB noted that NASA did report security costs on their FY 2003 budget materials.

- Oversight of contractor responsibility

NASA's Federal Acquisition Regulation Supplement 1852.204-76 – the ITS clause – requires contractor compliance with the GISRA, OMB, and other security requirements. NASA established December 31, 2000, as the deadline for incorporating the IT clause in its applicable contracts. However, as of May 2001, one of three Centers the OIG reviewed had not identified all contracts subject to the clause. Further, NASA did not include the applicable ITS requirements in its purchase orders (contracts), grants, and cooperative agreements. Consequently, the Agency lacked reasonable assurance of complying with GISRA requirements, and NASA's systems and information may be subject to additional security risks.

Over and beyond incorporating IT clauses into contracts, NASA must vigorously oversight its contractors. These contractors have wide ranging responsibilities, including providing system administrators; purchasing and providing desktops to and maintaining them for civil servants; and safeguarding sensitive information. Contractor oversight is an area where NASA needs to devote considerably more attention.

- Detecting, Reporting, and Sharing Information on Vulnerabilities

To its credit, NASA has implemented a generally effective automated incident response center. However, NASA's incident reporting process is not standardized. Specifically,

the OIG found significant differences in the quarterly ITS incident data used for managing the ITS program and the data used for reporting ITS incidents to outside agencies, such as the Federal Computer Incident Response Center (FedCIRC). Further, NASA's Automated Systems Incident Response Center (NASIRC)[10] and the OIG did not receive consistent, standardized information from the Centers on IT incidents.

The OIG also found that NASA had not adequately addressed recommendations from 1999 regarding standardized incident response capabilities and strong management controls to ensure appropriate Center reporting. Although NASA issued guidance based on our recommendations, the reporting discrepancies the OIG found indicate that NASA needed to take more stringent action to ensure its incident response capability provided the intended benefits. These benefits are meant for NASA, the Federal government, and the public at large since NASA reports to national centers that share information with the private and government sectors. I will discuss the importance of detecting and information on intrusions, reporting in the section, "Next Steps."

THE GOOD NEWS

This "Good News" section would not be nearly as long without the work performed by two individuals from OMB's Information and Technology Branch, Glenn Schlarman and Kamela White. They deserve special commendation for their considerable time and energy on the GISRA effort. They worked hard to make the GISRA process work. In forwarding their summary report to Congress, they did not try to paint a rosy picture, but attempted to present as accurate a summary as is possible. (This was not always an easy process when some agencies and the IGs seemed to be reporting two different worlds.) I also want to commend them for their steadfast insistence that management work with the IGs in developing corrective action plans. One of the major by-products of the GISRA review and correction action planning process has been a welcomed increase in the cooperation between most CIOs and IGs.

So the first part of the good news is that OMB has become very focused on the IT efforts of the Federal agencies. Equally important, GISRA brought accountability to heads of agencies. GISRA required these agency heads to forward to OMB the summary reports from management and the IGs. The agency heads, thus, had no plausible deniability – they could not claim that they did not know the IT issues at their agency.

For many IGs and their agencies, GISRA brought needed additional scrutiny to IT issues, expanding the more limited reviews by IG (or external) auditors during the course of the financial statement audits. In contrast, to the more narrow financial audit scrutiny, GISRA draws all agency information systems into the evaluation process. Moreover, the agencies could not ignore IG, GAO or other review recommendations since OMB specifically required agencies to submit how they planned to correct reported deficiencies.

[10]NASIRC provides NASA with ITS incident response capabilities including centralized incident tracking, technical assistance, inter-Center coordination, trend analysis, and proactive and responsive correction action.

Another benefit from GISRA is that it focuses responsibility for IT security to the managers who "own" the systems versus placing sole responsibility on the security organization. As one IG stated, "In other words, it makes security a part of the management's day-to-day job and mindset instead of compartmentalizing it with the security people."

NEXT STEPS

GISRA should be extended in some form for 2-5 years in order for agencies to implement agreed upon changes. In any subsequent legislation, Congress should consider allowing IGs more flexibility in their reporting responsibilities. The annual requirement creates resource problems, particularly for smaller IG offices regardless whether they use inside staff or utilize the services of a contractor. Many IGs also have been concerned that limited budgets and personnel may inhibit them from performing substantial and adequate audit procedures, particularly if continued extensive annual reporting is required.[11] Along the same line, IGs also are concerned that if they cannot use a risk based approach, they will drain resources from other high-risk program areas. Some IGs suggested that any extension of the GISRA Act include a "sunset provision" so that Congress can re-evaluate whether it wants to extend the Act and, if so, whether it wants to make some changes.

All these suggestions appear sound. Agencies need time to implement their plans. IGs need to be able to review agency implementation efforts. However, a sunset provision ensures that Congress will evaluate this legislation which requires resource-intensive reports, to ensure that the law is having its intended impact.

As part of next steps, OMB can provide greater clarity in the review process from OMB directed both to the agencies and the IGs. This process will provide a more accurate yardstick of how agencies are doing. However, if OMB intends to issue additional guidance for the reports, then this has to occur early in the review process.[12]

Another way to ensure greater uniformity is to eliminate the Act's bifurcation of responsibilities for national security systems. The Act provides that the head of the agency appoint the evaluators of agency's national security systems. The IG's role is to audit the evaluation. This provision is not efficient. Evaluators selected by the head of the agency do not use a common approach or methodology, whereas IGs use PCIE standards for reviews and generally accepted government auditing standards for audits. Also, the timing of the agency's review may cause problems for the IG evaluation. In NASA's case, the OIG did not receive the reports from the outside evaluators in time to perform the IGs required review. Moreover, this bifurcation ignores the fact that most

[11]When Congress passed the law requiring the resource intensive annual CFO financial audits by IGs (or an external auditor selected by the IG), most IG offices received additional resources to meet this obligation. Generally, this did not happen when GISRA became law.

[12]Some IGs observed that the OMB reporting instructions, issued June 22, 2001, required the OIGs to perform additional procedures in addition to those that had previously been communicated by OMB. Because the OIGs had to submit their independent evaluations in early September 2001, the June reporting instructions did not allow OIGs time to perform extensive audit procedures for the additional OMB areas.

IGs are already performing some reviews of their agencies' national security systems. Any GISRA follow-on legislation should provide that the IGs conduct, or at their discretion, the IGs select another source to conduct, the national security system reviews.

Some IGs wanted greater clarity from OMB as to the consequences for an agency which makes the review process a paper shuffling exercise without addressing the specific security risks identified by the GISRA reports. In this regard, OMB should emphasize that agency management overall, not just CIO's, will be held accountable for continuing IT security deficiencies and give some definition to what OMB envisions to enforce accountability.

In the coming year, OMB, the agencies, and IGs need to focus on the governmentwide deficiency in detecting and reporting incidents. In this interconnected world, ITS vulnerabilities in the Federal government impact the private sector and vice versa.[13] The GISRA reports made clear that many agencies do not have the infrastructure for detecting and, thereafter, reporting intrusions. They have not established an agency clearing house which can report and analyze data for the agency and forward to and receive information from FedCIRC. Many do not have staff trained as first responders who can analyze the patterns of intrusions and take appropriate steps to meet the crucial need of law enforcement to have early access to evidence that is properly obtained and retained. The first responders must have training or they will only respond to the requests of the program managers to "fix" the "immediate problem". Program managers mistakenly believe their only concern is to have continued access to their networks. However, these "fixes" are sometimes harmful: they prevent law enforcement analysis of the intent and motive of the intruder; they may destroy the evidentiary trail to discern whether the intruder has left behind hacker tools and/or trojanized the systems for future attacks.

The Congress has enacted the USA Patriot's Act of 2001 in part to help law enforcement in this cyber war. Section 217 of that Act allows victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer system.[14] In short, the purpose of this law is to allow law enforcement to assist victims in the cyber world in the same way police with consent enter into homes to intercept burglars in the act of committing crimes.

---

[13] The previous Administration recognized the need to focus on the protection of the interconnected critical infrastructure through the issuance of Presidential Decision Directive 63 (PDD 63), on May 22, 1998. PDD 63 defines critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and the government." The current Administration has issued an Executive Order to further define the Federal government's response to the interdependencies of the nation's critical infrastructures.

[14] Before monitoring can occur, four requirements must be met: First, the owner or operator of the "protected" computer must authorize the interception of the trespasser's communications. Second, the person who intercepts communications must be engaged in an ongoing investigation. Authority to intercept ceases at the conclusion of the investigation. Third, the person acting under color of law must have reasonable grounds to believe the contents of the intercepted communication will be relevant to an ongoing investigation. Fourth, investigators must only intercept communications to and from the trespasser, and not intercept non-consenting users authorized to use the computer.

IGs during the current round of the GISR reviews should examine whether their agencies are implementing appropriate procedures to utilize this important tool which allows law enforcement to properly play its role in protecting their victim agencies. The time for establishing procedures is not in the midst of a critical cyber infrastructure attack.[15]

Summary

GISRA worked. It brought needed high level attention to IT issues. GISRA should be extended but modified in some respects along the lines suggested in today's testimony. Regardless of the fate of the Act, I hope that the attention to IT resulting from GISRA reviews does not follow the course of the Y2K crisis reviews. During that crisis, the Federal government, at the highest levels, focused on IT issues. OMB was very involved, requiring reports from agencies and monitoring their progress in corrective actions. The IGs committed considerable audit and inspection resources to this effort, reviewing agencies' efforts to ensure integrity in the process. The President used his office as a "bully pulpit" through the widely respected Special Assistant to the President, John Koskinen. Y2K came and went, and the intense scrutiny and focus of the agencies and OMB on IT came and went. IT issues require the continued and vigilant attention of the Federal government and the private sector.

[15]Another next step for IGs in protecting their victim agencies against cyber attacks will be to work with Howard Schmidt, Vice Chair, President's Critical Infrastructure Protection Board. He has initiated contact with the NASA OIG to help develop a framework for OIGs in their law enforcement capacity to protect agency cyber critical infrastructure. He turned to the NASA OIG because both the computer crimes and technical division staff in that organization are well recognized in national and international law enforcement communities for their expertise.

NASA is fortunate to have this dedicated and talent cadre. The Agency needs to provide it sufficient support or the Agency will be less protected. Before I left as NASA IG, I specifically asked NASA's Administrator to personally reach out to assure this group of his support. This is certainly a no cost-low cost use of his "bully pulpit."

Mr. HORN. Robert G. Gorrie is the Deputy Staff Director, Defense-wide Information Assurance Program Office, and Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

When did you fill that Assistant Secretaryship?

Mr. GORRIE. No, sir, I am Office of the Assistant Secretary. They have that a little backward there.

Mr. HORN. I see, OK.

Mr. GORRIE. I conspire to that, though, but——

Mr. HORN. Well, remind me, who is the Assistant Secretary in that area?

Mr. GORRIE. Mr. Stenbit is, sir.

Mr. HORN. Mr. Who?

Mr. GORRIE. John Stenbit.

Mr. HORN. How do you spell the last name?

Mr. GORRIE. S-T-E-N-B-I-T.

Mr. HORN. OK, yes, because I haven't really followed it, but in the days of Y2K, until the General occupying the effort left, I know there's been sort of up and down under the previous administration. I assume Mr. Stenbit, then, is the Bush administration?

Mr. GORRIE. Yes, sir, he followed Mr. Art Money, who was the previous ASDC3I.

Mr. HORN. Well, go ahead.

Mr. GORRIE. Yes, sir, thank you, Mr. Chairman and members of the subcommittee. I am honored to be here and pleased to have the opportunity to speak with your committee about lessons learned by DOD from assessments we conducted in response to the Government Information Security Reform legislation.

Secretary Rumsfeld, in his testimony last month before the House Appropriations Defense Subcommittee, identified six key transformational goals for the Department. Leveraging information technology to create seamless, interoperable network-centric environments is one of those foundation transformational goals.

However, as our dependence on information networks increases, it creates new vulnerabilities, as adversaries develop new ways of attacking and disrupting U.S. forces. In recognition of this dichotomy, the Secretary established the protection of U.S. information networks from attack as another foundation transformational goal.

Emphasizing that transformation is not an event, Secretary Rumsfeld described it as an ongoing process or a journey that begins with a transformed leading-edge force. Mr. Stenbit, the DOD CIO, is committed to support our transformation by providing the power to that information leading edge. To do that, he established three goals for his supporting efforts of Mr. Rumsfeld, and one of those is making the exchange of information available on a network that people depend and trust.

Now all of these goals in large measure are influenced by our ability to provide information assurance to the edge and throughout the entire information enterprise. Our senior leadership's stated commitment to these goals is testament to the importance placed on information assurance within DOD.

The Department initiated work on its 2001 assessment in January 2001. The former DOD CIO, Mr. Art Money, established an IA Integrated Process Team to lead the assessments. In addition, the

DOD IG ensured that independent audits were performed to assess and test DOD programs and policies for effectiveness and compliance with the law and other policies, procedures, standards, and guidelines.

The analysis of the system-specific data and the responses to the OMB questions indicate that DOD has good IA policies, practices, and procedures in place, but needs verification of compliance. Without a capability to enforce and properly audit IA policy compliance, it is difficult to ensure that all systems operate based on up-to-date procedures and proper configurations.

Based on the data analysis, however, it is evident that even for those systems lacking accreditation, most have robust IA measures in place and programs with high IA awareness. DOD has a strong foundation in IA that will be expanded and more fully developed as that program matures.

Without question, though, the biggest single lesson learned during the conduct of GISRA 2001 was the problems associated with our Security Certification and Accreditation Program. Compliance is a major issue. However, stricter audit and enforcement of DITSCAP, which is our Defense Information Technology Security, Certification, and Accreditation Program, stricter audit and enforcement of that will not necessarily rectify the problem. Non-compliance is more a symptom of the complexity of that process and the clarity of its implementing policy. These problems were previously identified, but definitively confirmed in the GISRA 2001 assessment.

That certification and accreditation policy is undergoing dramatic modification in policy as well as in implementation. The DOD policy governing DITSCAP will streamline the certification and accreditation process and provide better clarity on definitions and responsibilities. DOD is also pursuing the use of automated tools to ease the documentation burden on security and systems administrators. The combination of these two efforts should significantly improve our ability to conduct certification and accreditation and, as a result, improve compliance.

DOD, through the Defense Information System Agency, has also aggressively implemented comprehensive connection approval programs for both our Non-Secure and Secret Internet Protocol Router Networks, the SIPRNET and the NIPRNET. These programs have initial and subsequent periodic validation of network certification and accreditation as a precondition for connection to the network, and this will serve as a valuable compliance control mechanism to make sure that those programs are fully carried out.

The DOD IG identified oversight and review of IA policy implementation and programming of funds and resources to support IA as areas requiring attention in the last GISRA assessment. Conduct of worthwhile oversight and review of IA policy implementation requires not only an established process, but also relevant and current IA policy. As mentioned in the IG report, DOD Directive 5200.28 was, or still is, our current security policy, but that happened to be written in 1992 and was woefully out-of-date.

In its place, DOD is issuing a series of new IA directives and instructions to accommodate a more complex IA environment. The capstone directive is in formal coordination now within the Depart-

ment and will be released soon. Other supporting directives have recently been released or will be released later this year. The responsibilities established in these directives are clear and concise, as are the management controls associated with the policies.

Oversight of budgets and programming to support IA is one of the functions of my office, the Defense-wide Information Assurance Program Office. We are now reviewing, with all the DOD components, the services, and the agencies, IA budgets and programs during their development to coordinate efforts across the Department and to check for policy implementation. Subsequent to that, we conduct reviews to match the resource allocations and expenditures with the original plans to make sure that they match.

Now, those were the things we noticed during regular GISRA. However, there were some procedural lessons learned that we also developed. One, as was mentioned previously, was to work closely with the DOD IG in the conduct of GISRA. Unfortunately, during last year's GISRA, we weren't able to do that because of time constraints and previous scheduling problems with the DOD IG. They looked at one small population of DOD systems, and we looked at another population. Optimally, we would have looked, both we would have done an assessment of DOD systems and then the IG would have come behind us and audited the same systems to verify the veracity of the information that we were getting.

Because of that, DOD's Fiscal Year 2002 GISRA assessment efforts will focus on three particular areas. One is review of selected systems from 2001, and then we will go in and take a look at the major DOD networks, and also the third part of that is the departmental response to OMB IA management process questions.

Approximately 168 systems from the 2001 assessment will be reviewed. The second area of this year's effort will focus on a random sample of major local, wide, and metropolitan DOD area networks.

Then the final area in 2001 will be the response to the OMB IA management questions. OMB has indicated that the questions will be similar to those in the 2001 assessment, and will encompass all aspects of IA throughout the Department, from training and awareness to response capability. As DOD components conduct their assessments, the DOD IG will audit the subset of the 168 systems from last year, again, as I said before, to verify compliance and the veracity of the information that we collected.

We in DOD find the GISRA assessments as a valuable tool. Combined with other assessment tools we have—for instance, the Joint Chiefs of Staff Joint Monthly Readiness Reviews, the Commanders-in-Chief's Integrated Priority Lists, Mission Need Statements, and other requirements documents—we are better able to discern what actions and direction are needed to be taken to sustain our IA posture and to transition to a more robust posture. Having identified these necessary actions and directions, we were able to better coordinate more effectively our oversight and coordination of the Department's IA budgets and the entire enterprise-wide program.

That's it, sir.

[The prepared statement of Mr. Gorrie follows:]

Statement by

Robert G. Gorrie

Deputy Director

Defense-wide Information Assurance Program Office,

Assistant Secretary of Defense for

Command, Control, Communications and Intelligence

Before the

House Government Reform Committee

Subcommittee on

Government Efficiency, Financial Management and

Intergovernmental Relations

Hearing on

Lessons Learned from the Government Information Security Reform Act of 2000

March 6, 2002

For Official Use Only

Until Release by the

Committee on Government Reform

U.S. House of Representatives

Thank you Mr. Chairman and members of the Subcommittee. I am honored to be here and pleased to have the opportunity to speak with your committee about lessons the Department of Defense (DoD) has learned from assessments we conducted in response to the Government Information Security Reform (GISR) requirement of the Floyd D. Spence National Defense Authorization Act for FY2001. I believe we have and continue to make significant progress in our quest to secure and defend our computer networks. Today's testimony will highlight some of the efforts we've initiated over the past year and the challenges ahead in achieving Information Assurance (IA) within the Department.

Secretary Rumsfeld, in his testimony last month before the House Appropriations Defense Subcommittee, identified six key transformational goals for the Department around which we will focus our defense strategy and develop our force. Leveraging information technology to create a seamless, interoperable, network-centric environment is one of those foundation transformational goals. The opportunities to give U.S. forces unparalleled battlefield awareness are impressive- if they can "see" the entire battlefield and the enemy cannot, their ability to win wars grows exponentially. However, as our dependence on information networks increases, it creates new vulnerabilities, as adversaries develop new ways of attacking and disrupting U.S. forces. In recognition of this dichotomy, the Secretary established the protection of U.S. information networks from attack as another foundation transformational goal.

Emphasizing that transformation is not an event, Secretary Rumsfeld described it as an ongoing process, a journey that begins with a transformed "leading edge" force, which, in turn, leads the U.S. Armed Forces into the future. Mr. Stenbit, DoD CIO, is committed to support our transformation by providing the power of information to that leading edge. To bring power to the edge, he established three goals for his supporting effort: make the exchange of information available on a network that people depend and trust; populate that network with dynamic sources of information to defeat the enemy; and deny the enemy those same advantages by exploiting his weaknesses. These goals, in large measure, are influenced by our ability to provide information assurance to the edge and throughout our entire information enterprise. Our senior leadership's

stated commitment to these goals is testament to the importance placed on Information Assurance within DoD.

The Department initiated work on GISR 01 in January 2001. The former DoD CIO, Mr. Art Money, established an IA Integrated Process Team (IA IPT) to evaluate and consolidate component assessments of the adequacy and effectiveness of Department IA policies, procedures, and practices, including testing the implementation for a subset of DoD systems. In addition, the DoD Inspector General (IG) ensured that independent audits were performed to assess and test DoD programs and policies for effectiveness and compliance with the law and other policies, procedures, standards, and guidelines.

Optimally, the IA IPT and the DoD IG would have evaluated and audited systems chosen from a common pool. Time available for planning and scheduling, and the nascent nature of the effort, however, resulted in the IG providing assessments based on their own evaluation criteria rather than an audit of the IA IPT GISR efforts. The IG's review differed from the IPT's in its approach to what was actually evaluated. The IPT selected a sample of 560 systems from the almost 4,000 systems listed in the DoD Information Technology (IT) Registry while the IG started with a universe of 4,939 applications, supported by the Defense Information Systems Agency (DISA) at certain Centers and Detachments. Of these, the IG assessed 90. The IG evaluated these 90 applications for Certification and Accreditation (C&A) and Interim Authorities to Operate (IATO). The IPT evaluated for C&A and IATO but additionally assessed its sample of systems from the IT Registry for other security measures in part based on the National Institute of Standards and Technology (NIST) Security Self-Assessment Guide for Information Technology Systems.

The analysis of the system-specific data and the responses to the OMB questions indicate that DoD has good IA policies, practices, and procedures in place but needs verification of compliance. Without a capability to enforce and properly audit IA policy compliance, it is difficult to ensure that all systems operate based upon up-to-date procedures and proper configurations. Based on the data analysis, however, it is evident that even for those systems lacking accreditation, most have robust IA measures in place and program managers with high

IA awareness. DoD has a strong foundation in IA that will be expanded and more fully developed as this capability is matured.

The IPT categorized information systems into two groups: Mission Critical if loss of the system would cause the stoppage of or affect the direct mission support of warfighter operations; and Mission Essential when the acquiring Component head designates it as basic and necessary for the accomplishment of the organizational mission. Sixty-nine percent of the evaluated DoD systems had an Accreditation or an IATO. Almost 90% of the accreditations and IATO were current (based on the DoD standard of 3 years for accreditations and 1 year for IATO). Another 6% listed accreditation as "in progress." Eighty-one percent of Mission Critical systems had accreditation or IATO compared to 63% of Mission Essential systems.

Accreditation statistics alone are not completely representative of measures taken to secure DoD Information Systems. Also included in the evaluation were questions about specific security related measures that have been taken without regard to accreditation status. Generally, it was apparent that a great majority of reported systems have significant protection measures in place.

Components reported the following affirmative results regarding protection of systems:

- Positive Security Measures:
  - access controls – 97%
  - physical security – 97%
  - administrative controls – 96%
  - personnel security measures – 94%
  - security incident response capability – 87%
  - boundary protection – 83%
  - intrusion detection system – 65%
  - data integrity – 94%

- IA Relevant Plans:
  - hardware/software maintenance plan – 92%
  - existence of contingency plan – 81%

- exercise of contingency plan– 31%
- risk management plan – 79%
  - system security plan – 78%
  - system life cycle plan – 74%

- IA Compliance and Testing Mechanisms
  - connection approval – 77%
  - Information Assurance Vulnerability Alert (IAVA) compliance – 66%
  - Red/Blue team – 25%

In addition to the assessment of specific systems, components were required to answer fourteen questions based on the GISR legislation and OMB Circular A-11. These questions addressed the existence and implementation of DoD IA policy and procedures. Responses to two particular questions indicated areas requiring attention. Responses to the questions obtained by both the IPT and the DoD IG indicate problems with the DoD Information Technology Security Certification and Accreditation Program (DITSCAP), specifically in the areas of program compliance, complexity, and clarity. In addition the DoD IG identified oversight and review of IA policy implementation and programming of funds and resources to support IA as areas requiring attention.

Without question, the biggest single lesson learned during the conduct of GISR 01 was the problems associated with our Security Certification and Accreditation Program. Compliance is a major issue. However, stricter audit and enforcement of DITSCAP compliance will not rectify the problem. Non-compliance is more a symptom of the complexity of the DITSCAP process and clarity of its implementing policy. These problems were previously identified but definitively confirmed in the GISR 01 assessment.

The DITSCAP is currently undergoing dramatic modification in policy as well as implementation. The DoD policy governing DITSCAP will streamline the certification and accreditation (C&A) process and provide better clarity on definitions and responsibilities. DoD is also pursuing the use of automated tools to ease the documentation burden on security and

systems administrators. The combination of these two efforts should significantly improve our ability to conduct C&A and as a result improve compliance. DoD through DISA has also aggressively implemented comprehensive connection approval programs for both the Non-secure and Secret Internet Protocol Router Networks (NIPRNET/SIPRNET.) Those programs have initial and subsequent periodic validation of network C&A as a precondition for connection approval. This will serve as a valuable compliance control mechanism.

The DoD IG's identification of oversight and review of IA policy implementation and programming of funds and resources to support IA as areas requiring attention is another lesson learned. Conduct of worthwhile oversight and review of IA policy implementation requires not only an established process but also relevant and current IA policy. DoD Directive 5200.28 identified by the IG in its report is out of date. In its place, DoD is issuing a series of new IA directives and instructions to accommodate a more complex IA environment. The capstone directive is in formal coordination within the Department and will be released soon. Other supporting directives have recently been or will be released later this year. The responsibilities established in these directives are clear and concise, as are the management controls.

Oversight of budgets and programming to support IA is one of the functions of the Defense-wide IA Program (DIAP) office. We are now reviewing, with all DoD components, IA budgets and programs during their development, to coordinate effort across the Department and check for policy implementation. We conduct subsequent reviews to match resource allocation and expenditures with the original budget plans.

In addition to the lessons learned about the IA posture of our information enterprise, we have also learned valuable procedural lessons concerning the conduct of GISR assessments. As mentioned previously, the IA IPT and the DoD IG examined systems from different populations. We were also late in our strategy development and planning, waiting for definitive guidance to help shape our effort. Building on our experience from GISR 01, we initiated strategy development and planning for GISR 02 immediately after the completion of the GISR 01 report in October 2001. The IA IPT and the DoD IG worked in concert to produce a strategy and plan that integrates the efforts of the IPT and the IG.

DoD's FY02 GISR assessment effort will focus on three major areas: review of select systems assessed in FY01, assessment of a sample of major DoD networks, and Departmental response to OMB's IA management process questions. Approximately 168 systems from the FY01 assessment will be reviewed. The second area of this year's effort will focus on assessment of a random sample of major (Local, Wide, and Metropolitan Area) DoD networks. The final area of the FY02 GISR assessment is the response to Office of Management and Budget (OMB) IA management questions. OMB has indicated that the questions will be similar to those in the FY01 assessment and will encompass all aspects of IA throughout the Department from training and awareness to response capability. As DoD components conduct their assessments, the DoD IG will audit a subset of the 168 systems brought forward from last year's assessment.

GISR assessments are a valuable tool. Combined with other assessment tools (Joint Chiefs of Staff Joint Monthly Readiness Reviews (JMRR), Commanders-in-Chief (CINC) Integrated Priority Lists, Mission Need Statements, requirements documents, etc.) we are better able to discern what actions and direction are needed to sustain the IA posture of our information infrastructure and position ourselves to transition to a more robust posture. Having identified necessary actions and direction we are better able to conduct more effective oversight and coordination of the Department's IA budgets and enterprise wide program.

Mr. HORN. Thank you very much. I want to ask you about the role of Mr. Stenbit. Now he is Assistant Secretary for the three C's—Command, Communications, and what else is it?

Mr. GORRIE. Command, Communications, and Control and Intelligence.

Mr. HORN. Control and Intelligence?

Mr. GORRIE. Yes, sir, and he is also the DOD CIO.

Mr. HORN. Yes. Now is that too much for one person to handle?

Mr. GORRIE. No, sir. Actually, it is probably a pretty good combination because not only does he see or oversee the policy and the budgetary parts of IT within the Department, but then, again, as the CIO of DOD, that gives him a more pervasive view not only of the programming and budgeting aspect and bringing new systems on board, but getting into the daily operational things that go on within the Department.

Is it too big of a job to handle? No. I mean, he obviously has staff to deal with his CIO functions and also with his Assistant Secretary functions, but to have that all brought together in one person is valuable, because you get to see not only the policy development and also the procurement side of it, but also the operational side of it.

Now there are people who would disagree with that and say that we should split this function and have a separate DOD CIO and a separate Assistant Secretary for Command, Control, Communications and Intelligence. The jury is still out on that. I don't personally subscribe to splitting those responsibilities, but until I become the Secretary, I won't be able to make that decision, sir. [Laughter.]

Mr. HORN. Well, I would like a little table with little boxes as to how many people we have for those various functions. I have gone through this with another agency 5 or 6 years ago. They piled everything onto what Congress had said about Chief Financial Officers, Chief Information Officers, and the thrust of that was to get somebody of high-rank that we could get in the private sector or in the executive branch out of the Senior Service. We just looked at it, and not much was happening because the poor soul was overloaded.

So I would like a chart at this point in the record. Without objection, it will be put there. So if you and everybody else can give us one, just so we can see the picture of who's helping and how many are helping and addressed to this?

Mr. GORRIE. Yes, sir.

And if I might add one other reason why I don't think you necessarily want to separate those functions is because the level—if you split those functions, I don't know that necessarily the level of importance of the person holding that job would carry enough sway within the Department to have influence. At the Assistant Secretary level—and, actually, I think it should be at the Under Secretary level, but, again, I am not in a position to make that call—there is enough leverage there, and they have enough influence and the ear of the Secretary of Defense to make things happen. If you split it and diluted it, that might not necessarily be the case.

Mr. HORN. I have great admiration for the Secretary of Defense. I remember, going back about seven administrations, one person

had about 12 of the functions we now have Assistant Secretaries hold. As you know, he did a very fine job. But when we have troubles in this area, where we haven't had it yet up where they can get a C, B, or A in looking at the computing operation, it just means we have got to focus on that and not be waylaid by all the other things that are very important.

Mr. GORRIE. Yes, sir.

Mr. HORN. OK, so we now have our last presenter, Chief Information Officer Karen S. Evans of the U.S. Department of Energy.

Glad to have you here. When were you appointed? I see January 28th.

Ms. EVANS. Yes, sir, just 6 weeks ago.

Good morning, and thank you for this opportunity to appear today to address the very important issue of improving the security of our Federal information systems. I was named the Department of Energy's Chief Information Officer 6 weeks ago, on January 28, 2002. As the CIO, I believe that effective cyber security is a balance of managed policies, procedures, technology, training, and people. It is also a major enabler of our Department's information technology initiatives, especially our e-government initiatives.

My remarks today focus on the implementation of the Government Information Security Reform Act, improvements in the Department's cyber security infrastructure, and our plans for further strengthening our cyber security posture.

GISRA provides a comprehensive framework for establishing and ensuring effectiveness of security controls over information resources that support Federal operations and assets. Secretary Abraham submitted the Department's first annual security review last September. This committee established grading criteria, and the Department received an "F."

The scoring acknowledged that we were either complete or in the process of implementing 9 of 10 areas. Our raw score was 71. The score was weighed against weaknesses identified by our previous Department Inspector General and the Office of Independent Oversight and Performance assurance audits and assessments. Our final scoring was lowered to 51.

Since the passage of GISRA, the Department has taken an active leadership role to further strengthen its cyber security posture. First, we developed and incorporated an enterprise-wide perimeter defense strategy to reduce the number and the severity of successful attacks. Analysis reveals that while the overall threat from virus and malicious code increased, the number of successful intrusions diminished. Virus and malicious code incidents dropped from 60 in fiscal year 2000 to 39 in fiscal year 2001, a 35 percent reduction. In addition, while probes and scans escalated over 2,000 percent from fiscal year 1999 to 2001, unauthorized access and Web defacements diminished by over 50 percent.

In addition, we have trained 6,200 managers and cyber security staff in the last year alone, and are continuing an aggressive training and awareness program, so that every Department member is aware that cyber security is an integral part of his or her job.

Like many other government agencies, we still have a long way to go, but we have an excellent foundation on which to build. We recognize the importance of cyber security as a management issue.

Our goal is to give line management the authority to determine how to implement policy, because it is in the best position to assess the appropriate levels of protection.

Our Performance Improvement Plan and Performance Report Card provide a clean remediation road map for those program offices with GISRA-identified deficiencies, and our sites have made significant progress toward their elimination.

Today I am pleased to announce additional cyber security initiatives. First, I will focus initially on developing and implementing a Department-wide certification and accreditation process to ensure that our unclassified information systems comply with departmental cyber security policies. Our Certification and Accreditation Program will establish a Department-wide process to certify that an information system or a site complies with documented security requirements, and that the program will continue to maintain an accredited security posture throughout the system life cycle.

Processes such as certification and accreditation are insufficient without adequate risk-management and configuration management directives. The Department has identified some shortcomings in its approach in both areas, and I am committed to developing directives in these areas.

The Department is also committed to protecting our national critical and mission-critical assets. As one of the first five agencies to complete the Critical Infrastructure Assurance Office Project Matrix Step One, we now have a comprehensive list of our most critical assets, which we used to focus our enhanced protection efforts.

In addition, I am committed to implementing a robust, independent validation and verification process to provide an additional objective level of assurance regarding the continuity of operations for all of Department of Energy's mission-critical cyber assets.

The Department has also initiated a renewed IT capital planning process to manage the cost of acquiring and maintaining IT assets. We are improving that process to ensure the seamless integration of security into each system's lifecycle costs. Although each of these efforts is only a part of our cyber security program, together they are effective tools to protect the Department's critical information assets. They will also serve as enablers for our electronic government efforts.

I am intent on making the Department a national center of excellence for safeguarding classified and unclassified information on electronic systems. This will be accomplished through three objectives: strengthening the Department's cyber security community, ensuring a Department-wide risk-based approach to cyber security implementation, and enhancing protection of our internal cyber assets, especially our nationally critical and mission-critical assets.

As CIO, I have been given programmatic authority to provide management oversight of the Department's cyber security program through the use of information technology capital planning and investment process. Our Performance Improvement Plan and Performance Report Card clearly communicate the status of identified issues of concern. This plan builds upon the foundation provided by GISRA and fosters solution-sharing within the enterprise.

Our performance metric program provides us feedback on key elements for a healthy cyber security program. I am moving for-

ward to strengthen our approach to risk and configuration management; implement a comprehensive certification and accreditation process, and an independent validation and verification process. With these initiatives, I am confident that the Department will continue to strengthen its cyber security posture.

Success in this area takes continued and focused efforts due to the increasing complexity of threats and the rapid evolution of technology. We at the Department are committed to meeting this challenge.

Mr. Chairman, this concludes my statement, and I would be happy to answer any questions.

[The prepared statement of Ms. Evans follows:]

Statement of Karen S. Evans
Chief Information Officer

U.S. Department of Energy

Before the

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

Committee on Government Reform

U.S. House of Representatives

March 6, 2002

Mr. Chairman and Members of the Subcommittee:

I want to thank you for this opportunity to appear today to address the very important issue of improving the security of our federal information systems.

I was named the Department of Energy's (DOE) Chief Information Officer on January 28, 2002. As CIO, I believe that effective cyber security is a balance of managed policies, procedures, technology, training, and people. I also believe that cyber security is a major enabler of our Department's information technology (IT) initiatives, especially our e-government initiatives. Although I have been at DOE for a very short period of time, I cannot emphasize strongly enough how important cyber security is for protecting the Nation's and Department's critical information assets.

My remarks today will focus on the implementation of the Government Information Security Reform Act (GISRA), improvements in the cybersecurity infrastructure at the Department, and our plans for further strengthening our cyber security posture.

GISRA Implementation

The purpose of GISRA is to provide a comprehensive framework for establishing and ensuring effectiveness of security controls over information resources that support Federal operations and assets. Secretary Abraham submitted the Department's first annual security review on September 7, 2001 in response to GISRA requirements and Office of Management and Budget guidance. The Committee established grading criteria and based on the application of these criteria, the Department received an "F". The

scoring by the Committee showed that we received a full score in the areas of budgeting, control of contractor's services, and training. The scoring also gave us credit for partial implementation of our performance metrics program, incident reporting and response program, critical asset identification, and capital planning program. The Committee found it difficult to determine whether the Department had integrated information and information technology with our critical infrastructure protection program. Our raw score was 71. This was weighed against the analysis of issues identified by our Inspector General and the Office of Independent Oversight and Performance Assurance through a review of past audit and assessments and our final score was lowered by 20 points.

While we have made good progress over the past two years, we still have a long way to go. It is on that basis that I will present what we have done and what we are doing to further improve our information asset security.

Marked Stages of Improvement

Since the passage of GISRA, the Department has taken an active leadership role and made significant progress in strengthening the department's cybersecurity posture.

First, we have developed and incorporated an enterprise-wide perimeter defense strategy to reduce the number and severity of successful attacks. Our incident response program clearly shows that our investment in this strategy has had a significant and positive impact. Analysis of DOE data reveals that while the overall threat from virus and malicious code has increased, the number of successful intrusions has diminished. For

example, virus and malicious code incidents have dropped from 60 in fiscal year (FY) 2000 to 39 in FY2001, a 35% reduction. In addition, while probes and scans have escalated by over 2,000 percent from FY1999 to FY2001 (2,317 to 45,444), unauthorized access and web defacements have diminished by over 50% (130 to 64). The number and severity of malicious code infestations has lessened significantly as the department has implemented this strategy to include training our users. Since no program can be successful unless people have been properly trained and are aware of new threats and vulnerabilities, we have trained 6,200 managers and cyber security staff in the last year alone. We are continuing an aggressive training and awareness program so that every member of the DOE infrastructure is aware that cyber security is an integral part of his or her job.

Second, the Department has strengthened the implementation of cybersecurity controls of unclassified, sensitive unclassified and classified systems at our weapons laboratories. A congressionally mandated "Red Team", has tested the bottom-line effectiveness of the Department's cyber security program at these facilities and conducted penetration tests in an attempt to find and exploit security "holes." This team, composed of some of the most preeminent government security experts, was unable to penetrate any sensitive unclassified or classified systems.

On the technology front, the department has instituted several internal software development efforts to boost the level of cyber system protection. DOE's Safepatch, an automated security patching program for information systems, provides enhanced

network monitoring and sophisticated data mining tools to correlate activity to detect potential intrusion attacks. This tool is being used within the Department of Justice, Health and Human Services, and other government departments and agencies to ensure that critical systems are kept up to speed. Another Department developed software tool, the Network Software Detection (NID), protects the network security perimeters at the Department and is utilized at the FBI, Department of Transportation and 15 other federal departments and agencies.

Like many other Government agencies, we still have long way to go, but we have an excellent basis on which to build. We have recognized the importance of cyber security as a management issue. Among our objectives are a clear definition of the roles and responsibilities for line management. Our goal is to give line management the authority to determine how to implement policy. We believe that line management has the greatest insight as to the level of protection that is required for the assets for which they are responsible. Our Performance Improvement Plan and Performance Report Card, our most recent management innovations, provide a clear remediation roadmap for those DOE Program Offices with GISRA-identified deficiencies and our sites have made significant progress toward their elimination.

Our Goals

Today, I am pleased to announce additional cyber security initiatives. I will focus initially on developing and implementing a DOE-wide certification and accreditation process to ensure that our unclassified information systems comply with departmental cyber security

policies. We already have an effective certification and accreditation process to protect DOE's classified cyber security assets.

Our certification and accreditation program establishes a department-wide process to certify that an information system or site complies with documented security requirements and that the program will continue to maintain an accredited security posture throughout the system life-cycle. Certification and authentication is founded upon sound risk management processes, which aides in determining the protection requirements for the information stored or processed on the DOE information system.

My commitment to you and the public is to make executive management accountable for all information systems, both classified and unclassified. Processes such as certification and accreditation are insufficient without adequate risk management and configuration management directives. DOE has identified some shortcomings in its approach in both areas. I am committed to developing directives in these areas.

The Department is also committed to protecting our national-critical and mission-critical assets. As one of the first five agencies to complete the Critical Infrastructure Assurance Office Project Matrix Step 1, we now have a comprehensive list of our most critical assets. We are committed to enhancing the protection of these assets and will use the Project Matrix results to focus our enhanced protection efforts.

In addition, I am committed to implementing a robust independent validation and verification process. This process provides an additional, objective level of assurance that ensures continuity of operations for all of DOE's mission-critical cyber assets.

The Department has initiated a renewed IT capital planning process to manage the cost of acquiring and maintaining IT assets. We are improving that process to ensure the seamless integration of security into each system's lifecycle costs. Although each of these efforts is only a part of our cyber security program, together they are effective tools to protect the Department's critical information assets. They will also serve as enablers of our electronic government efforts, another primary interest of mine.

I am intent on making the Department a national center of excellence for safeguarding classified and unclassified information on electronic systems. This will be accomplished through three objectives: strengthening DOE's Cyber Security Community, ensuring a DOE-wide risk-based approach to cyber security implementation, and enhancing protection of our internal cyber assets, especially our nationally-critical and mission-critical assets.

Conclusion

As CIO, I have been given programmatic authority to provide management oversight of DOE's cyber security program, through the use of the information technology capital planning and investment process. Our Performance Improvement Plan and Performance Report Card clearly communicate the status of identified issues of concern. This Plan

builds upon the foundation provided by GISRA and fosters solution sharing within the DOE enterprise. Our performance metric program provides us feedback on the key elements for a "healthy" cyber security program. I am moving forward to strengthen our approach to risk and configuration management; implement a comprehensive certification and authentication process, and an independent validation and verification process. With these initiatives, I am confident that the Department will continue to strengthen its cyber security posture.

In conclusion, we know there is no simple solution for cyber security. Success in this area takes continued and focused efforts due to the increasing complexity of the threats and the rapid evolution of technology. We at the department are committed to meeting this challenge.

Mr. HORN. Thank you very much. We appreciate your presentation.

We are now going to go down the line for a few questions. I would like all of you to give us some information on them.

The question basically is, are there adequate standards and known best practices to implement an effective information technology security program, especially for the CIOs, as to where that source is. Is it OMB? Is it GAO, so forth?

Mr. Dacey.

Mr. DACEY. Let me answer that question at two levels. I think we have some guidance at GAO with respect to overall security management programs. I have included that as best practices from leading organizations for security management programs and for risk-assessment.

With respect to more details controls, I think there isn't consistent information out there. There is a lot of good information in industry, and there is a lot more being developed. I would say that NIST, a combination of NIST and the NSA, through the NIIAP, another organization, and some others, are starting to develop more detailed policies. These have been received fairly well for those who are trying to implement security in their systems. So it is, again, at two levels: one at the management level and one at the detailed standards level.

Mr. HORN. Mr. Forman.

Mr. FORMAN. I think the focus is wrong there. I think there are a plethora of standards, best practices tools. I think you have got to go beyond the United States and look at what the U.K. has done and other countries.

The reality that we are working in, the environment that I am trying to bring about here, has to operate as fast as the Internet. Traditional bureaucratic processes simply will not give us the security we are looking for. We have—and I will lay out some of the elements of the puzzle—threat data aggregation, NIPC at the FBI, FedCirc for the Federal Government, Cert at Carnegie-Mellon, the Sands Institute, the National Security Agency, organizations within the Defense Department.

So if there is a threat on the Internet and it moves at Internet speed, by the time any one of these organizations finds out about it and puts out an alert, you or I may hear about it on WTOP coming into the office in the morning. That is a day.

We are talking about, on the other hand, an annual process with GISRA. We are moving to a quarterly process to oversee the management by the President's Management Council for Security Management. At once I feel, yea, finally, after for me 12 years of trying to get management attention, we've got the management attention; we've got a terrific set at both the policy levels and the technology levels of standards from NIST, from NSA, from DOD, and others. Those standards are adequate to do what we need to do for the management policy, but they are inadequate to address some of the major issues within the Internet in regards to vulnerabilities.

We need to look at how we put in place a process, not standards. If, in the end, we want fast identification of threats, fast remediation of vulnerabilities, we need to make sure that we are providing for that infrastructure. I fear the path we are going on right

now is identifying people who are accountable, identifying visible sets of metrics and are they following them? If so, the potential exists to ignore the fact this stuff is moving in hours or days, not months, quarters or years.

In essence, this is what we are trying to bring about with the Critical Infrastructure Protection Board. The process needs threat data aggregation. It needs vulnerability assessment. We have to make some decisions as a country about the remediation and deployment of remediation. In other words, is that going to be industry-driven or government-driven? I fear that the type of structures we put in place for Y2K, from a bureaucratic standpoint, won't work now.

So, clearly, all of that is evolving, and we are working through that. But, by the same time, there is this issue of enterprise security issue, and that has been the focus of GISRA. That has been the focus of many people at this table as well as many of our staff in the back for well over a decade. There we have made the progress.

I would rather see the focus being on, "What do we need to be successful at Internet time" than, "How do we continue down this path of enterprise security management in a bureaucratic process?"

Mr. HORN. You mentioned that there were certain nations that would seem to be ahead of us in some of these areas. Could you give us a feeling for that?

Mr. FORMAN. I wouldn't say necessarily ahead of us in the sense that they have done a better job, but had some perhaps more complete or some accepted standards. I think the U.K was one of those. I know when I was at IBM, we used the U.K. standard for our security audits that we did in a number of industries. Since then, of course, NIST has, I believe, widely recognized, has put together a much broader set of standards from the technology level to the management level, which now many of the CIOs adopted. We didn't have that 2 years ago.

Mr. HORN. Dr. Bement, how do you feel about what's happening abroad that we might use in our own administration?

Dr. BEMENT. Well, in this area I think our current standards and accepted best practices are current and will put us in good standing, but it's very dynamic. The technology is changing rapidly. So we have to continually review these standards. Also, our risk models need to be changed as we get new threat information. So we have to keep on top of that.

But we have cross-cutting alliances with Canada, with the U.K., and many other countries in the work that we do.

Mr. HORN. How about Australia?

Dr. BEMENT. Pardon me?

Mr. HORN. How about Australia? Or New Zealand? I mean, they've got a particularly different government.

Dr. BEMENT. I think all the members of the Coordinating Committee are very closely coupled with the work that we do, and Australia, New Zealand, Canada, the U.K. would be included in that.

I feel that, apart from the standards and the best practices, and again we're going to come right back again to training, awareness, high-level oversight and compliance, there has to be enforcement of compliance. There has to be critical monitoring, and, of course, peo-

ple really have to continually keep on top of the changes, as Mr. Forman mentioned. I think those are the critical issues.

Mr. HORN. Moving to another country before we finish that part of the question, India produces a tremendous number of very talented people that relate to computing.

Dr. BEMENT. Yes, that is correct.

Mr. HORN. What do we know about India's Government. Many or most of the people probably come to the United States. I don't know if they are within the Government of India, but do you have any thoughts on that?

Dr. BEMENT. I don't know that NIST has strong interactions with India and I don't know that we have a number of citizens from India working at NIST. We may have some. But I am certainly aware of the fact that industry looks to the talent and the capabilities in India and draws on that very actively. Of course, we also interact very much with industry. So indirectly we probably do have some connections.

Mr. HORN. Ms. Gross——

Dr. BEMENT. Oh, Mr. Chairman, may I ask a privilege?

Mr. HORN. Sure.

Dr. BEMENT. I have another hearing in 15 minutes, and if I may, I would like to be excused.

Mr. HORN. Fine, and if we have a couple of questions, we will send them to you, and we will put them in the record at this point.

Dr. BEMENT. I would be pleased to respond to those. Thank you.

Mr. HORN. Fine. Thank you.

[The information referred to follows:]

Questions for Dr. Arden Bement,
National Institute of Standards and Technology

1. Question: What were the results of Federal agencies using the NIST Computer Security Expert Assist Team?

- **Were there any "success stories" you would like to share with the subcommittee?**

Answer: Yes, our initial efforts have been successful and will help improve the security programs at Federal agencies. Let me offer one example. The CIO at FEMA, the first agency reviewed by the NIST CSEAT team, was most appreciative of our efforts:

> " I just wanted to let you know that the NIST CSEAT Team has just finished their review of our Information Security program and given us the draft report. They have done a great job for us. The report is a first-rate product and gives us a very practical guide on how best to apply our limited resources to fix our shortfalls. Of all the reviews and audits we have had done on us or against us, this is the most useful...Good show! "
> *Clay Hollister, CIO FEMA*

The success of our efforts, and the needs of civil agencies for helpful assistance, is one reason that the Administration has called for funding of the CSEAT program next year.

2. Question: What systemic security issues and challenges did the NIST Computer Security Expert Assist Team discover during its work with the agencies?

Answer: Among the many security challenges agencies face are how to effectively:

- implement a comprehensive strategy to build an effective security program;
- integrate security into the system development lifecycle;
- use risk assessment methodology;
- train personnel/contractors on security procedures and responsibilities;
- understand the security risks and benefits of new and rapidly evolving technologies;
- address security in the capital planning processes; and
- identify where best to invest limited security resources to get the highest degree of improvement in their existing security programs.

I would also recommend to you the recently completed OMB report "FY 2001 Report to Congress on Federal Government Information Security Reform", which identified many agency security issues as a result of the GISRA reporting process.

3. Question: What do you see as the most significant barriers to securing Federal information technology resources?

- **What can be done to overcome these barriers?**

Answer: Among the most significant barriers to improving security are: ***Poorly trained staff*** (security personnel, system managers, system users and IT support staff) and ***lack of management support.*** Both seriously undermine agency security. It is important that security be fully integrated into all major agency processes and that agency heads, leading by example, foster a security-conscious culture to reinforce its importance.

To overcome these barriers, certainly more emphasis is needed on training and establishment of formal agency-wide training plans for employees to address training needs by position and role in the organization. Agency management officials who administer security programs (CIOs and agency heads) need to fully understand security requirements and put mechanisms in place to ensure enforcement.

Agencies must also better understand the benefits of using information technology products that have undergone third-part security validation or evaluation. The long-standing research challenges to improve the technical capability to conduct such security analysis on the wide-range of heterogonous information technology products on a timely basis should not be underestimated.

Improvements can also be achieved by more widely applying the process of *certification* (i.e., technical review) and *accreditation* (i.e., management's formal acceptance of risk and approval of system operation) throughout the government. More must be done to educate agencies on what is available to help them in this process. Agencies also need a way to determine if the technical consultants who are assisting in this process have the needed competence. NIST is now in the process of revising its guidance to agencies on certification and accreditation, which we intend to follow with an accreditation program for system certifiers.

Lastly, a strategy for hiring and retaining highly skilled technical staff in government must be implemented since addressing security as technology rapidly evolves grows ever more complex.

Mr. HORN. Ms. Gross, how do you feel about, are there adequate standards and known best practices to implement an effective information technology security program?

Ms. GROSS. I think there are a number of standards that are developing and, if implemented, would make our systems safer. I think you have to talk about human capital. You can have all the policies and all the procedures, but, ultimately, security is a matter of layers. It is policies; it is procedures; it is having the right people. If you don't have the right person as the CIO, you don't have the right people in law enforcement. It doesn't matter that you have an NIPC if the people there are not technical agents or they don't have technicians that know what they are doing.

You can't have this vision of reacting to Internet speed unless you make sure that, in fact, you have the human capital in place. We need to start reacting with Internet speed; about making sure we have the right people in the right places. I think you can get your layers of policies and procedures, but I am not sure we have been good about sharing best practices. You have organizations like SANS to give out some and so does OMB.

I think this focus needs to be done. What are those best practices? You can't have that many "F's" and say that we have people that know what best practices are or know what the right procedures are, or don't have the right people in place.

Mr. HORN. How about your thoughts, Mr. Gorrie?

Mr. GORRIE. Standards and best practices, yes, sir, there are standards and best practices out there, and we use them, but they have to be tailored to specific environments. You just can't run out willy-nilly and pull them out of the blue. The NIST guidance for evaluating systems, NASA, NIST, security configuration, guidance for operating systems, they're all good, but you have to bring them in and build them into your own system and then evolve your own system along the way.

To just elaborate a little bit on what we heard about human capital, the training of people and the problems we have associated with that, people turning over and leaving the service and things like that, that is really more symptomatic of a deeper problem. That is again what was alluded to before, which is the velocity of the technology.

In order for us to be able to track that velocity or track that technology as it moves forward, you are constantly having to retrain people, constantly having to modify operational techniques and procedures to keep up with that. However, as we look at that technology as it progresses along, we find that, in the terms of my boss, it isn't born secure, that security isn't built in from the beginning. That is what needs to be done, not only the technological security, the crypto-algorithms, the built-in entries and detection and things of that nature, but also a systemic view where you have to have security management built into it, too. It can be a very, very secure box, but if you can't put it in the system and be able to manage all these disparate security devices, then you're sort of barking up the wrong tree.

I think Mike Vatis, when he testified before your committee last September, sort of alluded to that problem, that it is not necessarily the training of the people; it is not necessarily the oper-

ational techniques that you employ, is looking ahead to where technology is going and to try to track it. Now that is only part of the problem. You can track technology and try to build in security later, but the better part would be to engineer in security at the front, and not only the security technology, but to enable it to be managed effectively.

Because today we have applications that are point-click, and before you used to have to sit down forever and a day to program these things out. What we need is security and security management that is also point and click, which would remediate some of our training problems, would remediate some of our operational problems, and go a long way to making this big bear of information security a little bit easier to tame.

Mr. HORN. Two weeks ago I was talking about various things with members of the NATO Assembly. Of course, you have a lot of problems in terms of the various countries in the Eastern part of Europe. I wonder, is the CIO role of Mr. Stenbit, do they relate to NATO and different things, where we do a lot of computing?

Mr. GORRIE. Yes, sir. As a matter of fact, one of the reasons I am here today, and not my boss, is that he is in first—not China, somewhere in the Far East, and then going down to Australia and New Zealand. But there is a very large international play in the ASDC3I and in the CIO, too.

One, interface with the five I's, which are the five English-speaking nations, the United States, the U.K., Canada, New Zealand, and Australia. But then even further than that, in through all the NATO subcommittees that we sit on, and then the Partnership for Peace People, and all the other people that it is expanding to, and then actually to even third-party countries to make sure that, when we need to go somewhere, that we have not only infrastructure support, but infrastructure support that has high availability, security, and some confidence that there isn't anybody prowling around in that infrastructure.

Mr. HORN. On Y2K, and now on this, where computing is a major factor, it comes up under Department of Defense, and they didn't do too well overall. When they have a lot of other things there besides the services. My instinct was that the Air Force was way ahead of the father, namely, the DOD, and we would have been giving them an "A" and still giving a "D" to the other groups, like Logistics and Procurement.

I just wonder, is there a way to get the pressure so that the services that are doing well with CIOs—and maybe my instinct is wrong; you're on top of it, but I just think sometimes we ought to put the "A's" there if they are doing "A" work.

Mr. GORRIE. I don't know if I can address that, sir. I mean, I work with not necessarily the CIOs, but their IA underlings. I don't know if I am qualified to answer that question.

Mr. HORN. Well, if you could get me an answer, I would like to know that——

Mr. GORRIE. Yes, sir, I will.

Mr. HORN [continuing]. Because we ought to see the breakdown by the services and make sure that they are moving along on a path, and they aren't just off in a corner.

Mr. GORRIE. From that particular perspective, sir, at least as far as IA goes, and that is my area of responsibility, so the only thing that I can talk to, you have each of the services—at least about 3 years ago, when I was on the Joint Staff, there were certain services that excelled in particular areas. For instance, the Air Force was far ahead of the Navy and the Army in terms of its ability to do intrusion detection, consolidated intrusion detection, across the enterprise. Such is not the case now. They have pretty much become even-keeled, because of the sharing of best practices and being able to go in and audit the capabilities for the individual services to do those things and then to apply resources for those services and actually prod them along to come about a little bit better.

Things like information assurance vulnerability alerts, where we find out that there is a particular vulnerability in a piece of equipment or piece of software, those things are starting to become enterprise-wide endeavors, and not strictly limited to the services. The services have realized that in order to be successful in this world, that they have to exercise enterprise-wide solutions and not just limit them strictly to services, because they are all vulnerable. They all ride the basic backbone network. They all, both security and non-secure, know that if they are going to succeed, that they have to cooperate, and by and large they are cooperating.

So from that perspective, the IA perspective, I do not see a great disparity in the capability of either the Air Force, the Army, or the Navy, or, as a matter of fact, across any of the agencies. We have endeavored, like I said before, to try to enforce enterprise-wide solutions rather than stovepipe solutions within the services.

Mr. HORN. If you would, just for the record, on IA, could you spell it out?

Mr. GORRIE. Information Assurance. I'm sorry, sir.

Mr. HORN. OK, and that's your office basically?

Mr. GORRIE. The Defense-wide Information Assurance Program Office, yes, sir.

Mr. HORN. Yes. Is that the way most of the agencies have——

Mr. GORRIE. Federal agencies or?

Mr. HORN. Yes, Federal.

Mr. GORRIE. I don't know that. The DIAP, or Defense-wide Information Assurance Program Office, was mandated in legislation, and I can't think off-the-top-of-my-head what that was, but it was in 1998, where the Secretary was told, "You will have a defense-wide information assurance program," and a year after that's when the office that I belong to was formed. Now whether or not that is as pervasive across all of the other Federal agencies, I can't speak to that, sir.

Mr. HORN. OK, thank you. That was Secretary Cohen that put that mandate in.

Mr. GORRIE. Yes, sir.

Mr. HORN. Yes, well, he was very knowledgeable in that area, as a Member of the Senate.

Ms. Evans, any thoughts on best practices? Because you have put a lot of emphasis on it.

Ms. EVANS. Yes, I did. It is my opinion that we do have adequate standards and that there are best practices available today for a

good security program. In many cases a lot of the best practices are obtained currently from our National Laboratories, and they are being used by other Federal departments and agencies.

The Department itself does use the NIST standards best practices for our own classified systems, and we use the Committee on the National Security Systems for best practices for our classified systems. But I believe to have an effective security program, it is a discipline that needs to be practiced every day, and it has to be incorporated into the daily operations.

So a lot of the comments that have been made by my esteemed colleagues here I support all the way down the line, in that as a CIO I need to incorporate that for the Department as a whole, so that it is practiced on a daily basis, so that we can effect remediation in Internet time, when a vulnerability is identified.

Mr. HORN. Well, thank you. That is very helpful.

Let me ask just a few more questions, and then we will call it a day.

Ms. Gross——

Ms. GROSS. Yes?

Mr. HORN [continuing]. You've got a very active record, through the President's Council on Integrity and Efficiency, in helping both the agencies and Inspectors General implement the—excuse us. [Bells are ringing.] How many minutes? Ten? It is 9 minutes to go.

You can see you are about to be released by the votes. This would be a great place if it wasn't for all the votes, you know. [Laughter.]

You have given us some very good testimony. So, Ms. Gross, helping both the agencies and the Inspectors General implement the government information security reform provisions, I was just interested; you have been active in this. You have helped in that. What challenges do you see for Inspectors General expanding their annual evaluations to encompass all agency systems?

Ms. GROSS. I think the challenges for the Inspectors General are to make sure that there is implementation with agreed-upon recommendations, but I think a wider perspective than just the narrow, let's do the next GISRA report, which is very time-consuming and very resource-intensive, is to make sure that they are focusing on issues governmentwide. I think that it is very important that the individual Inspectors General go back into the PCIE, which is the IGs' group, and look to see both best practices and also look to see about how can they help. Since the President is going to have an initiative with e-government, IG's need to make sure that information will be available, that it will be secure, and that it will have integrity. Unless the IGs move out governmentwide and look past their own agencies, I think we are going to have a problem. So that would have been my thrust.

Mr. HORN. Well, thank you.

Mr. Forman, has your office considered imposing mandatory security standards and requirements on Federal agencies?

Mr. FORMAN. Requirements we have; we will continue to do that, and we will tighten that up. Standards we rely on NIST, under the Computer Security Act for Federal information processing standards.

There is another area where some people would call them standards, but they are architecture elements that are agreed upon. They are not technology standards at the NIST or FIPS level. For that, we have orchestrated—and I have actually done some changes in my role as directing the CIO Council. We have the Architecture Committee, which focuses on this. Lee Holcomb, the CIO at NASA, chairs it. John Gilligan, who had been chairing or co-chair of the Security Committee is now co-chair of the Architecture Committee. It is through that I believe we can be most successful.

There is a final element, which is, how do we get patches out rapidly when major threats are identified? That is an area where we need to rapidly get in touch with at least 40,000 people. So I am making increasing use of FedCirc for that.

Mr. HORN. Well, I want to thank the following people that prepared this hearing: J. Russell George, staff director and chief counsel, standing-up back there; and Bonnie Heald, deputy staff director; Claire Buckles, on my left, a very fine professional staff member on loan to us. And thank you.

Earl Pierce, professional staff, isn't here today, and then Justin Paulhamus, majority clerk, is with us doing a great job. He just came in with us. And Michael Sazonov, subcommittee intern, and our court reporter, Joan Trumps. Thank you very much, and thanks to all of you.

If we might, I think we will send you a few questions, and put them at this point in the record.

So, unfortunately, I have got to get over there and vote. We are adjourned.

[Whereupon, at 12:01 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]

[Additional information submitted for the hearing record follows:]

United States General Accounting Office
Washington, DC 20548

April 16, 2002

The Honorable Stephen Horn
Chairman, Subcommittee on Government Efficiency,
Financial Management and Intergovernmental Relations
Committee on Government Reform
House of Representatives

Subject: *Information Security: Subcommittee Post-Hearing Questions Concerning the Additional Actions Needed to Implement Reform Legislation*

This letter responds to your March 26, 2002, request that we provide answers to questions relating to our testimony of March 6, 2002.[1] In that hearing, we discussed efforts by the Office of Management and Budget (OMB), 24 of the largest federal agencies, and these agencies' inspectors general to implement requirements and report evaluation results according to provisions for Government Information Security Reform (the reform provisions) that were enacted as part of the National Defense Authorization Act for Fiscal Year 2001.[2] Your questions, along with our responses, follow.

1. *Do you agree with OMB's assessment of the top six security weaknesses within the Federal agencies? Why or why not?*

We agree that the six security weaknesses OMB identified in its report to the Congress represent significant deficiencies in federal departments' and agencies' information security programs. Specifically, these are (1) a lack of senior management attention to information security; (2) inadequate accountability for job and program performance related to information technology security; (3) limited security training for general users, information technology professionals, and security professionals; (4) inadequate integration of security into the capital planning and investment control process; (5) poor security for contractor-provided services; and (6) limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

However, as OMB indicates, for the most part, its report focuses on management issues, not those of technical or operational implementation. As pointed out in my written statement, our analyses of the reports submitted to OMB by 24 of the largest federal agencies and their inspectors general showed that there are other key security requirements of the reform provisions that agencies have not fully implemented, such as those that require periodic risk assessments for all agency systems and periodic testing and evaluation of controls to ensure

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

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

that they are implemented and operating as intended. In addition, our analyses of GAO and inspector general audit reports issued from July 2000 through September 2001 confirm that most agencies have significant weaknesses in their information security general controls, that is, 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. In particular, we found that for the 24 large federal departments and agencies we reviewed, all had significant weaknesses in *security program management*, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented, and in *access controls*, which ensure that only authorized individuals can read, alter, or delete data.

2. *In your statement, you indicated that "an important step toward ensuring information security is to fully understand the weaknesses that exist, and as the body of audit evidence expands, it is probable that additional significant deficiencies will be identified."*

   - *Why are security weaknesses in Federal information systems still not fully understood?*

     In past years, most reviews of information security controls were performed as part of agency financial statement audits and, thus, focused on financial systems. However, since the reform provisions are applicable to essentially all systems including national security systems and other types of risk beyond financial statements, audit coverage, as well as the required annual management reviews of agency information security programs, should include such additional risks and more nonfinancial systems. This is particularly true for agencies with significant nonfinancial operations, such as the departments of Defense and Justice. It is the extent of the weaknesses for these nonfinancial systems that are still not fully identified.

   - *Is there any way to characterize the impact of those undiscovered weaknesses?*

     While we do not know the extent of the weaknesses in many nonfinancial systems, any weaknesses would likely be similar to those found in financial systems. Such weaknesses are categorized within six general control categories, which are described in GAO's *Federal Information System Controls Audit Manual*.[3] These general control categories 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.

     My written statement characterizes the impact of such control weaknesses as placing a broad array of federal operations and assets at risk. For example,

     - resources, such as federal payments and collections, could be lost or stolen;

[3]U.S. General Accounting Office, *Federal Information System Controls Audit Manual, Volume 1—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999).

- 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 or 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.

Until these undiscovered weaknesses are fully identified, corrective actions will not be fully effective.

- *Are current evaluation and audit methodologies adequate to uncover these weaknesses?*

While adequate methodologies currently exist to identify and detect information security weaknesses, such methodologies must be appropriately applied to provide necessary audit and management review coverage. Further, periodically evaluating the effectiveness of security policies and controls is essential to ensuring that controls are implemented and functioning as intended. For example, GAO's *Federal Information System Controls Audit Manual* provides a methodology for evaluating information system controls. However, audit coverage should be expanded to cover both financial and nonfinancial systems. This will place a significant new burden on the existing audit capabilities of agency inspectors general and will require that they have appropriate resources to either perform or contract for the needed work. As another example, the reform provisions require program officials to perform annual program reviews, which are to include periodic testing and evaluation of the effectiveness of information security policies, procedures, controls, and techniques. To help perform these reviews, the National Institute of Standards and Technology developed its *Federal IT Security Assessment Framework*,[4] which 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. While many of the 24 agencies we contacted said that they used this questionnaire in performing their reviews, many also said that their results were based on management self-assessments, which did not include control testing to ensure that information security controls were implemented and operating as intended.

3. *What do you see as the most significant barriers to securing Federal information technology resources? What can be done to overcome these barriers?*

Through our audit work and analyses, we have noted several significant barriers to securing federal information technology resources. Three such barriers—poor information security program management, obtaining appropriate funding, and acquiring needed technical and audit expertise—are discussed below.

---

[4]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).

Poor Information Security Program Management

GAO and inspector general audit work reviewed for 24 of the largest federal agencies indicates that a significant barrier to securing federal information technology resources is agencies not fully implementing a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks in a cost-effective manner rather than reacting to individual problems in an ad-hoc manner only after a problem has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, virtually all the agencies for which this aspect of security was reviewed had deficiencies. Specifically, many had not (1) developed security plans for major systems based on risk, (2) documented security policies, and (3) implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, these agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- had a false sense of security because they were relying on ineffective controls, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Obtaining Appropriate Funding

Another barrier frequently mentioned by agencies is obtaining appropriate information security funding. However, while OMB requires agencies to identify amounts for information security in their budget submissions, agencies do not always provide this information. For example, the fiscal year 2001 and 2002 security costs that OMB requested agencies to identify as part of their reform provision reporting were not provided in some cases, and in other cases, there was no detail as to what these costs consisted of or how they are actually reflected in agency budget submissions. Further, OMB reports that it assessed the agencies' performance against the amount agencies spent and did not find that increased security spending equals increased security performance. As a result, OMB concludes that there is no evidence that poor security is a result of lack of money.

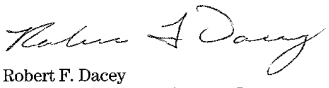
To help overcome this funding barrier, agencies must identify their information security costs to demonstrate their understanding of such costs and justify continued or additional funding. Further, as OMB indicates in its report to the Congress, much can also be done to cost-effectively address common weaknesses, such as security training, across government rather than piecemeal by agency. New funding initiatives by the administration may also help provide additional information security resources to federal agencies. For fiscal year 2003, the president is requesting $4.2 billion for information security funding from a total information technology investment request of approximately $52 billion as compared to about $2.7 billion reported for fiscal year 2002 from a total reported information technology investment of about $48 billion. This fiscal year 2003 amount does not include new governmentwide initiatives of the Office of Homeland Security, which include $298 million for cyberspace security.

Acquiring Technical and Audit Expertise

As highlighted during the Year 2000 challenge, the availability of technical and audit expertise is a continuing concern to agencies. Agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Programs are now underway to increase these resources by encouraging the creation of and participation in information security curriculums in educational institutions. In addition, the federal government must also maximize the value of its technical staff by sharing expertise and information.

We are sending copies of this letter to OMB and other interested parties. Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512-3317. I can also be reached by e-mail at *daceyr@gao.gov*.

Sincerely yours,



Robert F. Dacey
Director, Information Security Issues

(310154)

Questions for Mark Forman from Representative Horn

1. **In your report to Congress, you indicated that you conditionally approved some agencies' security programs.**

   - **Can you describe the process you used to review the plans?**

     OMB guidance directed agencies to report the results of the reviews and evaluations required by the Security Act. This includes annual reviews conducted by the Chief Information Officer (CIO) and program officials and the independent evaluations by Inspectors General's (IG). This information was due to OMB last September with agency's budget submissions.

     OMB's process for reviewing agency security programs was based on: 1) review of information (described above) that was transmitted by the agency head to OMB; 2) information gathered from the annual capital planning meetings with agencies; and 3) assessment of every agency's integration of security into their capital planning process.

   - **What specific criteria must an agency meet to receive a conditional approval, and what criteria is required to receive an approved security program?**

     OMB used the security requirements listed in the Government Information Security Reform Act and OMB policies to determine whether an agency's security program would be conditionally approved. OMB did not use any new security criteria in making these determinations but rather relied upon long-standing security policy and requirements.

     Specifically, OMB assessed the extent to which agencies have:
     - developed a program to monitor the effectiveness of the entire agency's security status;
     - integrated security into their capital planning and investment control process;
     - incorporated and funded security throughout the life cycle of systems and programs;
     - established performance measures for the CIO and program officials;
     - identified and prioritized the protection needs of critical assets;
     - trained their employees;
     - implemented an incident response capability and share and consult with FedCIRC;
     - integrated their IT security program with critical infrastructure protection efforts and other security programs; and
     - applied methods to ensure that contractor provided services are adequately secure.

     Additionally, OMB's assessment is conditional based upon the successful development, implementation, and maintenance of agency's corrective action

plans. The plans must identify all security weaknesses – performance gaps – found by the agency, IG, GAO, or OMB. Provided they appropriately address all weaknesses and are implemented properly, these plans will provide the agency with a solid foundation for remediating security weaknesses and closing performance gaps. They are essential management tools for the agency, IG, and OMB.

- **Which agencies received a conditional security program approval?**

  Especially in light of the events of September 11, the Director requested that such decisions remain private between OMB and the agencies.

- **How did having a conditional security program approval affect an agency's budget?**

  Approval was based on the findings presented by the IGs, CIOs, OMB, and other work we had done over the year and did not have a direct effect on budget decisions. Rather, budget decisions were made based on the agency's plans to close their IT security gaps that they and we had identified. Many of these gaps are management issues not requiring financial resources to remediate.

2. **In your written statement, you describe the format of a security committee on Executive Branch Information Systems Security as a standing committee under the Critical Infrastructure Protection Board, chaired by Mr. Clarke.**

   - **What are the standing committee's security roles and responsibilities in relation to the Federal CIO Council, agency heads, and your office for the development and oversight of security policies and programs?**

     Neither the Critical Infrastructure Protection Board under Executive Order 13231, the OMB-chaired Committee under the Board or the Federal Chief Information Officers Council under Executive Order 13011, has any policy or guidance setting authorities. These entities are coordinating groups that provide advice and recommendations to appropriate authorities.

     The Director of OMB has the responsibility to develop and oversee the implementation of government-wide policies, principles, standards, and guidelines for the security of information systems that support the executive branch departments and agencies, other than national security information systems that are the responsibility of the Secretary of Defense or the Director of Central Intelligence. These authorities are based in statute beginning with the Computer Security Act of 1987, and further supported by: 1) the Paperwork Reduction Act of 1995 (PRA); 2) the Clinger-Cohen Act of 1996 which linked OMB and agency security responsibilities to the information resources management, capital planning, and budget process; and 3) the Government Information Security Reform Act of 2000 (Security Act) which codified OMB's

security policies and continues the same framework. Additionally, OMB has under the Security Act, limited authorities over the management and evaluation of national security systems.

Within this statutory framework, OMB issues security policies and the National Institute of Standards and Technology (NIST) of the Department of Commerce issues technical guidance. NIST is responsible for developing technical security standards and guidelines for sensitive but unclassified Federal information and systems under the Computer Security Act. Again, the PRA, Clinger-Cohen Act and the Security Act all reinforce NIST's role. OMB policy requires that agency security programs and practices be consistent with NIST guidance.

The OMB-chaired Committee on Executive Branch Information Systems Security will assist agencies in improving and maintaining their security programs for non-national security information and information technology. It will advise and assist OMB, NIST, and Executive branch agencies in fulfilling their statutory responsibilities. The OMB Committee will view security from a government-wide perspective, particularly including its impact on agency mission accomplishment and program operations. In line with this mission, the membership of the OMB Committee is not limited to IT and security officials but rather includes representatives from a number of key Federal stakeholders that have security responsibilities such as IGs, Chief Financial Officers, Procurement Executives, Human Resource officials, program officials, in addition to security program managers and CIOs.

To ensure communication between the CIO Council and the OMB Committee, the CIO Council's security coordinator and other CIOs are Committee members. In addition, the Chief Financial Officers Council, President's Council on Integrity and Efficiency, Procurement Executives Council, Human Resources Management Council, Budget Officers Advisory Council, and Small Agency Council are all represented on the OMB Committee.

The OMB Committee's work on government-wide IT security issues will assist agencies and agency heads in improving the agency's security by closing performance gaps identified by the annual reviews under the Security Act and other audit work. The bulk of the OMB Committee's work will be accomplished through issue groups formed to review specific IT security issues. At the completion of their work, each issue group will make recommendations to the OMB Committee. Where appropriate, recommendations will be made to OMB for further action, such as official guidance.

3. **What do you see as the most significant barriers to securing Federal information technology resources? What can be done to overcome these barriers?**

Through the course of OMB's review of agency Security Act reports, corrective action plans, and IT budget materials, OMB has identified seven common

government-wide IT security weaknesses. To effectively remediate the seven weaknesses agencies must:

- Greatly increase the degree of senior management attention. Senior leaders must consistently establish and maintain control over the security of the operations and assets for which they are responsible.
- Establish measures of performance to ensure senior agency management can evaluate the performance of officials charged with securing agency operations and assets.
- Improve security education and awareness. Ensure that general users, IT professionals, and security professionals have the knowledge to do their jobs effectively.
- Fully integrate security into capital planning and investment control. Security must be built into and funded within each system and program through effective capital planning and investment control.
- Ensure contractor services are adequately secure as most Federal IT projects are developed and ultimately operated through outsourcing.
- Improve their ability to detect, report, and share information on vulnerabilities.
- Ensure timely installation of patches and adequate use of automated tools to scan systems for vulnerabilities and proper configuration.

These security performance gaps reveal that while agency officials with security responsibilities need the authority within their agency to fulfill their responsibilities, they must also be held accountable for their performance. OMB has required that agencies develop corrective action plans for all programs and systems where a security weakness was found. These plans assist the agency and OMB in ensuring that the agency officials responsible for the security of a program or system are held accountable.

Additionally, OMB's FY02 reporting guidance to agencies provides high-level management performance measures for agency CIOs and program officials to assist the agency and IG in assessing the performance of these individuals. Further, integration of IT security into the President's Management Agenda Scorecard will hold the agency head accountable for the agency's overall performance.

QUESTIONS ADDRESSED TO MS. ROBERTA L. GROSS:

GISRA-LESSONS LEARNED

Question: You recommend in your written testimony that the Office of Management and Budget emphasize overall management accountability within the Agency (rather than emphasizing the CIO's accountability) to avoid making the reporting process a "paper shuffling process". What actions would you recommend that OMB take to accomplish that goal?

Response: Accountability starts at the top. During the budget process, OMB should require each Agency head to certify that s/he has personally met and discussed with the CIO the past year's progress and the coming year's steps to implement training, personnel recruiting and retention, evaluation of internal controls including security, and capital planning. This certification should also include the Agency head's actions (e.g., memoranda, all hands, etc.) to use his/her office as a bully pulpit to convey that IT is a priority and personal steps taken to ensure headquarter and regional managers are implementing IT policies. To ensure integrity in this process, OMB - the budget examiners - should request from the IG an evaluation whether the head of the agency has taken steps to make IT a priority that is reflected at all levels of agency management.

Question: You identify the need for "first responder" training staff to analyze patterns of computer intrusions and take appropriate steps to help law enforcement to quickly assess

evidence of the intrusions. Are there training programs within the Government, and are agencies using them?

Response: Some agencies have established variations of a first responders program, most notably the Department of Energy and the Defense Department. At NASA, the Office of Inspector General Computer's Crime Division offered to the CIO to develop a program for and train Agency personnel as first responders at each NASA center. The training would consist of a protocol that would balance the need for NASA to operate its sensitive programs but also maintain evidence related to felonious intrusions of NASA's systems. However, because intruders do not confine themselves to one agency or one company, the NASA OIG has been considering a protocol that could be implanted government-wide. A more broad based approach is necessary both to ensure the protection of victim agencies and to enable prosecution of the hackers. Currently, the NASA OIG Computer Crimes Division is in contact with the IT security experts at the White House to discuss a broad based approach to computer intrusions.

I suggest that you contact NASA OIG through Paul Shawcross for additional briefing on this topic, including best practices and impediments to implementation.

Question: What do you see as the most significant barriers to securing Federal information technology resources? What can be done to overcome these barriers?

Response: A primary barrier to securing Federal information technology resources is the lack of accountability in the private sector for releasing products which have vulnerabilities. Companies rush to the market with their latest version of software, hardware and supporting equipment without sufficient testing and/or "fixes" for discovered vulnerabilities.

The federal government as a whole has to better exercise its buying power to require better security from the vendors. While some steps are being taken in this direction, the federal government needs to secure assurances from vendors and enforce these assurances. This will require creative contracting by the government and its lawyers to fashion appropriate agreements. Alternatively, the federal government should consider submitting appropriate legislation creating causes of action for negligent or grossly negligent release of IT products.

Further compounding this vendor problem is the conduct of purchasers, including the government, who are not sufficiently aware about the need (or are not motivated) to take affirmative, low cost/no cost steps to minimize their IT vulnerabilities. Both IGs and the GAO have reported this problem. Another barrier to securing IT resources is the lack of sufficient government oversight of the contractors who run most agencies' IT resources. During the downsizing in the 90's, many agencies outsourced their IT capabilities. They did not maintain sufficient numbers of trained, competent staff to ensure the best interests of the government. Trained and experienced personnel are needed to ensure the structuring of contracts to ensure sufficient and appropriate security clauses and for

evaluating the security practices of the contractors who have been empowered with a broad range of responsibilities (e.g., procuring, installing, maintaining and securing IT programs).

At the present time, because of market conditions, the federal government is in a position to recruit, train and deploy a skilled work force. It remains to be seen whether sufficient FTE's will be allotted to the IT function. OMB should be careful about requiring all agencies to find these slots from current (and often stretched) FTE ceilings. While some agencies and some departments within agencies have excess or underutilized personnel, the OPM rules make it difficult to quickly and efficiently utilize these potential slots.

Question: Security has been identified as a key enabler for e-government initiatives. Considering the outcomes of the National Aeronautics and Space Administration's) security evaluation and the OMB report, do you think the agency's security plans ands procedures are sufficient to support an aggressive move towards e-government? Do you see the priorities of e-government in competition with the priority of securing Federal IT systems?

Response: The problem in implementing an aggressive e-government initiative is not solely related to policies and procedures. Good policies and procedures have been around for some time. For example, OMB Circular A-130 sets forth good policies and procedures which NASA has adopted in its own internal guidelines. However, most agencies, including NASA, do not effectively implement their guidelines, do not monitor

to ensure that employees and contractors are abiding by them and have no sanctions or consequences (e.g., loss off access to certain uses of the network) for failure to follow required policies.

There are also potential legal issues which, in the past, the Justice Department's Computer Crimes and Intellectual Property Division raised for discussion. Their concerns centered on the legal consequences of a paperless government envisioned by the e-government initiatives. These concerns are evidentiary (the need to be able to prove that an individual or a corporation is bound by an electronic transaction). There are well accepted conventions in the paper world for interpreting binding agreements. There is also a large body of law to guide Courts in their resolution of contract disputes. This is not true in the electronic world where a party can deny ever entering into the deal or deny the authenticity of the terms of the deal. Some of these concerns will be taken care of once interoperable, secure encryption and authentication systems become widely adopted and recognized as safe and secure both by the government and private sector. Currently, the federal government, while working on this problem, is very far from solving these issues.

It is important to note that e-government initiatives can and do exist where security is not a paramount issue. For example, accessible web sites are already available to the public at most agencies. However, as most agencies have learned from widespread intrusions or virus infections, sensitive information and systems must be protected by more sophisticated security to ensure only authorized users have access.

OMB has tasked the CIO Council to take steps (e.g., common architecture, public keys, etc.) to be able to implement e-government. However, to fund these efforts, OMB "taxes" each agency to provide money to support OMB and the CIO Council. If the President truly views IT and e-government as a priority, then he should request a budget for OMB instead of asking each Agency to take it out of regular programs funds.

Moreover, if OMB is serious about e-government and IT security, then it must takes steps to approve Agency initiatives only where adequate security is in place. OMB should scrutinize plans carefully. In the past, when an Administration places a priority on an initiative (e.g., downsizing, outsourcing), some agencies implement these initiatives without good plans and the appropriate resources. Also, Congress should carefully probe claims by agencies and OMB when they announce e-government initiatives to discern what steps were taken to implement security. As Congress knows, agencies often overstate their progress. The NASA OIG has reported in audits and inspections that the Agency has often overstated its safeguards and progress in implementing IT security.

Question: What are some of the key differences between how unclassified and classified systems are managed at the National Aeronautics and Space Administration? How does the Agency develop its policies, requirements and guidelines for classified systems? How does the Agency oversee implementation of these policies, requirements and guidelines? Does the Agency have an Agency-wide security plan covering all classified systems?

Response: NASA places the jurisdiction of classified and unclassified systems under two different organizations. The CIO sets policies and procedures for unclassified systems; the Security Office has jurisdiction over classified systems. This fragmentation often results in the failure by personnel in these directorates to communicate and share risks and technology. This is a serious problem since NASA conducts many programs which are not classified but are sensitive. While there has been discussion about the need to coordinate, at the time I was still with the Agency there still was not effective communication. In part, this is caused by the lack of sufficiently trained personnel who can evaluate risks. It is also caused by the security personnel limiting security clearances by being overly narrow in defining who has a need to know. We have had instances where we were not able to brief members of the CIO community (and other senior NASA managers) about certain risks because they lacked the requisite clearances. Illustrative of the attitude of the NASA security personnel is the fact that it took the OIG several years, many memos and many meetings to obtain clearances for staff to conduct audits and evaluations of NASA's classified programs. NASA's security argued that the OIG did not "have a need to know" despite the broad access provisions of the IG Act. The Security personnel should have welcomed the OIG's reviews for assurance that NASA was being sufficiently protected. That definitely was not the attitude.

In establishing its policies and procedures for classified systems, NASA looks to the standards required by law, executive orders and the policies and regulations of the intelligence community. We have issued some reviews criticizing NASA's policies or its implementation for certain classified programs.

NASA asked the NSA to conduct the GISRA review of its classified systems. That review was not done in sufficient time for the OIG to fully evaluate it. However, I note that the NSA criticized NASA generally for failure to have any consistent oversight or follow-up for its IT policies other than the OIG.

For more details on this topic, I suggest that you contact the OIG for a briefing.

QUESTIONS FOR THE RECORD
HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON
GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND
INTERGOVERNMENTAL EFFICIENCY

LESSONS LEARNED FROM
THE GOVERNMENT INFORMATION SECURITY REFORM ACT
OF 2000

MARCH 6, 2002

Question #1

What do you see as the most significant barriers to securing Federal information technology resources?

- **What can be done to overcome these barriers?**

Answer:

Conventional wisdom often identifies training, the human element, as the most significant challenge to securing Federal information technology resources. While it is an immediate challenge and integral to the IT security equation, the training challenge is more a symptom of the increasingly complex IT enterprise. We now address increased IT complexity with both more training and flexible operational processes. However, in the long term IT complexity must also be addressed technologically. As IT functionality becomes more point and click, so too must configuration and security management. IT products and systems must made technically secure, "borne secure" in their development. They and the networks that support them must be configured with security management as one of the primary design goals. A secure enterprise with simplified and adaptive configuration and security management systems will ease the training challenge. Together they will enable us to operate more secure IT enterprises.

Question #2

The Office of Management and Budget Report suggests that a cultural or leadership change is needed that will focus attention and resources on securing information technology systems.

- **What actions have you taken -- or do you plan to take – to transform your agency's security priorities?**

Answer:

As I stated in both my oral and written testimony, the importance placed on Information Assurance (IA) within DoD begins with Secretary Rumsfeld and permeates throughout the department. We are far beyond introducing the concept of 'security as essential to mission success' to all levels of leadership. Leveraging information technology to create a seamless, interoperable, network-centric environment and the protection of U.S. information networks from attack are two of six key transformational goals for the Department around which we focus our defense strategy and develop our force.

Joint, Service, and Agency CIOs and IA principals routinely engage in collective forums to discuss enterprise IA issues and develop unified actions. Senior leaders as well as CIOs in the Unified Commands are personally involved in the IA posture of their commands. U.S. Space Command is specifically tasked with the mission to conduct Computer Network Defense. OMB reported that, "DoD operates the most comprehensive security training program of any Federal agency." The percentage of our Information Technology budget dedicated to IA is among the highest in the Federal Government and it is managed aggressively. Acquisition programs are scrutinized to ensure IA is given proper treatment throughout their life cycles. IA is an integral part of DoD, recognized and given high priority by its leadership both in word and practice.

Question #3

Security has been identified as a key enabler for e-government initiatives.

- **Considering the outcomes of your own agency's security evaluation and the OMB report, do you think your security plans and procedures are sufficient to support an aggressive move toward e-government?**

- **Do you see the priorities of e-government in competition with the priority of securing Federal IT systems?**

Answer:

The IA robustness of DoD is sufficient to support an aggressive move toward e-government and DoD is making that move. Maturing Public Key and Security Management Infrastructures (PKI/SMI) support several e-government programs.

The relationship between priorities of e-government and Federal IT systems security can be competitive and disruptive. Managed properly the relationship is more akin to dynamic tension. Access to government systems and information, especially from the public domain, creates unique security exposures and risks. However, prudent business practices require such access. The solution is design of functionality with security as a design factor. Appliqué security is the cause of competition between e-government functionality and system security. Program Managers who neglect to include IA requirements early during program development are often dismayed when the cost of appliqué security solutions generates cost overruns, program slips and sometimes curtailing of functionality. In that case, there is a competition between priorities. When IA requirements are included early during program development, the Program Manager can pragmatically balance all requirements. That balance produces a dynamic tension between functionality and security that is accommodated through risk management decisions rather than competition between priorities resolved through crisis management.

Question #4

What are some of the key differences between how unclassified and classified systems are managed at your agency?

- **How does your agency develop its policies, requirements and guidelines for classified systems?**
- **How does your agency oversee implementation of those policies, requirements and guidelines?**
- **Does your agency have an agency-wide security plan covering all classified systems?**

Answer:

DoD maintains separate classified and unclassified networks. The basic policy governing both is the same. Implementation and requirements differ in terms of cryptologic, physical, and personal security requirements. The key element is boundary management between domains and DoD has specific policy to manage the movement of data and information between security domains.

At the DoD level, IA policy for all systems assigns responsibility and gives generalized guidance for implementation. Guidance is based on law, national policy, and applicable best practices. Components promulgate supporting policy crafted for their specific environment. At the sub-component level, detailed security plans are developed for backbone, enterprise-wide, and enclave systems and networks. Oversight of policy implementation is similarly conducted with successive levels of management overseeing implementation at the next lower level.

Question #6

Your written testimony describes specific protection measures afforded individual systems. However, only 78 percent of you systems had a system security plan.

- **Without a comprehensive security plan, how can you determine if the system is adequately protected?**

- **What actions is the department taking to ensure that all critical systems have an approved security plan?**

Answer:

Without a comprehensive security plan, short of a system audit, you cannot objectively assess the adequacy of a system's IA posture. Within DoD we recognize this shortfall and are pursuing multiple efforts to streamline the DoD Information Technology Security Certification and Accreditation Program (DITSCAP) that requires the development and maintenance of system security plans, and institute management controls for implementation verification. As I mentioned in both my oral and written testimony, responses obtained by both the GISR IPT and the DoD IG during the conduct of the GISR 2001 assessment indicate problems with DITSCAP, specifically in the areas of program compliance, complexity, and clarity. Absence of system security plans is a symptom of the complexity of the DITSCAP process and clarity of its implementing policy. The DITSCAP is currently undergoing dramatic modification in policy as well as implementation. The DoD policy governing DITSCAP will streamline the certification and accreditation (C&A) process and provide better clarity on definitions and responsibilities. DoD is also pursuing the use of automated tools to ease the documentation burden on security and systems administrators. The combination of these two efforts should significantly improve our ability to conduct C&A and develop attendant system security plans, and as a result improve compliance. DoD through DISA has also aggressively implemented comprehensive connection approval programs for both the Non-secure and Secret Internet Protocol Router Networks (NIPRNET/SIPRNET.) Those programs have initial and subsequent periodic validation of C&A as a precondition for connection approval. This will serve as a valuable compliance control mechanism.

Question #7

The OMB report stated that the department lacks a department-wide methodology to identify and prioritize critical assets.

- **What actions is the department taking to develop a methodology to identify and prioritize critical assets, and their dependencies on key external systems, in order to protect them?**

Answer:

The DoD Critical Infrastructure Protection (CIP) Directorate has reviewed the Critical Infrastructure Assurance Office's Project Matrix methodology that is being used throughout the Federal government to identify critical assets and assess their dependencies within the public and private sectors. The CIP Directorate has designated the Joint Program Office for Special Technology Countermeasures to serve as the Office of the Secretary of Defense's technical agent for identifying and assessing DoD's critical assets. The CIP Directorate is encouraging the use of the JPO methodology, which is somewhat analogous to Project Matrix, throughout the Department. The Pacific Command (USPACOM) is serving as the testbed for the JPO methodology. The CIP Directorate also is preparing a DoD Directive and Instruction to address this activity.

Q1. Your automated security patching program, "Safepatch" is especially interesting since one of the recurring problems in the Federal computing environment is keeping up with security patches for vulnerable commercial software. Can you give us some details on how the program works?

A1. We developed SafePatch from a proof-of-concept in April 1996 into a fully functional and extremely powerful tool that has been successfully deployed within the Department of Energy and the U.S. Air Force. SafePatch is freely available to Federal agencies and has been offered to GSA as a government wide solution.

SafePatch provides automated analysis, notification, distribution, and installation of related security patches to network-based computer systems. In addition, Safepatch grants system administrators the ability to "back-out" of installed patches, restore a system's previous state, and collect site-wide software statistics or metrics on patch status. Our current version patches UNIX systems, and a Windows version will be rolled out this fall. SafePatch allows network administrators to query, maintain, and upgrade the software integrity of hundreds of individual systems from a central point through an automated means.

Q2. What do you see as the most significant barriers to securing Federal information technology resources? What can be done to overcome these barriers?

A2. Cyber security has classically been considered a technical issue. We believe it is primarily a management issue. Executive management needs to recognize this responsibility and be accountable for the security of all information systems, both classified and unclassified. Organizations need to focus their management's priority on cyber security and seamlessly integrate it into all IT investments.

Q3. The Office of Management and Budget report suggests that a culture of leadership change is needed that will focus attention and resources on securing information technology systems.

What actions have you taken – or do you plan to take – to transform your agency's security priority?

A3. The Department is shifting to a culture that integrates cyber security into all levels of work. As an example, two policies were issued last year that hold management accountable for protecting all information systems assets. As a key member of the executive leadership of DOE, I am committed to ensuring that the vision for IT asset security is disseminated throughout the Department. We are finding that the Government Information Security Reform Act is an effective tool to ensure that all department levels are cognizant of cyber security's importance in the IT capital investment process.

Q4. Security has been identified as a key enabler for e-government initiatives. Considering the outcomes of your own agency's security evaluation and OMB report, do you think your security plans and procedures are sufficient to support an aggressive move toward e-government? Do you see the priorities of e-government in competition with the priority of securing Federal IT systems?

A4. We have completed the development of many key elements that constitute an effective cyber security program and are in the process of enhancing and fully implementing those that are still outstanding. As part of our e-government program we will mandate that all new IT investments have security appropriately addressed using the A-11 process or they will not be funded.

We find no competition between e-government priorities and the securing of Federal IT systems. They are in fact the same priority. We see e-government as our entire IT investment portfolio. Therefore, in order to achieve effective e-government goals, I am committed to ensuring that management internalizes the importance of cyber security and is

held accountable for its implementation with e-government initiatives. Security must be integrated into our business processes and policies.

Q5. What are some of the key differences between how unclassified and classified systems are managed at your agency? How does your agency develop policies, requirements, and guidelines for classified systems? How does your agency oversee the implementation of those policies, requirements and guidelines? Does your agency have an agency-wide security plan covering all classified systems?

A5. The key difference between how unclassified and classified systems are managed is that classified systems are governed by a very rigorous set of policies and procedures that are defined by the national security community, while unclassified systems are governed by a risk-based and cost-effective approach. Classified policies operate under the premise that significant harm will result if classified information is compromised. Unclassified systems span much greater sensitivity levels and as such, must be viewed with the "appropriate levels of safeguard."

The Department develops policies, requirements, and guidelines for classified systems utilizing government-wide policies and standards. We actively participate with the National Institute of Standards and Technology in developing best practices for unclassified information. We participate with the Committee on National Security Systems (CNSS), in developing national policy and best practices for classified information.

The Department oversees the implementation of these classified system policies through a defense-in-depth approach. My office actively monitors the performance and implementation of key elements of our cyber security program through performance metrics and the review of independent oversight audits. In addition, the Department takes advantage

of the capabilities of the Offices of Independent Oversight and Performance Improvement and the Inspector General to provide insight into program implementation.

The Department has developed policy documents that prescribe the process for ensuring the security of all classified systems. Although there is a not a single security plan that covers all systems, all systems are required to be covered by a security plan.