AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBER SECURITY: THE STATUS OF INFORMATION SECURITY AND THE EFFECTS OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT [FISMA] AT FEDERAL AGENCIES

HEARING

BEFORE THE

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

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JUNE 24, 2003

Serial No. 108–100

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

91–648 PDF WASHINGTON : 2004

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

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

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

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

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

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

ADAM H. PUTNAM, Florida, *Chairman*

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

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

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

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

CONTENTS

	Page
Hearing held on June 24, 2003	1
Statement of:	
Charbo, Scott, Chief Information Officer, Department of Agriculture	115
Cobb, Robert, Inspector General, NASA	101
Dacey, Robert F., Director, Information Security Issues, General Accounting Office	23
Forman, Mark A., Administator for Electronic Government and Information Technology, Office of Management and Budget	12
Frazier, Johnnie E., Inspector General, Department of Commerce	71
Ladner, Drew, Chief Information Officer, Department of Treasury	126
Morrison, Bruce, acting Chief Information Officer, Department of State	146
Letters, statements, etc., submitted for the record by:	
Charbo, Scott, Chief Information Officer, Department of Agriculture, prepared statement of	118
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	58
Cobb, Robert, Inspector General, NASA, prepared statement of	104
Dacey, Robert F., Director, Information Security Issues, General Accounting Office, prepared statement of	25
Forman, Mark A., Administator for Electronic Government and Information Technology, Office of Management and Budget, prepared statement of	15
Frazier, Johnnie E., Inspector General, Department of Commerce, prepared statement of	73
Ladner, Drew, Chief Information Officer, Department of Treasu128	
Miller, Hon. Candice S., a Representative in Congress from the State of Michigan, prepared statement of	10
Morrison, Bruce, acting Chief Information Officer, Department of State, prepared statement of	148
Putnam, Hon. Adam H., a Representative in Congress from the State of Florida, prepared statement of	5

CYBER SECURITY: THE STATUS OF INFORMATION SECURITY AND THE EFFECTS OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT [FISMA] AT FEDERAL AGENCIES

TUESDAY, JUNE 24, 2003

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

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

Present: Representatives Putnam, Miller, Clay and Watson.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Chip Walker and Lori Martin, professional staff members; Ursula Wojciechowski, clerk; Suzanne Lightman, fellow; Bill Vigen and Richard McAdams, interns; Jamie Harper and Kim Bird, legislative assistants; David McMillen, minority professional staff member; and Cecelia Morton, minority office manager.

Mr. PUTNAM. A quorum being present, this hearing on the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order. Good morning, and welcome to the second in a planned series of hearings addressing the important subject of cyber security.

Today we continue our in-depth review of cyber security issues affecting our Nation. Specifically this hearing will focus sharply on the efforts within the Federal Government to secure our own computer networks. Our critical infrastructure of the cyber kind must have the same level of protection as our physical security if we are to be secure as a Nation from random hacker intrusions, malicious viruses or, worse, serious cyber terrorism.

There are several things unique to cyber attacks that make the task of preventing them particularly difficult. Cyber attacks can occur from anywhere around the globe, from the caves of Afghanistan to the warfields of Iraq, from the most remote regions of the world, or simply right here in our own backyard. The technology used for cyber attacks is readily available and changes continually, and maybe most dangerous of all, is the failure of many people critical to securing these networks and information from attack to take the threats seriously, to receive adequate training and to take the steps necessary to secure their networks.

A serious cyber attack would have serious repercussions throughout the Nation in a physical sense and in very real economic terms. A recent report under Government Information Security Reform Act once again demonstrates that we have a long way to go in the Federal Government to feel the least bit confident that we have secure computer networks. Before going into more detail about the report, I want to comment briefly about the timing. This latest GISRA report was released this May. It was based on information provided to OMB in September 2002. This is kind of like being an astronomer and looking in the telescope at the stars, all the while realizing that what you are viewing actually occurred a long, long time ago. We need to find a way to get more real-time reporting, and I want to work with OMB on improving the timeliness of their information.

The current GISRA report demonstrates that progress in computer security at Federal agencies is proceeding slowly, and that simply is no longer acceptable. The OMB report to Congress identified a number of serious weaknesses. Many agencies are facing the same security weaknesses year after year, such as the lack of system-level security plans and certifications and accreditations. Some IGs and CIOs from within the same agencies have vastly different views of the state of the agency security programs. Many agencies are not adequately prioritizing their IT investments and are seeking funding to develop new systems while significant weaknesses exist in their legacy systems. Not all agencies are reviewing all programs and systems every year as required by GISRA. More agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. The old thinking of IT security as the responsibility of a single agency official or the agency's IT security office is out of date, contrary to law and policy, and that significantly endangers the ability of these agencies to safeguard their IT investments.

The Departments of Treasury, State and Agriculture all have serious problems with their information security. Both the CIOs and the IGs of these agencies have concerns. In addition, GAO has indicated a concern with computer security for all three agencies in its performance and accountability series.

In the fiscal year 2002 GISRA report, the Department of Agriculture reported that less than 26 percent of its systems were in compliance with the eight metrics that the OMB reported. The agency had 70 material weaknesses in the area of information security reported by the IG. In addition, according to the IG, the agency is not conducting risk assessments of its systems in compliance with either OMB or GISRA's requirements. This year the agency reported an increase in systems operating without written authority and an increase in systems that do not have up-to-date IT security plans.

The Department of State did not report information for the fiscal year 2001 GISRA report. It reported three material weaknesses for information security for fiscal year 2002. In June 2001, the Department's IG released a report that highlighted a number of areas that State needs to address. They included assessing vulnerability of systems, conducting security control evaluations at least once every 3 years, and testing security controls. State reported in their

fiscal year 2002 report that none of its systems have been certified and authorized, and only 15 percent have an up-to-date IT security plan. Finally, State reported that only 11 percent of its systems have contingency plans, and of those, none had ever been tested.

Although the Department of Treasury reported that, in the 2002 GISRA report, 41 percent of its systems were assessed for risk, its IG reported that Treasury did not use an adequate methodology to determine that risk; therefore, its assessments were not valid under the law. There are also significant discrepancies in many of the metrics reported in the GISRA report between the Department and its IG. For example, the Department reported 451 of its systems were reviewed; however, the IG reports that only 204 systems were reviewed. Treasury has also reported 11 material weaknesses related to information security.

I understand that many of those testifying today are relatively new to their jobs. We are not here today to point fingers, although I have serious questions about accountability and responsibility for these egregious failures to perform minimum requirements. We are here to identify weaknesses or roadblocks, find solutions and make progress.

In a recent edition of the Federal Times headlined "Computer Security Dilemma: Agencies Must Choose—Follow the Law or Fix the Problem," several government IT managers complained that the documentation process set up by Congress gives them a choice to document their security problems for Congress or to fix them. This attitude is disturbing, to say the least. For most IT managers, the documentation process set up by Congress is the only reason they discovered many of their security weaknesses. Before the documentation process, many IT managers couldn't identify their critical systems. Sadly, even with the documentation process required by Congress, many systems are still unidentified. That said, the committee will try and remain open-minded, and if any of the witnesses today would like to support this either/or contention as reflected by the article, we look forward to hearing it.

As the subcommittee continues to examine the cyber security issue, we see the same recurring theme. Securing these networks is not about money or technology, but about management. The weaknesses identified are weaknesses that would be significantly reduced if approved procedures and protocols or best practices were actually followed. For example, GAO still conducts audits to this day where they find default passwords in place or where systems have not been tested in a production environment. Patches remain uninstalled on systems for months after known vulnerabilities are identified. These rudimentary lapses are not acceptable.

There are a number of issues still up for consideration before the Congress. These include requiring that the common criteria be the standard government-wide; automated vulnerability scanning; new levels of accountability; and confronting the issue of CIO retention head on.

While some progress is clearly being made at Federal agencies, going from an F to a D is not saying a lot. It is my hope that the Congress, OMB, the CIOs, the IGs and the GAO can work together to move our level of IT security government-wide into a range

where we have some degree of comfort that our systems are secure. We are far from that point today.

I would like to thank the witnesses for coming today and presenting the valuable testimony. As with all of our hearings, today's can be viewed live via Webcast by going to reform.house.gov and clicking on the link under multimedia.

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

TOM DAVIS, VIRGINIA
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH 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
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER, MARYLAND
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT, INDEPENDENT

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

Oversight Hearing

"Cyber Security: The Status of Federal Information Security and the Effects of the Federal Information Security Management Act at Federal Agencies."

Tuesday, June 24, 2003

Opening Statement

Chairman Adam Putnam (R-Fl)

Good morning. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order. Good morning and welcome to the second in a planned series of hearings addressing the important subject of cyber security.

Today we continue our in-depth review of cyber security issues affecting our nation. Specifically this hearing will focus sharply on the efforts within the Federal Government to secure our own computer networks. Our critical infrastructure, of the cyber kind, must have the same level of protection as our physical security, if we are to be secure, as a Nation, from random hacker intrusions, malicious viruses or worse – serious cyber terrorism.

There are several things unique to cyber attacks that make the task of preventing them particularly difficult. Cyber attacks can occur from anywhere around the globe: from the caves of Afghanistan to the war fields of Iraq, from the most remote regions of the world or simply right here in our own back yard. The technology used for cyber attacks is readily available and changes continually. And, maybe most dangerous of all, is the failure of many people -- critical to securing these networks and information from attack -- to take the threat seriously, to receive adequate training, and to take steps needed to secure their networks. A serious cyber attack could have serious repercussions throughout the nation both in a physical sense and in very real economic dollars.

A recent report under Government Information Security Reform Act (GISRA) once again demonstrates that we have a long way to go in the Federal government to feel the least bit confidant that we have secure computer networks. Before going into more detail about the report, I want to comment briefly about the timing. This latest GISRA report was released this May. It was based on information provided to OMB in September of 2002! This is kind of like being an astronomer and looking into a telescope at the stars all the while realizing that what you are viewing happened a long long time ago. We need to find a way to get more real time reporting and I want to work with OMB on that aspect of the reporting.

The current GISRA Report demonstrates that progress in computer security at Federal agencies is proceeding slowly and that simply is no longer acceptable. The OMB report to Congress identified a number of serious weaknesses:

- Many agencies are facing the same security weaknesses year after year, such as lack of system level security plans and certifications and accreditations;
- Some IGs and CIOs -- from within the same agencies -- have vastly different views of the state of the agency's security programs;
- Many agencies are not adequately prioritizing their IT investments and are seeking funding to develop new systems while significant weaknesses exist in their legacy systems;
- Not all agencies are reviewing all programs and systems every year as required by GISRA;
- More agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. The old thinking of IT security as the responsibility of a single agency official or the agency's IT security office is out of date, contrary to law and policy, and significantly endangers the ability of agencies to safeguard their IT investments.

The Departments of Treasury, State and Agriculture all have serious problems with their information security. Both the CIOs and the IGs of these agencies have concerns. In addition, GAO has indicated a concern with computer security for all three agencies in its Performance and Accountability Series.

In the FY 2002 GISRA report, the Department of Agriculture reported that less then 26% of its systems were in compliance with the 8 metrics that OMB reported. The agency had 70 material weaknesses in the area of information security reported by the IG.

In addition, according to the IG, the agency is not conducting risk assessments of its systems in compliance with either OMB or GISRA requirements. This year, the agency reported an increase in systems operating without written authority, and an increase in systems that do not have up-to-date IT security plans.

The Department of State did not report information for the FY 2001 GISRA report. It reported 3 material weaknesses for information security for FY 2002. In June 2001, the Department's IG released a report that highlighted a number of areas that State needs to address.

These areas included assessing vulnerability of systems, conducting security control evaluations at least once every three years, and testing security controls. State reported, in the FY 2002 GISRA report, that none of its systems have been certified and authorized, and only 15% have an up-to-date IT security plan. Finally, State reported that only 11% of its systems have contingency plans, and of those, none had ever been tested.

Although the Department of Treasury reported that in the FY 2002 GISRA report that 41% of its systems were assessed for risk, its IG reported that Treasury did not use an adequate methodology to determine risk. Therefore, its assessments were not valid under GISRA.

There are also significant discrepancies in many of the metrics reported in the GISRA report between the Department and its IG. For example, the Department reported that 451 of its systems were reviewed. However, the IG reports that only 204 systems were reviewed. Treasury has also reported 11 material weaknesses related to information security.

I understand that many of those testifying today are relatively new to their jobs. We're not here, today, to point fingers, although I have serious questions about accountability and responsibility for these egregious failures to perform minimum requirements, we are here to identify weaknesses or roadblocks, find solutions and make progress.

In a recent edition of the *Federal Times* headlined "Computer Security Dilemma: Agencies Must Choose – Follow the Law or Fix the Problem," several government IT managers complain that the documentation process set up by Congress gives them a choice: document their security problems for Congress or fix them.

To say that I am disturbed by this attitude would be an understatement. For most IT managers the documentation process set up by Congress is the only reason they discovered many of their security weaknesses. Before the documentation process, many IT managers couldn't even identify their critical systems.

Sadly, even with the documentation process required by Congress, many systems are still unidentified. All that being said, I will try and remain open minded and if any of the witnesses today would like to support this either/or contention I would like to hear it.

As the subcommittee continues to examine the cyber security issue, we see the same recurring theme. Securing these networks is not about money or technology but about people and management. The weaknesses identified are weaknesses that would be significantly reduced if approved procedures and protocols or best practices were actually followed.

For example GAO still conducts audits to this day where they find default passwords in place or where systems have not been tested in a production environment. Patches remain uninstalled on systems for months after known vulnerabilities are identified. These rudimentary lapses are simply not acceptable.

There are a number of issues still up for consideration for the Congress. These include:

- Requiring that the Common Criteria be the standard government-wide.

- Automated vulnerability scanning.
- New levels of accountability.
- Confronting the issue of CIO retention head-on.

While some progress is clearly being made at federal agencies, going from an F to a D or D to a C isn't saying much. It's my hope that the Congress, OMB, the CIOs, the IGs and the GAO can work together to move our level of IT security government-wide into a range where we have some relative degree of comfort that our systems are secure. We are a long way from that point today.

I would like to thank all the witnesses for coming today and presenting your valuable testimony.

Mr. PUTNAM. At this point I would like to yield to the vice chairwoman of the subcommittee, the gentlelady from Michigan, Mrs. Miller.

Mrs. MILLER. Thank you, Mr. Chairman.

In a post-September 11 environment, the Federal Government has been forced to reevaluate its security procedures. The logistics associated with such an attack are huge, and today we focus on the security of Federal information systems.

There has been a long-held belief that there should be one oversight facilitator for the entire Federal Government, government chief technology officer in a sense. I think this idea has some merit in order to ensure that government-wide uniformity occurs. However, one thing is clear, as technology continues to evolve at quite an astonishing rate, quite frankly, the Federal Government must not be left behind utilizing technology and systems designed for a different time and different type of threat. For these reasons, I am pleased, Mr. Chairman, that you have called this hearing so that Congress has an opportunity to objectively evaluate security measures taken by Federal agencies.

To be frank, with the active measures that international terrorists are taking against our freedoms, I am concerned that certain Federal agencies appear to be lax with their efforts to improve system safeguards. Oversight reports by the GAO and the OMB frequently identify areas of concern and countless examples of Federal agencies in noncompliance with various laws and regulations related to system securities. Incomplete and inaccurate reports that are required of Federal agencies, the apparent inability of agencies to reach their own stated performance goals, and in many cases the blatant and utter disregard of federally mandated requirements are just some of the issues that we face in this regard.

Since September 11, Americans have stated in poll after poll that homeland security and the war against terror is the most important issue facing our great Nation. I am concerned that individuals within the Federal Government, individuals that Americans trust to protect them and their families, do not seem to understand the nature of the cyber threat. However, in spite of current problems, the government is faced with a historic opportunity. With the passage of GISRA and the E-Government Act of 2002, which includes the FISMA, Federal agencies now have the tools and the necessary support to develop and implement substantial information security reform.

There has been some success, as the government moves forward. The work being done at the Department of Commerce is really a great example. And those examples of success should be used as a model for other agencies. I certainly look forward to working with you, Mr. Chairman, and the other members of this committee to assist agencies with their reform objectives. Thank you.

Mr. PUTNAM. I thank the gentlelady for her interest in these issues and her outstanding work on behalf of the subcommittee.

[The prepared statement of Hon. Candice S. Miller follows:]

Congresswoman Candice S. Miller

Opening Statement
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census
June 24, 2003

OPENING STATEMENT

Thank you, Mr. Chairman.

In a post-September 11th environment, the Federal government has been forced to re-evaluate its security procedures. The logistics associated with such a task are vast, and today we focus on the security of Federal information systems.

There has been a long-held belief that there should be one oversight facilitator for the entire Federal government – a government Chief Technology Officer, in a sense. This idea may have some merit, in order to ensure a government-wide standardization and interoperability. However one thing is clear -- as technology continues to evolve at an astonishing rate, the government must not be left behind, utilizing technologies and systems designed for a different time and a different type of threat. For these reasons, I am pleased that you have called this hearing, Mr. Chairman, so that Congress has the opportunity to objectively evaluate security measures taken by Federal agencies.

To be quite frank, with the active measures that international terrorists are taking against our freedoms, I am concerned that certain federal agencies appear to be lax with their efforts to improve systems safeguards. Oversight reports by the General Accounting Office and the Office of Management and Budget frequently identify areas of concern and countless examples of Federal agencies in non-compliance with various laws and regulations related to systems security. If an individual forgets to staple his or her w-2 form to a tax return, then that person lives in fear that the I.R.S. is going to conduct an audit. But it appears that some Federal agencies are above the law – feeling no need to fulfill even administrative requirements.

Incomplete and inaccurate reports that are required of Federal agencies, the apparent inability of agencies to reach their own stated performance goals, and in many cases, the blatant and utter disregard of Federally-mandated requirements are just some of the issues we are facing in this regard. Since September 11th, Americans have stated in poll after poll that homeland security and the war against terror

is the most important issue facing our great nation. But I am concerned that individuals within the Federal government – individuals that Americans trust to protect them and their children – do not seem to understand the nature of this cyber-threat.

However, in spite of the current problems, the government if faced with a historic opportunity. With the passage of the Government Information Security Reform Act and the e-Government Act of 2002, which includes the Federal Information Security Management Act, Federal agencies now have the tools and the necessary support to develop and implement substantial information security reform. There has been some successes as the government moves forward – the work being done at the Department of Commerce is a fine example – and those examples of success should be used as a model for other agencies. I look forward to working with the Chairman and other Members of the Subcommittee to assist agencies with their reform objectives.

Thank you.

Mr. PUTNAM. At this time we will move to witness testimony. Witnesses will please rise and raise their right hands for the oath.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record both witnesses responded in the affirmative, and we will move forward with opening statements. I will begin with our first witness for his 5-minute statement, Mark Forman. In June 2001, Mr. Forman was appointed by President Bush to oversee implementation of the 21st century information technology throughout the Federal Government. Mr. Forman is the first person in the Federal Government to fulfill responsibilities normally associated with a corporate chief information officer. Under his leadership, the Federal Government has received broad recognition for its successful use of technology in the government. He manages over $58 billion in IT investments and leads the President's E-Government Initiative to create a more productive citizencentric government. He is a frequent guest of our hearings and always has a very fruitful and candid view of the government's progress in all matters related to technology and electronic government.

Mr. Forman, you are recognized for 5 minutes. Welcome to the subcommittee.

STATEMENT OF MARK A. FORMAN, ADMINISTATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET

Mr. FORMAN. Thank you, Mr. Chairman and Congresswoman Miller. Thank you for inviting me to discuss the status of the Federal information security and the effects of FISMA at the departments and agencies. I do look forward to working with you to improve the timeliness of our report, and I agree with you that it should come up early as well.

I think we have a number of actions at the staff level. We have been working with your staff to accelerate the reporting and make sure we are both getting good data on the status. As noted in our report to Congress, progress has been made in identifying and remediating longstanding IT security problems, but there is much work that remains before we can say IT systems are adequately secured in the Federal Government.

FISMA requires that Federal agencies report as a material weakness any significant deficiency in a policy, procedure or practice, and over half of the large agencies have declared at least one material weakness relating to IT security. Deficiencies exist in a number of areas, including access controls, configuration management, security policy and training. From a government-wide perspective, the most common weaknesses include a lack of system-level security plans, legacy systems that are not appropriately secured, and plans of actions and milestones that do not include all of the agency systems.

Nonetheless, in fiscal year 2002, departments and agencies have made measurable progress in IT security by conducting activities such as risk assessment, security planning, certification and accreditation, training and contingency planning. Of Federal systems in fiscal year 2002, 65 percent have been assessed for risk; 62 percent had an up-to-date security plan, 47 percent had been certified

and accredited, and 55 percent had a contingency plan. We believe that is about double the status of IT security in 2001. I know the General Accounting Office has some difference and would be glad to discuss that.

As noted in our report to Congress, agencies are testing an increasing percentage of their systems for management, operational and technical control weaknesses. These weaknesses, once identified, are included in agencies' plans of actions and milestones for prioritization, tracking and correction.

The administration is committed to rapid progress, so by the end of this calendar year, all agencies will have a rigorous process for developing and implementing plans of actions and milestones. As you mentioned this is a management issue. And second, 80 percent of the systems will be certified and accredited.

One reason we believe that IT security can be rapidly improved is that Federal agencies are incorporating security considerations into their capital planning process. Our analysis shows the percentage of Federal systems with security costs integrated into the life cycle of a system now stands at 62 percent.

Improving Federal information security requires that we focus on enterprise architecture rather than firewalls, intrusion detection, vulnerability patches or the latest IT security technology. FEA, the Federal Enterprise Architecture, reference models will enable better use of standards and configuration management that we need to secure the Federal information systems. In addition, improvements in agency enterprise architectures will enable CIOs to better ensure that security and privacy are properly incorporated into their IT operations.

To assist agency EA efforts in accordance with the responsibilities under FISMA, the National Institute of Standards and Technology recently published draft standards for security categorization of Federal information and information systems. This proposed standard will be used by all agencies to categorize systems according to risk. NIST is also drafting companion guidelines recommending the types of information systems to be included in each category as well as minimum information security requirements.

OMB and the CIO Council have developed a process to rapidly identify and respond to cyber threats and critical vulnerabilities. CIOs are advised via conference calls as well as e-mails of specific actions needed to protect systems. Agencies must then report to OMB on the implementation of countermeasures usually in 24 to 72 hours. As a result of these early alerts, agencies have been rapidly closing vulnerabilities that otherwise might have been exploited, and this includes use of patch management services to ensure rapid application of patches.

The Federal Information Security Management Act will be instrumental in improving the state of Federal IT security. The framework and processes in law and OMB policy highlight the importance of management, implementation evaluation and remediation for achieving progress.

In closing, the administration is committed to a Federal Government with secure information systems doing the significant work of this committee, Federal IGs and the agencies. I think we are able

to point to real improvements in government IT security, but there is much more work to be done. Thank you.

Mr. PUTNAM. Thank you, Mr. Forman.

[The prepared statement of Mr. Forman follows:]

STATEMENT OF
THE HON. MARK A. FORMAN
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS
U.S. HOUSE OF REPRESENTATIVES
June 24, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss the positive actions being taken by the federal government to address IT security challenges and issues. As noted in OMB's May 16th Report to Congress on Federal Government Information Security Reform, progress was made in FY 2002 to identify and begin to address long-standing IT security problems that are both serious and pervasive. This trend has continued in FY 2003 with Departments and agencies further strengthening management, operational and technical controls. Much work remains, however, for security to be adequately incorporated into the life-cycle of all IT investments. OMB intends to lead this effort through coordinated management and budget processes.

Measuring Agency Performance

Annual IT security reviews

In accordance with the Federal Information Security Management Act (FISMA), agency Chief Information Officers (CIOs) and program officials must conduct annual IT security reviews of their programs and the systems that support their programs. Additionally, agency Inspectors General (IGs) are asked to perform annual independent evaluations of the agency's IT security program and a subset of agency systems. The results of these reviews and evaluations are reported annually to OMB.

FY 2001 reports, conducted pursuant to the Government Information Security Reform Act (GISRA), established a baseline of agency IT security status. To ensure that progress could be consistently determined against that baseline, OMB's FY 2002 reporting instructions remained nearly identical to the FY 2001 requirements. The FY 2002 reporting instructions also included common IT security performance measures. For the first time, using these performance measures, the Federal government is able to determine progress in IT security. Federal agencies, OMB, the Congress, and the General Accounting Office are able to track and monitor agency status and progress using those measures.

OMB Analysis of Agency Reports

As stated in my April testimony, agencies have demonstrated quantifiable progress in conducting activities such as risk assessment, security planning, certification and accreditation and contingency planning. From FY 2001 to FY 2002, the Federal government made progress across all areas of IT security performance measures. Sixty-five percentage of federal systems in FY 2002 had been assessed for risk, 62% had an up to date security plan, 47% had been certified and accredited, and 55% had a contingency plan. The Clinger-Cohen report included in the President's 2004 budget builds on this pattern of improvement and establishes a goal that 80% of Federal IT systems be certified and accredited by the end of December 2003.

Additionally, agencies have reported that, in accordance with FISMA requirements, they are testing an increasing percentage of their systems for weaknesses in management, operational and technical controls.

At many agencies, program officials, CIOs, and IGs are engaged and working together. IGs have greatly expanded their work beyond financial systems and related programs and their efforts have proved invaluable to the process. Some IGs and CIOs, however, have significantly different views of the state of the agency's security programs. Agency heads need to understand the reason for such differences where they exist.

FISMA legislation requires that federal agencies report any significant deficiency in a policy, procedure, or practice as a material weakness. Over half of the large agencies (14 out of 24) have declared at least one material weakness relating to IT security. Deficiencies are noted in a number of areas including access controls, configuration management, risk management, security policy, physical security, intrusion detection, incident handling, training, and testing of contingency plans. Through the Plan of Action and Milestones (POA&Ms) process, OMB will oversee work by federal agencies to close these material weaknesses and substantially decrease the number that are repeated from prior fiscal years.

Increasing Agency Attention to IT Security Remediation

OMB has found that agency senior managers are paying greater attention to IT security. In accordance with OMB guidance, CIOs and program officials must maintain POA&Ms to ensure that program and system level IT security weaknesses are tracked and corrected. The agencies include in their plans the name of the person responsible for correcting the weakness, the resources required and the target completion date. Agencies provide quarterly updates to OMB on their progress in remediating their IT security weaknesses. To assist agencies and OMB in better tracking progress, agencies will also include with their quarterly updates their status against the IT security performance measures in OMB guidance. These updates will help inform the quarterly assessment of the President's Management Agenda scorecard.

Ensuring Effective and Accountable Information Security

While awareness of IT security requirements and responsibilities has spread beyond security and IT employees, more agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. Increased understanding of IT security requirements along with improved accountability will assist program officials in successfully securing their programs and services.

Rather to appropriately secure our operations and assets, all Federal employees must recognize and fully meet their security roles. Those agency officials with additional responsibilities, such as agency program officials and the agency CIO must be held accountable for meeting those responsibilities. The owner of a system must ensure that security has been incorporated throughout the entire life-cycle of the system, from planning and developing through operations and maintenance. Increased understanding of IT security requirements along with improved accountability will assist program officials in successfully securing their programs and services. OMB will continue to reinforce the responsibilities of agency program officials and CIOs via management and budget processes.

Additionally, OMB is working with federal agencies to ensure that CIOs have the necessary authority to ensure effective information security throughout the agency. This authority includes:

- Establishing and enforcing department-wide information system security policies, protocols and procedures;
- Approving IT investments, including proposed investments in information security;
- Managing the activities of component (e.g., bureau) CIOs;
- Regularly monitoring the security of all department systems and networks;
- Establishing and routinely updating department business continuity plans;
- Ensuring appropriate information security staffing and ongoing commitment to training throughout the department; and
- Ensuring the appropriate level of security awareness, including adherence to policies, protocols and procedures, throughout the department.

In FY 2002, OMB found that more Departments are exercising greater oversight over their bureaus. Additionally, nearly all agencies have designated a senior information security officer.

Improving Security Education and Awareness

Through the Administration's "GoLearn" e-government initiative on establishing and delivering electronic training, IT security courses were made available to all Federal agencies in late 2002. Initial courses were targeted to CIOs and program managers with additional courses to be added for IT security managers, and the general workforce. Agencies have also conducted on-site information security training sessions for their employees.

OMB Guidance on the Federal Information Security Management Act

GISRA, as well as its successor, FISMA, have both been instrumental in improving the state of Federal IT security. The framework and processes in law and OMB policy have underlined the importance of management, implementation, evaluation, and remediation to achieving real IT security progress.

OMB guidance to agencies and IGs on reporting the results of annual security reviews is largely consistent with the previous year's GISRA guidance. The guidance highlights the differences between GISRA and FISMA and reinforces the need for accountability through performance measures. The guidance also targets IG actions to assess agency remediation efforts. Accordingly, each IG will assess the existence of a Department-wide remediation process.

Integrating Security into Capital Planning and Investment Control

OMB continues to actively work with federal agencies to ensure they incorporate security into the capital planning and investment control process. The FY 2004 President's Budget established the goal that by the end of 2003, 80% of the Federal government's FY 2004 major IT investments will appropriately integrate security into the lifecycle of the investment.

Agencies have been instructed to report on their compliance with security requirements, i.e. development of security plans and certification and accreditation activities, when requesting funds for major systems. Failure to appropriately incorporate security in new and existing IT investments automatically requires the business case to be scored as "at-risk". As a result, that system is not approved for the fiscal year in which the funds were requested until the security weaknesses are addressed. There are approximately 495 systems in the FY 2004 budget at-risk either solely or in part due to IT security weaknesses. Most of these weaknesses can be found in operational systems that either have never been certified and accredited or systems that possess out-of-date certification and accreditation.

Many agencies are not adequately prioritizing their IT investments and therefore are seeking funding to develop new systems while significant security weaknesses exist in their legacy systems. OMB will assist agencies in reprioritizing their resources through the budget process.

Spending on IT security continues to increase. For FY 2002, Federal agencies spent about $2.7 billion from a total IT investment of about $48 billion. OMB estimates FY 2003 funding for IT security investments of $4.2 billion, and in FY 2004, Federal agencies plan to spend over $4.7 billion on IT security. Based on IT spending data and agency IT security performance, spending more on IT security does not always improve IT security performance. Rather, the key is effectively incorporating IT security in agency management actions and early in the life of IT systems.

Through the FY 2005 budget process agencies will identify the funding needed to correct specific security deficiencies that have been identified under the FISMA reporting process and included in agency POA&Ms.

Enterprise Wide Initiatives Positively Impacting Security

Federal Enterprise Architecture

In addition to agency-centric efforts, OMB is championing enterprise wide initiatives to encourage adoption of secure technologies. The Federal Enterprise Architecture (FEA) currently being developed will enable system developers to better manage security and privacy considerations. The FEA framework consists of five reference models, performance, business, information, technical and data. Each of these models will have key intersections with security as well as privacy, including:

- Performance metrics to identify and monitor progress in closing IT security gaps
- Lines of business to identify mission-critical security requirements
- Information and data by line of business to identify sensitive information that requires security and privacy protection; and
- Components and technical requirements to ensure and enhance IT security.

OMB will continue to work with agencies through the FEA framework and individual agency architectures to ensure IT security and privacy considerations are identified, prioritized, and managed.

NIST Standards and Guidelines

In 2002-2003, NIST published 12 security guidelines covering a wide variety of topics such as email, firewalls, telecommuting and contingency planning. NIST also published 10 draft guidelines for review by Federal departments and agencies concerning topics such as certification and accreditation, awareness and training, and considerations in Federal Information technology procurements. In accordance with its responsibilities under FISMA, the National Institute of Standards and Technology published draft *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standard 199). This proposed standard will be used by all agencies to categorize systems according to risk level. NIST is also drafting companion guidelines recommending the types of information systems to be included in each category as well as minimum information security requirements.

Security Testing

NIST has utilized the Cryptographic Module Validation Program (CMVP) to test a number of new algorithms that use the Advanced Encryption Standard. The CMVP has now validated over 500 modules, with another 100 or more expected within the next 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. To give a sense of the quality improvement that the program achieves, NIST statistics from the testing laboratories show that 48 percent of the modules brought in for voluntary testing had security flaws that were corrected during testing. In other words, without the NIST program, the Federal government would have had only a 50/50 chance of buying correctly implemented cryptography.

In addition, in recent years, NIST, along with many others, have worked to develop the "Common Criteria", an international standard which can be used to specify security requirements. These requirements, developed by either users or vendors, 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 National Security Agency (NSA) in a program known as the National Information Assurance Partnership (NIAP). The *National Strategy to Secure Cyberspace* calls for a review of the NIAP to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. NIST has already begun staff discussions with NSA to identify ways that they might improve the process, and to understand the resources needed for NIAP to fully succeed.

SmartBUY initiative

This month, OMB announced its SmartBUY initiative which will allow the federal government to leverage its buying power to achieve maximum cost savings on commercial software packages. Because of its widespread use, anti-virus software was among the first group of packages selected for enterprise wide licensing. Antivirus software is currently purchased using license agreements with terms and prices that vary based on volume. For one popular brand of desktop antivirus software, an agency paid $6.75 per seat, while a much larger department paid 35 cents (a 95 percent difference). It is OMB's belief that coordinated use of the best-priced software licenses will reap significant savings for the federal government.

E-Authentication Initiative

Through the E-Authentication e-government initiative, the Administration certified and accredited an e-Authentication capability early this year. Applications are in the process of being migrated to this service, which will allow for the sharing of credentials across government and allows for secure transactions, electronic signatures, and access controls

across government. OMB will also release draft e-authentication guidance for agencies which will ensure that electronic transactions have the appropriate type of authentication.

Federal Cyber Service: Scholarship for Service (SFS)

The National Science Foundation's Scholarship for Service program provides funding to colleges and universities so that they can award two year scholarships in the information assurance and computer security fields. Upon graduation, recipients must work for a federal agency for two years in fulfillment of their Federal Cyber Service commitment. Scholarship recipients are hired as information technology specialists and help to protect the U.S. Government's information infrastructure. This year, 39 graduates have been placed in federal agencies.

DHS' National Cyber Security Division

The Department of Homeland Security in implementing the President's *National Strategy to Secure Cyberspace* and the Homeland Security Act of 2002, has created the National Cyber Security Division under the Department's Information Analysis and Infrastructure Protection Directorate. The Division will provide for 7 x 24 functions, including conducting cyberspace analysis, issuing alerts and warning, improving information sharing, responding to major incidents, and aiding in national-level recovery efforts. The new division will provide additional information to OMB in support of its enforcement and compliance activities. This Division represents a significant step toward advancing the Federal government's interaction and partnership with industry and other organizations. The National Cyber Security Division builds upon the existing capabilities transferred to DHS from the former Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center, and the National Communications System. The creation of this Division strengthens government-wide processes for incident response and improves protection of critical cyber assets through maximizing and leveraging the resources of these previously separate offices.

Patch Authentication and Dissemination Capability

At the present time, thirty-seven agencies subscribe to DHS' Patch Authentication and Dissemination Capability through the Federal Computer Incident Response Center (FedCIRC). This service validates and quickly distributes corrective patches for known vulnerabilities. As part of the new NCSD, FedCIRC will continue to build upon and expand this capability.

In a June 6th article, Federal Computer Week remarked that the Bugbear worm had not adversely impacted federal agencies. The Department of Defense noted that this was because they "continuously and rapidly take proactive measures." In general, agencies have improved their protection against malicious code by installing patches, blocking executables at the firewall, and using anti-virus software with automatic updates.

Conclusion

In closing, OMB is committed to a federal government with secure information systems. Due to the significant work of Federal agencies and IGs, we are able to point to real advancement in closing the Federal government's IT security performance gaps. That said, many pervasive IT security weaknesses remain, leaving the Federal government with significant risks. OMB will continue to work with agencies, Congress and the GAO to ensure that appropriate risk-based and cost-effective IT security programs, policies and procedures are put in place.

Mr. PUTNAM. I would like to introduce our second witness and welcome our ranking member on the panel to the subcommittee hearing. We will move forward with Mr. Dacey's opening statement and then recognize Mr. Clay for his.

Mr. Dacey is currently Director of Information Security issues at the GAO. His responsibilities include evaluating information systems security in Federal agencies and corporations, including the development of related methodologies, assessing the Federal infrastructure for managing information security, evaluating the Federal Government's efforts to protect our Nation's private and public critical infrastructure from cyber threats, and identifying best security practices at leading organizations and promoting their adoption by Federal agencies.

We welcome you and your insight to the subcommittee and appreciate the work that you and GAO have done for us. You are recognized for 5 minutes.

STATEMENT OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, GENERAL ACCOUNTING OFFICE

Mr. DACEY. Thank you, Mr. Chairman and members of the subcommittee. I am pleased to be here today to discuss efforts by Federal agencies and the administration to implement GISRA and briefly discuss additional provisions of FISMA, which permanently authorized and strengthened GISRA's requirements. I will briefly summarize my written statement, which provides detail on the status and progress of these efforts.

This chart illustrates the average fiscal year 2001 and 2002 performance and related progress for 23 of the largest Federal agencies based on 6 selected performance measures detailed in OMB's fiscal year 2002 GISRA report. In summary, average improvements generally ranged from 3 to 10 percentage points for the selected measures. Our analysis excluded data for one agency that were not comparable for both years. Further, our analysis of individual agency reports showed mixed agency performance and progress, and that overall many agencies had not implemented security requirements for most of their systems. Nonetheless, the second-year implementation of GISRA yielded a number of benefits such as increased management attention to information security; important actions by the administration, such as integrating information security into the President's Management Agenda Scorecard; an increase in the types of information being reported and made available for oversight; and the establishment of a base line for measuring agency performance.

Also, in its fiscal year 2002 GISRA report, OMB highlighted actions and progress to address previously identified government-wide weaknesses as well as planned actions to address newly reported challenges.

Overall, GISRA reports continue to highlight that, as we have reported for the last several years, agencies have significant weaknesses in agency security management programs. For example, developing an effective corrective action plan is a key element of a security management program to ensure remedial action is taken to address significant deficiencies. However, of the 14 IGs who reported whether their agencies' corrective action plan addressed all

significant weaknesses, five reported that their agency's plans did include them, but nine reported that they did not include all material weaknesses.

It is important for agencies to ensure that they have the appropriate information security management structures and processes in place to strategically manage information security as well as to ensure the reliability of performance information. For example, processes to routinely provide an agency with reliable, useful and timely information for day-to-day management of information security could help to significantly improve performance. Further, continued congressional and administration oversight will undoubtedly be needed to achieve significant and sustainable results, including the implementation of new FISMA requirements.

FISMA established additional requirements that can assist agencies in implementing effective information security programs, help ensure that agencies incorporate appropriate controls and provide information for administration and congressional oversight. These requirements include the designation of and the establishment of specific responsibilities for an agency senior information security officer, implementation of minimum information security requirements for agency systems, required agency reporting to the Congress and inventories of major systems.

Successful implementation of FISMA is essential to sustaining agency efforts to identify and correct weaknesses. As FISMA is implemented, it will be important to continue efforts to establish agencywide security management programs; to certify, accredit, and regularly test systems to identify and correct all vulnerabilities; to complete development of and test contingency plans to ensure that critical systems can resume operations after an emergency; to validate agency reported information through independent evaluations; and to achieve other FISMA requirements.

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

Mr. PUTNAM. Thank you, Mr. Dacey.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at 10 a.m. EDT
Tuesday, June 24, 2003

INFORMATION SECURITY

Continued Efforts Needed to Fully Implement Statutory Requirements

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-03-852T

June 24, 2003

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-03-852T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

INFORMATION SECURITY

Continued Efforts Needed to Fully Implement Statutory Requirements

Why GAO Did This Study

Since 1996, GAO has reported that poor information security in the federal government is a widespread problem with potentially devastating consequences. Further, GAO has identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2003. To strengthen information security practices throughout the federal government, information security legislation has been enacted.

This testimony discusses efforts by federal departments and the administration to implement information security requirements mandated by law. In so doing, it examines

- overall information security weaknesses and challenges that the government faces, and the status of actions to address them, as reported by the Office of Management and Budget (OMB);
- GAO's evaluation of agency efforts to implement federal information security requirements and correct identified weaknesses; and
- new requirements mandated by the Federal Information Security Management Act of 2002 (FISMA).

www.gao.gov/cgi-bin/getrpt?GAO-03-852T.

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

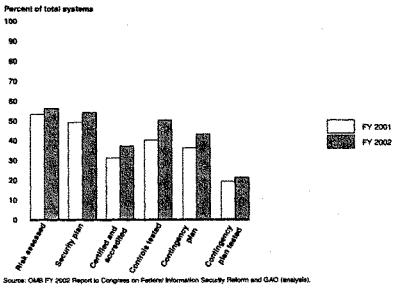
What GAO Found

Based on the fiscal year 2002 reports submitted to OMB, the federal government has made limited overall progress in implementing statutory information security requirements, although a number of benefits have resulted. Among these benefits are several actions taken and planned to address governmentwide information security weaknesses and challenges, such as lack of senior management attention. Nevertheless, as indicated by selected quantitative performance measures for the largest federal agencies, progress has been limited. Specifically, excluding data for one agency that were not comparable for fiscal years 2001 and 2002, improvements for 23 agencies ranged from 3 to 10 percentage points for the selected measures (see figure).

GAO's analyses of agencies' reports and evaluations confirmed that many agencies have not implemented security requirements for most of their systems, such as performing risk assessments and testing controls. Further, the usefulness of agency corrective action plans may be limited when they do not identify all weaknesses or contain realistic completion dates. Agencies also continue to face challenges in effectively implementing and managing their overall information security programs.

FISMA provisions establish additional requirements that, among other things, can assist agencies in implementing effective information security programs. However, attaining significant and sustainable results in implementing such requirements will also likely require processes that prioritize and routinely monitor and manage agency efforts, as well as continued congressional and administration oversight.

Performance Measure Percentages for Selected Information Security Requirements*



Source: OMB FY 2002 Report to Congress on Federal Information Security Reform and GAO (analysis).

*Excludes National Aeronautics and Space Administration data.

United States General Accounting Office

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss efforts by federal departments and agencies and the administration to implement statutory information security requirements. Since 1996,[1] we have reported that poor information security in the federal government is a widespread problem with potentially devastating consequences. Further, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2003.[2] 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, in October 2000 the Congress passed and the President signed into law Government Information Security Reform provisions (commonly known as GISRA) to strengthen information security practices throughout the federal government.[3] GISRA established information security program, evaluation, and reporting requirements for federal agencies, which are now permanently authorized and strengthened through the recently enacted Federal Information Security Management Act of 2002 (FISMA).[4]

In my testimony today, I will first summarize the federal government's overall information security weaknesses and challenges, as well as the status of the administration's efforts to address them as discussed in the May 2003 Office of Management and Budget (OMB) report to the Congress on fiscal year 2002 GISRA implementation.[5] I will also discuss the results of our evaluation of efforts by OMB and 24 of the largest federal agencies to implement federal information security requirements and correct identified weaknesses. Finally, I will describe new information security requirements contained in FISMA that can assist agencies in implementing effective information security.

In conducting this review, we analyzed OMB's May 2003 report to the Congress on GISRA implementation. We also compared the results of OMB's report with the results of our analyses of fiscal year 2002 GISRA reporting by 24 of the largest federal agencies and their inspectors general (IGs), which we had previously

[1] U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).
[2] U.S. General Accounting Office, *High Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).
[3] *Government Information Security Reform, Title X, Subtitle G, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*, P.L.106-398, October 30, 2000.
[4] *Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002*, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.
[5] Office of Management and Budget, *FY 2002 Report to Congress on Federal Government Information Security Reform.*, May 16, 2003.

reported in testimony before your subcommittee in April 2003.[6] We did not validate the accuracy of the data reported by OMB or by the agencies. We also analyzed the provisions of FISMA. We performed our work in June 2003, in accordance with generally accepted government auditing standards.

Results in Brief

In its fiscal year 2002 report to the Congress, OMB reported that the federal government had made significant strides in addressing serious and pervasive information technology (IT) security problems, but that much work remained. It highlighted actions and progress to address previously identified governmentwide weaknesses, such as lack of senior management attention to information security, as well as planned actions to address newly-reported challenges, such as agencies continuing to identify the same security weaknesses year after year. OMB also reported significant progress in agencies' IT security performance as indicated by the quantitative performance measures that OMB required agencies to report beginning in fiscal year 2002. These measures include the number of systems that have been assessed for risk, have an up-to-date security plan, and for which security controls have been tested. In particular, for selected performance measures for 24 large federal agencies, OMB's report showed increases from fiscal year 2001 to fiscal year 2002 ranging from 18 to 27 percentage points.

Although our review of GISRA implementation also showed a number of benefits resulting from this legislation, our analyses of governmentwide performance measures showed more limited overall progress. Excluding one of the 24 agencies because its performance data for these fiscal years was not comparable, our analyses showed that increases for these measures ranged from only 3 to 10 percentage points. Further, our analyses of individual agency reports showed that significant challenges remained in implementing information security requirements. For example, of the 24 agencies, 11 reported that they had assessed risk for 90 to 100 percent of their systems for fiscal year 2002, but 8 reported that they had assessed risk for less than 50 percent of their systems.

Developing effective corrective action plans is key to ensuring that remedial action is taken to address significant deficiencies. However, our analyses of agencies' OMB-required corrective action plans for fiscal year 2002, IGs' evaluations of these plans, and available quarterly updates showed that plan usefulness could be limited when plans do not identify all weaknesses, provide realistic completion estimates, or prioritize actions. For example, of 14 agency IGs

[6]U.S. General Accounting Office, *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-546T (Washington, D.C.: Apr. 8, 2003).

who reported whether their agency's corrective action plan addressed all identified significant weaknesses, 5 reported that their agency's plan did and 9 reported that it did not.

The governmentwide weaknesses identified by OMB, as well as the limited progress in implementing key information security requirements, continue to emphasize that, overall, agencies are not effectively implementing and managing their information security programs. For several years we have reported that most agencies have significant weaknesses in security program management and pointed out that agencies should implement a cycle of risk management activities—activities that are now required by law. Although agency reporting provides performance information, it is important for agencies to ensure that they have the appropriate management structures and processes in place to strategically manage information security, as well as to ensure the reliability of performance information. For example, disciplined processes can routinely provide the agency with timely, useful information for day-to-day management of information security.

FISMA provisions establish additional requirements that can assist the agencies in implementing effective information security programs, help ensure that agency systems incorporate appropriate controls, and provide information for administration and congressional oversight. These requirements include the designation of and establishment of specific responsibilities for an agency senior information security officer, implementation of minimum information security requirements for agency information and information systems, and required agency reporting to the Congress.

In addition to continued congressional and administration oversight, we believe that achieving significant and sustainable results, including the implementation of new requirements, will require agencies to integrate the use of techniques, such as corrective action plans and performance measures, into overall security management programs and processes that prioritize and routinely monitor and manage their information security efforts. Development of management strategies that identify specific actions, time frames, and required resources may also help to significantly improve performance.

Background

On October 30, 2000, the Congress enacted GISRA, which became effective November 29, 2000, for a period of 2 years. GISRA supplemented information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996, and was

consistent with existing information security guidance issued by OMB[7] and NIST,[8] as well as audit and best practice guidance issued by us.[9]

GISRA consolidated these separate requirements and guidance into an overall framework for managing information security and established new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight. GISRA assigned specific responsibilities to OMB, agency heads and chief information officers (CIOs), and IGs. OMB was responsible for establishing and overseeing policies, standards, and guidelines for information security. This included the authority to approve agency information security programs, but delegated OMB's responsibilities regarding national security systems to national security agencies. OMB was also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs. OMB released its fiscal year 2001 report in February 2002[10] and its fiscal year 2002 report in May 2003.

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

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- the development and implementation of risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained by or for the agency;
- training on security responsibilities for information security personnel and on security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;

[7]Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.
[8]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.
[9]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).
[10]Office of Management and Budget, *FY 2001 Report to Congress on Federal Government Information Security Reform*, February 2002.

- a process for identifying and remediating any significant deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- an annual program review by agency program officials.

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

For first-year GISRA implementation, OMB provided guidance to the agencies in January 2001, and in June issued final instructions on reporting results of annual agency security program reviews and inspector general independent evaluations to OMB to provide a basis for its annual report to the Congress.[11] These instructions listed specific topics that the agencies were to address in their reporting, many of which were referenced back to corresponding GISRA requirements. Agencies were to report their results to OMB in September 2001—the same time they were to submit their fiscal year 2003 budget materials. In October 2001, OMB also issued detailed guidance to the agencies on reporting their strategies for correcting the security weaknesses identified through their reviews, evaluations, and other reviews or audits performed throughout the reporting period.[12] This information was to include a "plan of action and milestones" (corrective action plan) that, among other things, listed the weaknesses; showed required resources, milestones, and completion dates; and described how the agency planned to address those weaknesses. The guidance also required agencies to submit quarterly status updates of their corrective action plans to OMB. Corrective action plans were due to OMB by the end of October, and the first quarterly updates were due January 31, 2002.

[11]Office of Management and Budget, "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; "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.
[12]Office of Management and Budget, "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.

For fiscal year 2002, OMB provided the agencies with updated reporting instructions and guidance on preparing and submitting corrective action plans.[13] Agencies were again to report their GISRA review and evaluation results to OMB in September with corrective action plans due October 1, 2002, and the next quarterly update due on January 1, 2003. Although similar to its previous guidance, in response to agency requests and recommendations we made to OMB as a result of our review of fiscal year 2001 GISRA implementation,[14] this guidance also incorporated several significant changes to help improve the consistency and quality of information being reported for oversight by OMB and the Congress. These changes included the following:

- Reporting instructions provided new high-level management performance measures that the agencies and IGs were required to use to report on agency officials' performance. These included, for example, the number and percentage of systems assessed for risk, the number and percentage of systems certified and accredited,[15] the number of contractor operations or facilities reviewed, and the number of employees with significant security responsibilities that received specialized training.

- OMB confirmed that agencies were expected to review all systems annually. It explained that GISRA requires senior agency program officials to review each security program for effectiveness at least annually, and that the purpose of the security programs discussed in GISRA is to ensure the protection of the systems and data covered by the program. Thus, a review of each system is essential to determine the program's effectiveness, and only the depth and breadth of such system reviews are flexible.

- Agencies were generally required to use all elements of NIST's *Security Self-Assessment Guide for Information Technology Systems* to review their systems unless an agency and its IG confirmed that any agency-developed methodology

[13]Office of Management and Budget, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones," Memorandum for Heads of Executive Departments and Agencies, Mitchell E. Daniels, Jr., M-02-09, July 2, 2002.
[14]U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation,* GAO-02-407 (Washington, D.C.: May 2, 2002).
[15]*Accreditation* is the authorization of an IT system to process, store, or transmit information, granted by a management official that provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. *Certification* is the comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. Certification provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. The accreditation decision is based on the implementation of an agreed upon set of management, operational, and technical controls, and by accrediting the system, the management office accepts the risk associated with it.

captured all elements of the guide.[16] The 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.

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

OMB Reports Significant Progress and Actions to Address Governmentwide Weaknesses

In its fiscal year 2002 report to the Congress, OMB stated that the federal government had made significant strides in addressing serious and pervasive IT security problems, but that more needed to be done, particularly to address both the governmentwide weaknesses identified its fiscal year 2001 report to the Congress and new challenges. Also, as discussed in a later section, OMB reported significant progress in agencies' IT security performance, primarily as indicated by the quantitative governmentwide performance measures that OMB required agencies to disclose beginning with their fiscal year 2002 reports.

OMB previously reported six common security weaknesses for the federal government. Actions and progress for these weaknesses reported by OMB in its fiscal year 2002 report were as follows:

Lack of senior management attention to information security. OMB reports that based on agencies' security reviews, remediation efforts, and IT budget materials, it either conditionally approves or disapproves agency security programs, and the OMB Director communicates this decision directly to each agency head. Further, OMB used the President's Management Agenda Scorecard to focus attention on

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

serious IT security weaknesses and, along with senior agency officials, to monitor agency progress on a quarterly basis. As a result, OMB concluded that senior executives at most agencies are paying greater attention to IT security.

Inadequate accountability for job and program performance related to IT security. OMB's instructions to federal agencies for fiscal year 2002 GISRA reporting included high-level management performance measures to assist agencies in evaluating their IT security status and the performance of officials charged with implementing specific security requirements.

Limited security training for general users, IT professionals, and security professionals. OMB stated that through the administration's "GoLearn" e-government initiative on establishing and delivering electronic training, IT security courses were available to all federal agencies in late 2002.[17] Initial courses are targeted to CIOs and program managers, with additional courses to be added for IT security managers and the general workforce.

Inadequate integration of security into the capital planning and investment control process. OMB continues to address this issue through the budget process to ensure that adequate security is incorporated directly into and funded over the life cycle of all systems and programs before funding is approved. Further, OMB stated that through this process, agencies could demonstrate explicitly how much they are spending on security and associate that spending with a given level of performance. OMB also provided agencies with guidance in determining the security costs of their IT investments.

Poor security for contractor-provided services. Through the administration's Committee on Executive Branch Information Systems Security of the President's Critical Infrastructure Protection Board (since eliminated), an issue group was created to review this problem and develop recommendations for its resolution, to include addressing how security is handled in contracts themselves. This issue is currently under review by the Federal Acquisition Regulatory Council to develop, for governmentwide use, a clause to ensure that security is appropriately addressed in contracts.

Limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections. OMB stated that addressing this weakness begins through incident detection and reporting by individual agencies to incident response centers at the Department of Homeland Security (DHS), the FBI, the Department of Defense, or elsewhere. OMB also

[17] Launched in July 2002 by the Office of Personnel Management, the *www.golearn.gov* site offers training in a online environment.

noted that agencies must actively install corrective patches for known vulnerabilities and reported that the Federal Computer Incident Response Center (FedCIRC) awarded a contract on patch management to disseminate patches to all agencies more effectively.[18] Among other actions, OMB and the CIO Council have developed and deployed a process to rapidly identify and respond to cyber threats and critical vulnerabilities.

Although not highlighted in OMB's report, in our April 2003 testimony before this subcommittee, we identified other activities undertaken to address these common weaknesses.[19] In particular, during the past year, NIST has issued related security guidance, including

- draft guidelines on designing, developing, implementing, and maintaining an awareness and training program within an agency's IT security program;[20]
- a draft guide on security considerations in federal IT procurements, including specifications, clauses, and tasks for areas such as IT security training and awareness, personnel security, physical security, and security features in systems;[21] and
- procedures for handling security patches that provided principles and methodologies for establishing an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches.[22]

In addition to these identified weaknesses, in its fiscal year 2001 report, OMB stated that it would direct all large agencies to undertake a Project Matrix review to more clearly identify and prioritize the security needs for government assets. Project Matrix is a methodology developed by the Critical Infrastructure

[18]FedCIRC, formerly within the General Services Administration and now part of the Department of Homeland Security, was established to provide a central focal point for incident reporting, handling, prevention and recognition for the federal government. FedCIRC introduced its Patch Authentication and Dissemination Capability Program in January 2003 as a free service to federal civilian agencies. According to FedCIRC, this service provides a trusted source of validated patches and notifications on new threats and vulnerabilities that have potential to disrupt federal government mission critical systems and networks. It is a Web-enabled service that obtains patches from vendors, validates that the patch only does what it states that it was created to correct, and provides agencies notifications based on established profiles.

[19]GAO-03-564T.

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

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

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

Assurance Office (CIAO) (recently transferred to the Department of Homeland Security) that identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector.[23] OMB reported that once reviews have been completed at each large agency, it would identify cross-government activities and lines of business for Project Matrix reviews so that it will have identified both vertically and horizontally the critical operations and assets of the federal government's critical enterprise architecture and their relationship beyond government. In its fiscal year 2002 report, OMB acknowledged this requirement, but did not assess agencies' overall progress or indicate a goal for when this process will be complete. As we testified in April 2003, 14 agencies reported they had identified their critical assets and operations—10 using Project Matrix and 4 using other methodologies. Five more agencies reported that they were in some stage of identifying their critical assets and operations, and three more planned to do so in fiscal year 2003. However, this process may take several more years to complete because OMB has not established any deadlines for the completion of Project Matrix reviews.

OMB's fiscal year 2002 report also identifies several additional governmentwide issues and trends as concerns. These are as follows:

- Agencies identify the same security weaknesses year after year, such as a lack of system-level security plans. OMB reports that it will assist agencies in prioritizing and reallocating funds to address these problems.
- Some IGs and CIOs have vastly different views of the state of the agency's security programs, and OMB reports that it will highlight such discrepancies to agency heads.
- Many agencies are not adequately prioritizing their IT investments and are seeking funding to develop new systems while significant security weaknesses exist in their legacy systems. OMB reports that it will assist agencies in reprioritizing their resources through the budget process.
- Based on the information in the reports, not all agencies are successfully reviewing all programs and systems each year, as required by information security law.

[23]The Project Matrix methodology defines "critical" as the responsibilities, assets, nodes, and networks that, if incapacitated or destroyed, would jeopardize the nation's survival; have a serious, deleterious effect on the nation at large; adversely affect large portions of the American populace; and require near-term, if not immed remediation (currently defined as within 72 hours). It defines "assets" as tangible equipment, applications, an facilities that are owned, operated, or relied upon by the agency, such as information technology systems or networks, buildings, vehicles (aircraft, ships, or land), satellites, or even a team of people.

- More agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure, rather than thinking of IT security as the responsibility of a single agency official or the agency's IT security office.

As part of its fiscal year 2002 report, OMB listed five areas in which it will continue to work with agencies to ensure progress in safeguarding the federal government's information and systems: (1) the plan of action and milestones process, (2) IT security performance measures, (3) the President's Management Agenda Scorecard, (4) governmentwide milestones for IT security, and (5) the threat and vulnerability response process. Key actions identified for these areas include the following:

- To ensure that remediation plans continue to be developed, implemented, and corrective actions prioritized and tracked, OMB guidance will instruct IGs, as part of their fiscal year 2003 FISMA work, to assess whether each agency has in place a robust agencywide plan of action and milestone process. A robust process, verified by agency IGs, is one of three criteria agencies must meet to "get to green" for security on the Expanding E-Government Scorecard.
- To assist agencies and OMB in better tracking progress, along with their plan of action and milestone updates, agencies will also be required to begin quarterly reporting of their status against the OMB-prescribed IT security performance measures.
- OMB set targeted milestones for improvement for some of the critical IT security weaknesses in the President's FY 2004 budget. Targets for improvement include that by the end of 2003
    - all agencies are to have an adequate agencywide process in place for developing and implementing program- and system-level plans,
    - 80 percent of federal IT systems shall be certified and accredited, and
    - 80 percent of the federal government's fiscal year 2004 major IT investments shall appropriately integrate security into the life cycle of the investment.

Agencies Show Limited Progress in Implementing Security Requirements

Our analyses of agency performance measure data and individual agencies' efforts to implement information security requirements showed limited progress in many cases. This limited progress is indicated despite other benefits that that have resulted from GISRA implementation, such as increased management attention to and accountability for information security; important actions by the administration, such as integrating information security into the President's Management Agenda Scorecard; an increase in the types of information being reported and made available for oversight: and the establishment of a baseline for measuring agencies' performance.[24]

As mentioned previously, for fiscal year 2002 OMB required agencies to report performance measure data related to key information security requirements, such as assessing systems for risk and having up-to-date system security plans. Summarizing these data for 24 large federal agencies and comparing results between fiscal years 2001 and 2002, OMB reported in its fiscal year 2002 report that these data indicated that agencies had made significant progress. Table 1 shows the governmentwide results of this analysis reported by OMB for selected performance measures, which indicates improvements for these measures ranging from 18 to 27 percentage points.

Table 1: Comparison of Fiscal Year 2001 and Fiscal Year 2002 Performance Measure Data for 24 Large Federal Agencies

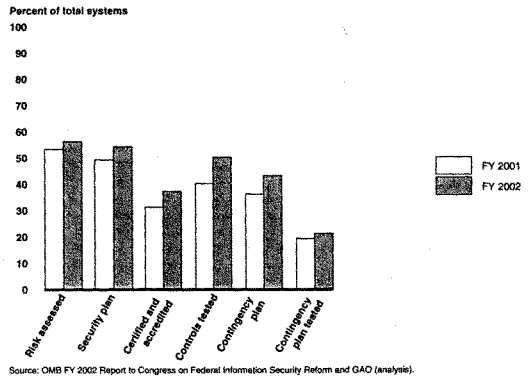
	Number of systems													
	Total		Assessed for risk and assigned a level of risk		Have an up-to-date IT security plan		Authorized for processing following certification & accreditation		Security controls have been tested and evaluated in the last year		Have a contingency plan		Contingency plan has been tested	
Year	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02
Number of systems	7,411	7,957	3,195	5,160	2,986	4,930	1,953	3,772	2,447	4,751	2,221	4,342	1,228	2,768
Percentage of total systems			43	65	40	62	26	47	33	60	30	55	17	35
Difference from FY01 to FY02	+546 systems		+22%		+22%		+21%		+27%		+25%		+18%	

Source: OMB *FY 2002 Report to Congress on Federal Government Information Security Reform* and GAO (analysis).

[24]U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Refon.. Legislation,* GAO-02-470T (Washington, D.C.: Mar. 6, 2002); GAO-03-564T.

However, our analyses showed that most agencies experienced more limited progress than the OMB analysis indicates. Specifically, excluding data for the National Aeronautics and Space Administration (NASA), our analysis showed that increases for these same measures only ranged from 3 to 10 percent. NASA's performance measure data were excluded because fiscal year 2001 data were based on a sample of 221 of its most critical systems, but were compared with data for its total of 1,641 systems for fiscal year 2002. As a result, including NASA data significantly affected the overall levels of governmentwide progress shown. Figure 1 shows the percentage change in performance measures based on our analysis, excluding data for NASA.

Figure 1: Performance Measure Percentages for Selected Information Security Requirements*



Source: OMB FY 2002 Report to Congress on Federal Information Security Reform and GAO (analysis).
*Excludes data for NASA.

In addition to the impact of the NASA data, the performance data reported by the Department of Defense (DOD) also represents only a small sample of the thousands of systems DOD identified in total for the department, and could significantly affect overall governmentwide results if data on all systems were available. DOD reported that because of its size and complexity, the collection of specific metrics required sizable lead time to allow for the collection and approval process by each military service and agency. For this reason, DOD focused its

fiscal year 2002 GISRA efforts on (1) a sample of 366 of its networks and (2) a sample of 155 systems that were selected from the sample of systems used for DOD's fiscal year 2001 GISRA review. It is these 155 systems for which DOD reported performance measure data.

In addition to the our analysis of these overall performance measures, we analyzed fiscal year 2002 GISRA reports by the 24 agencies and focused on the status of individual agencies in implementing federal information security requirements related to these and other measures. These analyses showed mixed agency progress but overall, many agencies still had not established information security programs that implement these requirements for most of their systems. Summaries of our analyses for selected information security requirements and reported performance measures follow.[25]

Many Systems Do Not Have Risk Assessments

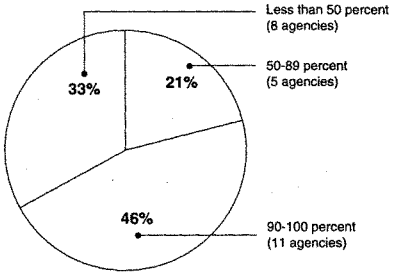
Agencies are required to perform periodic threat-based risk assessments for systems and data. Risk assessments are an essential element of risk managemen and overall security program management and, as our best practice work has shown, are an integral part of the management processes of leading organizations.[26] Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls. Our reviews of federal agencies, however, frequently show deficiencies related to assessing risk, such as security plans for major systems that are not developed on the basis of risk. 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's performance measure for this requirement mandated that agencies report the number and percentage of their systems that have been assessed for risk during fiscal year 2001 and fiscal year 2002. Our analyses of reporting for this measure showed some overall progress. For example, of the 24 agencies, 13 reported an increase in the percentage of systems assessed for fiscal year 2002 compared with fiscal year 2001. In addition, as illustrated in figure 2, for fiscal

[25]In performing our analyses, we summarized and categorized the reported information including data provided for the OMB-prescribed performance measures. There were several instances where agency reports either did not address or provide sufficient data for a question or measure. In addition, IGs' independent evaluations sometimes showed different results than CIO reporting or identified data inaccuracies. Further, IG reporting also did not always include comparable data, particularly for the performance measures. In part, this was because although OMB instructions said that the IGs should use the performance measures to assist in evaluating age officials' performance, the IG was not required to review the agency's reported measures.
[26]GAO/AIMD-98-68.

year 2002, 11 agencies reported that they had assessed risk for 90 to 100 percent of their systems. However, figure 2 also shows that further efforts are needed by other agencies, including the 8 that reported that less than 50 percent of their systems had been assessed for risk.

Figure 2: Percentage of Systems with Risk Assessments during Fiscal Year 2002



Source: Agency-reported data.

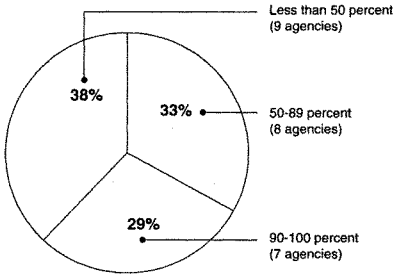
Systems Lack Up-to-Date Security Plans

An agency head is required to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. In its reporting instructions, OMB required agencies to report whether the agency head had taken specific and direct actions to oversee that program officials and the CIO are ensuring that security plans are up to date and practiced throughout the life cycle. Agencies also had to report the number and percentage of systems that had an up-to-date security plan. Our analyses showed that although most agencies reported that they had taken such actions, IG reports disagreed for a number of agencies, and many systems do not have up-to-date security plans. Specifically, 21 agencies reported that the agency head had taken actions to oversee that security plans are up to date and practiced throughout the life cycle. In comparison, of the 21 IGs that addressed this issue, 9 reported such actions had been taken and 12 reported that they had not. One IG reported that the agency's security plan guidance

predates revisions to NIST and OMB guidance and, as a result, does not contain key elements, such as the risk assessment methodology used to identify threats and vulnerabilities. In addition, another IG reported that although progress had been made, security plans had not been completed for 62 percent of the agency's systems.

Regarding the status of agencies' security plans, as shown in figure 3, 9 of the 24 agencies reported that they had up-to-date security plans for less than 50 percent of their systems for fiscal year 2002. Of the remaining 15 agencies, 7 reported up-to-date security plans for 90 percent or more of their systems.

Figure 3: Percentage of Systems with Up-to-Date Security Plans during Fiscal Year 2002



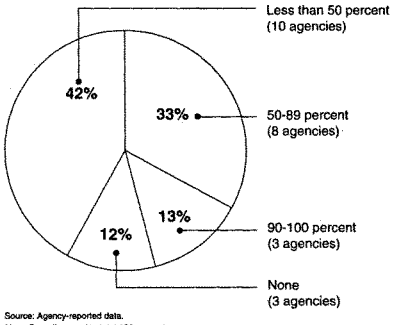
Source: Agency-reported data.

System Certification and Accreditation Remains a Problem

As one of its performance measures for agency program official responsibilities, OMB required agencies to report the number and percentage of systems that have been authorized for processing following certification and accreditation. Our analysis of agencies' reports showed mixed progress for this measure. For example, 10 agencies reported increases in the percentage of systems authorize for processing following certification and accreditation compared with fiscal ye

2001, but 8 reported decreases and 3 did not change (3 others did not provide sufficient data). In addition, as shown in figure 4, 11 agencies reported that for fiscal year 2002, 50 percent or more of their systems had been authorized for processing following certification and accreditation, with only 3 of these reporting from 90 to 100 percent. And of the remaining 13 agencies reporting less than 50 percent, 3 reported that none of their systems had been authorized.

Figure 4: Percentage of Systems during Fiscal Year 2002 that are Authorized for Processing by Management after Certification and Accreditation



Source: Agency-reported data.
Note: Rounding used to total 100 percent.

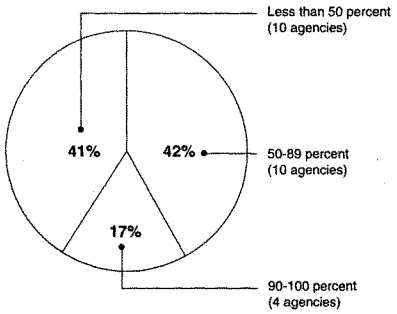
In addition to this mixed progress, IG reports identified instances in which agencies' certification and accreditation efforts were inadequate. For example, one agency reported that 43 percent of its systems were authorized for processing following certification and accreditation. IG reporting agreed,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

Further Security Control Testing and Evaluation Needed

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

As a performance measure for this requirement, OMB required agencies to report the number and percentage of systems for which security controls have been tested and evaluated during fiscal years 2001 and 2002. Our analyses of the data agencies reported for this measure showed that although 15 agencies reported an increase in the overall percentage of systems being tested and evaluated for fiscal year 2002, most agencies are not testing all of their systems. As shown in figure 5, our analyses showed that 10 agencies reported that they had tested the controls of less than 50 percent of their systems for fiscal year 2002. Of the remaining 14 agencies, 4 reported that they had tested and evaluated controls for 90 percent or more of their systems.

Figure 5: Percentage of Systems with Security Controls Tested during Fiscal Year 2002



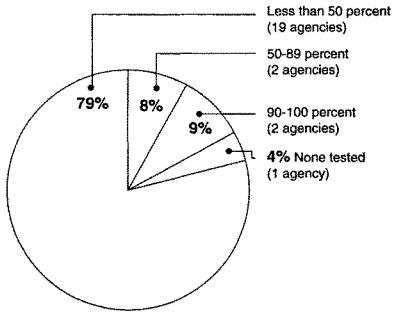
Source: Agency-reported data.
Note: Rounding used to total 100 percent.

Lack of Contingency Plan Testing Is a Major Weakness

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

As another of its performance measures, OMB required agencies to report the number and percentage of systems for which contingency plans have been tested in the past year. As shown in figure 6, our analyses indicated that for fiscal year 2002, only 2 agencies reported that they had tested contingency plans for 90 percent or more of their systems, and 19 had tested contingency plans for less than 50 percent of their systems. One reported that none had been tested.

Figure 6: Percentage of Systems with Recently Tested Contingency Plans for Fiscal Year 2002



Source: Agency-reported data.
Note: Rounding used to total 100 percent.

Security Training Efforts Show Mixed Progress

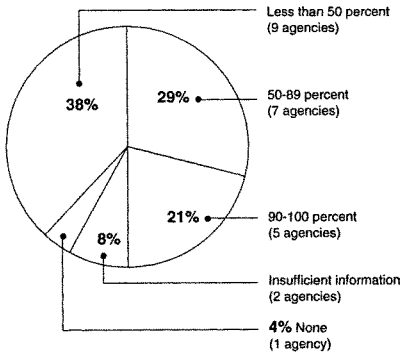
Agencies are required to provide training on security awareness for agency personnel and on security responsibilities for information security personnel. Our studies of best practices at leading organizations have shown that such organizations took steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed. They also recognized that staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. However, our past information security reviews at individual agencies have shown that they have not provided adequate computer security training to their employees, including contractor staff.

Among the performance measures for these requirements, OMB mandated that agencies report the number and percentage of employees—including contractors—who received security training during fiscal years 2001 and 2002, and the number of employees with significant security responsibilities who received specialized training. Our analyses showed that 16 agencies reported th they provided security training to 50 percent or more of their employees and

contractors for fiscal year 2002, with 9 reporting 90 percent or more. Of the remaining 8 agencies, 4 reported that such training was provided for less than half of their employees/contractors, 1 reported that none were provided with this training, and 3 provided insufficient data for this measure.

For specialized training for employees with significant security responsibilities, some progress was indicated, but additional training is needed. As indicated in figure 7, our analyses showed that 12 agencies reported that 50 percent or more of their employees with significant security responsibilities had received specialized training for fiscal year 2002, with 5 reporting 90 percent or more. Of the remaining 12 agencies, 9 reported that less than half of such employees received specialized training, 1 reported that none had received such training, and 2 provided insufficient data for this measure.

Figure 7: Percentage of Employees with Significant Security Responsibilities Receiving Specialized Security Training during Fiscal Year 2002



Source: Agency-reported data.

Incident-Handling Capabilities Established, but Implementation Incomplete

Agencies are required to implement procedures for detecting, reporting, and responding to security incidents. Although even strong controls may not block all intrusions and misuse, organizations can reduce the risks associated with such events if they promptly take steps to detect intrusions and misuse before significant damage can be done. In addition, accounting for and analyzing security problems and incidents are effective ways for an organization to gain a better understanding of threats to its information and of the cost of its security-related problems. Such analyses can also pinpoint vulnerabilities that need to be addressed to help ensure that they will not be exploited again. In this regard, problem and incident reports can provide valuable input for risk assessments, help in prioritizing security improvement efforts, and be used to illustrate risks and related trends in reports to senior management.

Our information security reviews also confirm that federal agencies have not adequately (1) prevented intrusions before they occur, (2) detected intrusions as they occur, (3) responded to successful intrusions, or (4) reported intrusions to staff and management. Such weaknesses provide little assurance that unauthorized attempts to access sensitive information will be identified and appropriate actions taken in time to prevent or minimize damage.

OMB included a number of performance measures in agency reporting instructions that were related to detecting, reporting, and responding to security incidents. These included the number of agency components with an incident-handling and response capability, whether the agency and its major components share incident information with FedCIRC in a timely manner, and the numbers of incidents reported. OMB also required that agencies report on how they confirmed that patches have been tested and installed in a timely manner.

Our analyses of agencies' reports showed that although most agencies reported that they have established incident-response capabilities, implementation of these capabilities is still not complete. For example, 12 agencies reported that for fiscal year 2002, 90 percent or more of their components had incident handling and response capabilities and 8 others reported that they provided these capabilities to components through a central point within the agency. However, although most agencies report having these capabilities for most components, in at least two cases, the IGs' evaluations identified instances in which incident-response capabilities were not always implemented. For example, one IG reported that the agency established and implemented its computer security incident-response capability on August 1, 2002, but had not enforced procedures to ensure that components comply with a consistent methodology to identify, document, and report computer security incidents. Another IG reported that the agency had

released incident-handling procedures and established a computer incident-response team, but had not formally assigned members to the team or effectively communicated procedures to employees.

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

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

Agencies are required to develop and implement risk-based, cost-effective policies and procedures to provide security protection for information collected or maintained either by the agency or for it by another agency or contractor. In its fiscal year 2001 GISRA report to the Congress, OMB identified poor security for contractor-provided services as a common weakness and for fiscal year 2002 reporting, included performance measures to help indicate whether the agency program officials and CIO used appropriate methods, such as audits and inspections, to ensure that service provided by a contractor are adequately secure and meet security requirements.

Our analyses showed that a number of agencies reported that they have reviewed a large percentage of services provided by a contractor, but others have reviewed only a small number. For operations and assets under the control of agency program officials, 17 agencies reported that for fiscal year 2002 they reviewed 50 percent or more of contractor operations or facilities, with 7 of these reporting that they reviewed 90 percent or more. Four agencies reported that they had reviewed less than 30 percent of contractor operations or facilities.

For operations and assets under the control of the CIO, 13 agencies reported that for fiscal year 2002 they reviewed 50 percent or more of contractor operations or facilities, with 7 of these reporting that they reviewed 90 percent or more. Of the remaining agencies, 3 reported that they reviewed less than 30 percent of contractor operations or facilities and 5 reported that they had no services provided by a contractor or another agency.

Processes Needed to Ensure Effective Corrective Actions

Developing effective corrective action plans is key to ensuring that remedial action is taken to address significant deficiencies. Further, a centralized process for monitoring and managing remedial actions enables the agency to identify trends, root causes, and entitywide solutions. OMB has required agency heads to work with CIOs and program officials to provide a strategy to correct security weaknesses identified through annual program reviews and independent evaluations, as well as other reviews or audits performed throughout the reporting period by the IG or us. Agencies are also required to submit corrective action plans for all programs and systems where a security weakness has been identified. OMB guidance requires that these plans list the identified weaknesses and, for each, identify a point of contact, the resources required to resolve the weakness, the scheduled completion date, key milestones with completion dates for the milestones, milestone changes, the source of the weakness (such as a program review, IG audit, or GAO audit), and the status (ongoing or completed). Agencies are also required to submit quarterly updates of these plans that list th total number of weaknesses identified at the program and system levels, as well as the numbers of weaknesses for which corrective actions were completed on time, ongoing and on schedule, or delayed. Updates are also to include the number of new weaknesses discovered subsequent to the last corrective action plan or quarterly update.

As reported in its fiscal year 2002 report to the Congress, OMB requires that agencies establish and maintain an agencywide process for developing and implementing program- and system-level corrective action plans and that these plans serve as an agency's authoritative management tool to ensure that program- and system-level IT security weaknesses are remediated. In addition, OMB requires that every agency maintain a central process through the CIO's office to monitor agency remediation activity.

Our analyses of agencies' fiscal year 2002 corrective action plans, IGs' evaluations of these plans, and available quarterly updates showed that the usefulness of these plans as part of agency management's overall process to identify and correct their information security weaknesses could be limited when they do not identify all weaknesses or provide realistic completion estimates. For example, of 14 agency IGs that reported on whether or not their agency's corrective action plan addressed all identified significant weaknesses, only 5 reported that their agency's plan did so, and 9 specifically reported that their agency's plan did not. Further, in several instances, corrective action plans did not indicate the current status of weaknesses identified or include information regarding whether actior were on track as originally scheduled.

In addition, most agencies did not indicate the relative priority of weaknesses for corrective action. As a result, it was difficult to determine whether an agency's actions are focused on achieving results for its most significant weaknesses. Further, three IGs reported that their agencies did not have a centralized tracking system to monitor the status of corrective actions, and one IG specifically questioned the accuracy of unverified, self-reported corrective actions reported in the agency's plan.

In its report, OMB highlighted several actions that may help to address such concerns. For example, OMB reported that since completion of their fiscal year 2002 reviews, agencies have been working to prioritize their IT security weaknesses. In addition, OMB stated that fiscal year 2003 FISMA reporting guidance would direct agency IGs to verify whether an agency has a central process to monitor remediation, as required by OMB.

Agencies Face Continuing Challenges to Implement Effective Information Security Management Programs

The governmentwide weaknesses identified by OMB in its reports to the Congress, as well as the limited progress in implementing key information security requirements, continue to emphasize that agencies have not effectively implemented programs for managing information security. For the past several years, we have analyzed the audit results for 24 of the largest federal agencies and found that all 24 had significant weaknesses in the policies, procedures, and technical controls that apply to all or a large segment of their information systems and help ensure their proper operation. In particular, our analyses in both 2001 and 2002 found that all 24 had weaknesses in security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls. Security program management covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.[27]

Establishing a strong security management program requires that agencies take a comprehensive approach that involves both (1) senior agency program managers who understand which aspects of their missions are the most critical and

[27]U.S. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001); and *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, GAO-03-303T (Washington, D.C.: Nov. 19, 2002).

sensitive and (2) technical experts who know the agencies' systems and can suggest appropriate technical security control techniques. We studied the practices of organizations with superior security programs and summarized our findings in a May 1998 executive guide entitled *Information Security Management: Learning From Leading Organizations*.[28] Our study found that these organizations managed their information security risks through a cycle of risk management activities. These activities, which are now among the federal government's statutory information security requirements, included

- assessing risks and determining protection needs,
- selecting and implementing cost-effective policies and controls to meet those needs,
- promoting awareness of policies and controls and of the risks that prompted their adoption among those responsible for complying with them, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action.

Although GISRA reporting provides performance information on these areas, it is important for agencies to ensure that they have the appropriate management structures and processes in place to strategically manage information security, as well as ensure the reliability of performance information. For example, disciplined processes can routinely provide the agency with timely, useful information for day-to-day management of information security. Also, development of management strategies that identify specific actions, time frames, and required resources may help to significantly improve performance.

FISMA Provisions Can Strengthen Information Security Implementation

With GISRA expiring on November 29, 2002, FISMA was enacted on December 17, 2002, to permanently authorize and strengthen the information security program, evaluation, and reporting requirements established by GISRA. In particular,

[28]GAO/AIMD-98-68.

FISMA provisions established additional requirements that can assist the agencies in implementing effective information security programs, help ensure that agency systems incorporate appropriate controls, and provide information for administration and congressional oversight. These specific requirements are described and discussed below.

Designating a Senior Agency Information Security Officer

FISMA requires an agency's CIO to designate a senior agency information security officer who, for the agency's FISMA-prescribed information security responsibilities, shall

- carry out the CIO's responsibilities;
- possess professional qualifications, including training and experience, required to administer the required functions;
- have information security duties as that official's primary duty; and
- head an office with the mission and resources to assist in ensuring agency compliance.

In contrast, GISRA required the CIO to designate a senior agency information security official, but did not specify the responsibilities, qualifications, or other requirements for this position. Agencies' fiscal year 2002 GISRA reports showed that the CIOs had designated a senior agency information security official for 22 of the 24 agencies (the remaining 2 agencies' reports did not indicate whether they had designated such an official), but OMB did not require the agencies to report any additional information on the responsibilities of this official.

Developing, Maintaining, and Updating an Inventory of Major Information Systems

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

implementation of this requirement. Although GISRA did not specifically require that agencies maintain an inventory of major information systems, OMB reporting instructions for fiscal year 2002 did require agencies to report the total number of agency systems, and most agencies reported a total number in their GISRA reports. However, six IGs specifically reported problems with the completeness of their agencies' system inventories.

NIST Development of Standards and Guidelines

FISMA includes a number of requirements for NIST to develop security-related standards and guidelines. These include, for systems other than those dealing with national security, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels, (2) guidelines recommending the types of information and information systems to be included in each category, and (3) minimum information security requirements information and information systems in each category.

For the first of these requirements—standards for security categorization—NIST is to submit the standards to the Secretary of Commerce for promulgation no later than 12 months after enactment (December 17, 2003). The guidelines on the types of information and information systems to be included in each category are required to be issued no later than 18 months after enactment (June 17, 2004). The minimum information security requirements are required to be submitted to the Secretary for promulgation no later than 36 months after enactment (December 17, 2005).

On May 16, 2003, NIST issued an initial public draft of the standards for security categorization for comment.[29] These proposed standards would establish three levels of risk—**low**, **moderate**, and **high**[30]—and would categorize information and

[29]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUB) 199, Initial Public Draft, Version 1.0, May 2003.

[30]As defined in the draft NIST standard, the level of risk is **low** if an event could be expected to have a limited adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals; and cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs. The level of risk is **moderate** if an event could be expected to have a serious adverse effect on agency operations, agency assets, or individuals; and cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs. The level of risk is **high** if an event could be expected to have a severe or catastrophic adverse effect on agency operation, agency assets, or individuals; and cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

information systems with respect to security by having an agency assign the appropriate level of risk to each of three security objectives: (1) **confidentiality**, defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information; (2) **integrity**, defined as guarding against improper information modification or destruction, and including ensuring information nonrepudiation and authenticity; and (3) **availability**, defined as ensuring timely and reliable access to and use of information. Also according to the draft standard, because an information system may contain more than one type of information that is subject to security categorization (such as privacy information, medical information, proprietary information, financial information, and contractor-sensitive information), the security categorization of an information system that processes, stores, or transmits multiple types of information should be at least the highest risk level that has been determined for each type of information for each security objective, taking into account dependencies among the objectives.

FISMA also requires NIST to develop, in conjunction with the Department of Defense, including the National Security Agency, guidelines for identifying an information system as a national security system. On June 3, 2003, NIST released a draft working paper of these guidelines that provides the basis and method for identifying national security systems, including agency determination and reporting responsibilities.[31]

Agency Reporting to the Congress

For non-national-security programs, GISRA required those performing the annual independent evaluations (essentially the IGs) to report the results of their evaluations to OMB and required OMB to summarize these results in an annual report to the Congress. In addition, OMB required the agencies to report the results of their annual GISRA security reviews of systems and programs. FISMA now requires agencies to report annually to OMB, as well as to the House Committees on Government Reform and Science; the Senate Committees on Governmental Affairs and Commerce, Science, and Transportation; the appropriate congressional authorizing and appropriations committees; and the Comptroller General; on the adequacy and effectiveness of information security policies, procedures, and practices, including compliance with each of FISMA's requirements for an agencywide information security program.

[31]National Institute of Standards and Technology, *Guideline for Identifying an Information System as a National Security System*, NIST Special Publication 800-59, Draft, Version 0.3, June 3, 2003.

In summary, with few exceptions, agencies' implementation of federal information security requirements has not yet shown significant progress. Legislation, congressional oversight like today's hearing, and efforts by OMB through the budget process, the President's Management Agenda Scorecard, and other tools, such as corrective action plans and performance measures, have all contributed to increasing agency management's attention to information security. Also, new techniques, such as establishing governmentwide performance goals and quarterly reporting of performance measures, may help to further encourage agency progress and facilitate congressional and administration oversight.

However, in addition to these steps, achieving significant and sustainable results will likely require agencies to integrate such techniques into overall security management programs and processes that prioritize and routinely monitor and manage their information security efforts. These programs and processes must focus on implementing statutory security requirements, including performing risk assessments, testing and evaluating controls, and identifying and correcting weaknesses to ensure that the greatest risks have been identified, security controls have been implemented to address these risks, and that critical operations can continue when unexpected events occur. Development of management strategies that identify specific actions, time frames, and required resources may also help to significantly improve performance. Further, agencies will need to ensure that systems and processes are in place to provide information and facilitate the day-to-day management of information security throughout the agency, as well as to verify the reliability of reported performance information.

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

(310194)

Mr. PUTNAM. I would also like to recognize and thank Ms. Watson for joining the subcommittee and recognize the ranking member for his opening statement.

Mr. Clay, you are recognized for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman, for calling this hearing. I have asked my staff to put up a poster that is from the last computer security hearing held by the Subcommittee on Government Efficiency in the 107th Congress. The majority staff, working from the same agency reports that are the basis of the OMB report issued last month, created this report card. However, the story this report details is quite different from the more optimistic tone laid out by the administration.

Of the 24 agencies examined, 12 showed no improvement in computer security, and 11 of those agencies had a grade of F in both 2001 and 2002. Those agencies include the General Services Administration, which had a grade of D both years; the Departments of Agriculture, Defense, Energy, Interior, Justice, Transportation, Treasury and Veterans Affairs; the Agency for International Development; the Office of Personnel Management; and Small Business Administration. Other agencies showed dramatic decline in grade. For example, the National Science Foundation went from a B plus in 2001 to a D minus in 2002. The National Aeronautics and Space Administration went from a C minus to a D plus. The Environmental Protection Agency went from a D plus to a D minus. The Department of State went from a D plus to an F. The Federal Emergency Management Agency went from a D to an F. And the Department of Housing and Urban Development went from a D to an F. However, if we look at the chart on page 11 of the administration's report, the government is improving on nearly every indicator.

One conclusion might be that the agencies have done a lot of work between last November and now. Unfortunately, this report card and the OMB report are drawn from the exact same agency report. Last week I sent my staff over to the Department of Transportation, which, according to this report card, is one of the failing agencies, and they came back with a report of an agency that was making significant improvement in computer security. In fact, the Department of Transportation may well be a leader in implementing the requirements of the Federal Information Security Management Act. I hope today we can learn why we have such different summaries on the same agency report.

And again, thank you, Mr. Chairman, and my thanks to the witnesses for taking their time to be here today.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

STATEMENT OF THE HONORABLE WM. LACY CLAY
AT THE HEARING ON
COMPUTER SECURITY

JUNE 24, 2003

Thank you Mr. Chairman for calling this hearing. I have asked my staff to put up the poster that is from the last computer security hearing held by the Subcommittee on Government Efficiency in the 107th Congress.

The majority staff working from the same agency reports that are the basis of the OMB report issued last month created this report card. However, the story this report card tells is quite different from the more optimistic tone laid out by the administration.

Twelve of the 24 agencies examined showed no improvement in computer security, and eleven of those agencies had a grade of F in both 2001 and 2002. Those agencies include the General Services Administration (which had a grade of D both years); the Departments of Agriculture, Defense, Energy, Interior, Justice, Transportation, Treasury, and Veterans Affairs; the Agency for International Development; the Office of Personnel Management; and the Small Business Administration.

Other agencies showed dramatic decline in grade. For example, the National Science Foundation went from a B+ in 2001 to a D- in 2002. The National Aeronautics and Space Administration went from a C- to a D+; the Environmental Protection Agency went from a D+ to a D-; the Department of State went from a D+ to an F; the Federal Emergency Management Agency went from a D to an F; and the Department of Housing and Urban Development went from a D to an F.

However, if we look at the chart on page 11 of the administration's report, the government is improving on nearly every indicator. One conclusion might be that the agencies have done a lot of work between last November and now. Unfortunately, this report card, and the OMB report are drawn from the exact same agency reports.

Last week, I sent my staff over to the Department of Transportation, which according to this report card is one of the failing agencies, and they came back with a report of an agency that was making significant improvement in computer security. In fact, the Department of Transportation may well be a leader in implementing the requirements of the Federal Information Security Management Act.

I hope today we can learn why we have such different summaries of the same agency reports.

Again, thank you Mr. Chairman, and my thanks to the witnesses for taking their time to be here today.

Mr. PUTNAM. I thank the gentleman from Missouri and would recognize the gentlelady from California for her opening statement, if she would like to make one.

Ms. WATSON. Mr. Chairman, thank you. I don't have an opening statement, but I am looking at the details of the report card, and the question comes—and this is from GAO. Apparently they have described the shortfall. My question to anyone on the panel is why don't we see more progress, more upward movement in the security, and what accounts for these low grades, the grades of F?

Mr. PUTNAM. If it is OK, Ms. Watson, we will give them a heads up. We will lead off with Mrs. Miller and then come back.

At this time I recognize the vice chairwoman of the subcommittee Mrs. Miller for the first round of questions. You are recognized for 5 minutes.

Mrs. MILLER. Thank you, Mr. Chairman, I will be a few moments here, but I am new to the Congress and obviously new to the subcommittee, but I have to say that looking at that report card is rather startling when we think about the piece of educational legislation, No Child Left Behind. Fortunately we are not being graded on that kind accountability with where we are, but as a former elected official at the local level, State level, dealing with audits for the last 25 years, any time I would see the term "material weakness," you know, your heart would begin to pound. Material weakness is a bad thing, obviously.

And, Mr. Forman, I think you mentioned—I was taking some notes—over half of all the government agencies are reporting. Was that just in the last go-around, reporting material weaknesses in information security? And is that operational audits that are being conducted, performance evaluations?

Mr. FORMAN. These were part of the financial management audits where it is required, and I think, as the chairman pointed to, a good example of that would have been the Treasury Department. That was one area where as part of the reviews of the reports from the IG and the CIOs, at that time Assistant Secretary for Management Ed Kingman noticed the significant gap, tracked it down, and indeed recognized that would be a reportable or should be considered as a reportable material weakness, and I think properly handled it at that point.

Mrs. MILLER. You know, when you do certification, I think that starts with accountability. It appears as though we have some difficulty in the Federal Government of retaining CIOs. You have a revolving door going with some of these CIOs. Is this something that Congress could assist you in addressing? Could you tell us a little bit to why we have that situation? You have to have a point person, and you have to have accountability if we are losing some of our brain trusts there and the institutional knowledge is going out the door with them. What can we do there?

Mr. FORMAN. Officially we are looking at this as part of the skills gap assessment, Clinger-Cohen reports that never were really done, the Ego Vac site, we would like to make sure the agencies do that, and as well the agencies should modernize those reports. The Ego Vac did have rather strong human capital work force reporting. And we in the budget passed back to the agencies and said that those reports must come into OMB this September. So I think

sometime in the fall would be appropriate after we have had time to look at those reports.

Traditionally the issues that have come up are money-related, and the administration did ask for the performance fund. I think that will help a tremendous amount.

Now on a less than official side, the personal note, we are trying to drive an awful lot of transformation through the agencies, and these have become some of the most stressful jobs. The area is—and you will hear from some of the folks that are driving major changes. The areas that need the most change, like computer security, forces an awful lot of management reform. I think the chairman was exactly correct. This is very much a management issue, and I am not quite sure yet how you keep people from burning out, although that is something we are going to have to start looking at more and more, because we do need this magnitude of change, and we can't let that stop as the people change. We have to figure out how we deal a little better with the stress, because I would not like us to slow down on some of the transformation in this important area in particular.

Mrs. MILLER. Just a note on that, the burn-out in those kinds of jobs is not particularly inherent to the Federal Government. You find it throughout the inventory really now because there is so much stress.

Looking at some of the States that are really on the leading edge of utilizing technology, they are all struggling with the same thing that the Federal Government is, is retaining those kinds of individuals so they don't lose them off into the private sector.

But you talked about money in those kinds of things, and in the GISRA report you are saying approximately 500 systems are sort of at risk again with the security weaknesses and apparently subject to having some of their funding withheld. Is that an appropriate thing for us to be doing as a Congress? I mean, we want to encourage improvement in this report card certainly, and we don't want to be a rat holding the taxpayers' money. On the other hand, how does all of that work, with you doing your performance evaluations and withholding dollars from the agencies?

Mr. FORMAN. The framework is investment justification. We call it the business case, and the way it works is that there are a number of criteria that we know if we don't adequately address before the project really starts to ramp up, chances are we will be picking up the pieces in the end. The way that plays out in cyber security is that it costs us a lot more to go back and fix the security problems of the systems that are deployed. Had this been correctly addressed early on in the program, it would have been done much more effectively and at a lower cost. So our policy position has been until that gets built in from the beginning, we don't want the system to go forward because we know it increases both the risk and the cost of the system.

Mrs. MILLER. When you are making those kinds of determinations about withholding funding, how do you interact with the Congress as far as talking to the appropriators and those kinds of things? And is there some sort of exemption they could get if they show you measurable performance increase?

Mr. FORMAN. There are a set of criteria. It is based on NIST standards and OMB guidance, A–130, that we use, and generally that is part of the budget process discussed with the agencies via Circular A–11, the basic document used to put the budget together. That is associated with what is called an apportionment process, which is a financial term of art for how appropriations dollars are managed, and that is worked through with the appropriators.

I will say the understanding of all that as it relates to IT varies from agency to agency because so much of the IT budget is not explicitly appropriated. It is funded out of working capital. There are salaries and expenses.

Mrs. MILLER. Just a quick question.

Mr. PUTNAM. We are going to have to wrap up this first round if that is OK, Mrs. Miller.

And Mr. Clay is glad to defer to Ms. Watson, so you get another crack at it, and you are recognized for 5 minutes.

Ms. WATSON. Thank you, Mr. Chair.

I guess if I read the GAO report, I would have my questions answered, but listening very closely, I hear you really have a personal management resource factor that gets in the way of making more progress. Can you expound a bit?

Mr. FORMAN. First of all, let me say about the grade, I think there are two aspects of this: Where are you in terms of status, and how much progress are you making. And I will tell you in terms of progress, there is clear progress. We have laid out an 80 percent target, to move from 60 percent to 80 percent this year, and very much I am accountable. I am the person to hold me accountable. It helps me hold the agency accountable for that. So I am the person that has signed up to the Congress to make sure we achieve that under FISMA and the EGO VAC. And you will see some of the CIOs, there is a commitment throughout the administration making the progress, and the management commitment from the leadership level is key to making this a success. I am fairly comfortable we are making progress. We are tracking that quarterly, and you will be getting data to see that as well.

On the status side, whether it is an F or D minus, I would ask that you not grade us on a bell curve, that you hold us to standard academic levels of success.

Ms. WATSON. Let me just ask, what is the source of this grading chart?

Mr. DACEY. Let me jump in a minute. The grades were given by the committee essentially based upon, for fiscal 2002, the GISRA reports that were provided by the various agencies. The committee weighted those responses and came up with a composite grade, and that yielded the scores. The prior year was based upon some—the work on 2001 from the GISRA report. So it is pretty much coming from the GISRA reports and the various performance measures and information that are reported therein.

Ms. WATSON. What kind of progress have you made since this came out in November 2002 up to what you have today?

Mr. DACEY. One of the challenges is measuring that progress, and that is something the chairman mentioned in his opening statement, and that is the need to be looking at more frequent reporting, and Mark might talk about some of the quarterly reporting

they are moving to for FISMA in the first year. But I think that is a key element. As I said in my oral statement, it is going to be important for agencies to really build this into a systematic process so they are getting information to regularly manage information security along with other IT and other areas that they manage. And it is going to be important to build those systems, so that GISRA and FISMA reporting are an outgrowth of those systems, not the primary direction for gathering the data to include in the reports. And some of that is going to happen, but I think that an important element to make this succeed is to really have that management process in place and some of this information regularly coming to agencywide management CIOs and so forth, and they have the right responsibilities and authorities to move forward and make sure that security's improved.

In terms of the overall issue you mentioned in your initial question, I think it's going to be important, as I said, to make sure we have security management programs in place. And that's the management structure at the top and commitment by leadership to these things, because it does come down to a management issue to make sure that technology is properly implemented.

Ms. WATSON. Have we appropriated the funds to be able to put management personnel in the right place?

Mr. DACEY. There's a process, and Mr. Forman may want to speak, but it's part of the process of requesting budgets and so forth and so on. They do request what they need. And Mr. Forman might want to expand upon that a little more.

Mr. FORMAN. Virtually all the agencies have chief information security officers. What really is, I think, the heart of getting the Federal Government more secure is what we are doing with the infrastructure, networks, telecommunications, the basic competing platforms that we're using. We have tried to, in this year's budget process, significantly empower the CIOs. It gets to an esoteric risk level the way we are managing IT in the Federal Government, but we use a business case. And last year we had hundreds of projects. The rule of thumb in security is the more systems you have, the harder it is to make sure they're secure. You want to integrate and consolidate infrastructure.

Ms. WATSON. Let me cut through this. You are talking insider language. Do you have the necessary resources to organize in a way that will guarantee greater security at a time when the technology has gone above the line, and people can hack in and expose information, reveal information that can be very harmful and damaging? And particularly when I look at NASA and other security systems, I get really worried. Have we done all we can for you, or is it that you are having challenges in organizing and placing—you know, how do we get to the problem and show progress? That's my interest.

Mr. FORMAN. I think we're fine with resources. We've added a significant amount of resources.

Ms. WATSON. And the challenge is?

Mr. FORMAN. It is a lot of work, and it takes time. The older the systems, less security was built in, the more you find when you do the audit of the system, and then there is work to fix that.

Ms. WATSON. So it's the timing of trying to improve these sluggish systems and bring them up to top operation capacity.

Mr. FORMAN. And we continue to modernize. By the same token we continue to modernize. And I believe we've learned our lesson as a government that if you do not work in security before you start the system, it's going to take you longer and cost you more to fix it at the back end. So we're trying to fix the things that are out there, the so-called legacy systems. But we have made good progress in building in—before we move forward, making sure security is built in and hence Congresswoman Miller's questions.

Ms. WATSON. Thank you, Mr. Chairman.

Mr. PUTNAM. Let me follow up on Ms. Watson's question. Federal Times ran an article, essentially highlighting some of the excuses that agencies have used for not being in compliance. And the FAA said this: "We have told OMB that we can't be in compliance for a while. We don't have the money to both secure our systems and document we have done so." Do you buy that, Mr. Forman?

Mr. FORMAN. No.

Mr. PUTNAM. Later in the article, an anonymous information security specialist from a social service agency stated, "someone at our parent department told OMB we would have it done in July. We can't get it done right by then, so we will throw together some documentation and make it look like we did." They go on to say that same information security specialist at the social service agency points out that even if they had the money to do the assessments, they do not have the authority to make local offices cooperate. "They have their own funding and don't report to us. When I call them and ask for this or that, they just ignore me," the specialist said.

Have you received reports that were so off or so inaccurate or so hastily put together that you believe that they deliberately put something together to meet an artificial deadline but knowingly submitted something that was not accurate or complete?

Mr. FORMAN. I think the Treasury situation that you alluded to in your opening statement is very clear documentation that happens. It is so important to have the independent review by the ITs come concurrent with the report from the CIOs. There are so many pressures. I know funding issues. We cannot allow ourselves to make this into a paperwork exercise. And so the audit is incredibly important to us.

On the other hand, what I would say is the market is stepping up. There are an awful lot of automated tools out there that reduce the cost. And the other thing is NIST is in the second iteration of a tool kit that assists agencies in classifying. The lower the risk of the system or the fact that may be disconnected in the Internet means that there are cheaper and faster ways to get the certification and accreditation done. And that is laid out in the new set of NIST guidelines.

Mr. PUTNAM. Everybody seems to agree this is a management issue. So what are the consequences for someone with that responsibility who would submit such a report?

Mr. FORMAN. Well, I can't say in blanket how this works. I would ask you to keep in mind the reason that the CIO at the State Department did change out, and while I can't speak to all the specifics

and the details here, there's no question that the State Department acted partly in response to the IG report that indicated lack of progress in IT security. We downgraded the score on the scorecard—progress, that is, and that had a substantial impact, ultimately resulting, I believe, is my personal belief, in restructuring greater emphasis in some very tough management decisions including allocation of funding that weren't being taken before.

Mr. PUTNAM. Mr. Dacey, how widespread do you believe that this attitude is, that it's just another congressional report, just another paper that is supposed to be filed, its fine whether its done or not?

Mr. DACEY. Mr. Chairman, I am not aware of any instances where we know that reports have been intentionally prepared with improper data or data that's not accurate. At the same time, in looking at FISMA and its implementation, I think it will be important in the long term, as Mr. Forman suggested, that we have an independent audit process that starts to begin to look at those performance measures and do auditing on the performance measures, which is not currently required, and think about that as part of that process. I think that would give more credibility to the numbers. It would also make it clear to people in the agencies that someone was going to be auditing the numbers and lessen the likelihood of people preparing statements that might not be accurate.

Mr. PUTNAM. You said there is no indication of anyone having deliberately done it. But clearly, you just didn't fall off the turnip truck. Somebody has been quoted by a reporter saying this. It's probably indicative of something more widespread, don't you suspect?

Mr. DACEY. I suspect without any cross-checks that there is great pressure to report such information. That could have happened, sure. But again, it gets backs to the issue I think FISMA is a basic process that will work. We really need to put in place a process to make sure those numbers are accurate. They are self-reported so that the numbers you see in our chart and in OMB's testimony are self-reported numbers inherently not audited in any way, shape or form other than some information we have on inventories which was specifically asked for in the OMB requirements. I think that will always be a challenge unless we put in some kind of effort that is going to assure both the agency, the administration and Congress that these numbers that are being reported are accurate. Until that happens, there is a possibility that their reporting could be inaccurate.

Mr. PUTNAM. I will abide by my own time element and recognize the ranking member, Mr. Clay, for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman.

I'd like each of the witnesses to explain for me the difference between the report card prepared by former Chairman Horn and the OMB report before us today. Which is correct, and has the government improved since 2001 in the OMB reports, or is the government still failing and going from bad to worse as the subcommittee reported last year?

Mr. FORMAN. I think there are substantial improvements. I can go through from the data some differences that I would have in the grades. But let me just say, there are some agencies that are doing really well. And if you scored a 60 percent as a—if you were gener-

ous and you scored that as a D, at best, most of the agencies would get a D. It's not good enough. It's just not flat good enough. We need to be up in the 80 or 90 percent range, or A and B range. And that has to be the standard. We can talk about how much progress that we made or not, but for me a progress from an F to a D is not enough. It's just not simply good enough.

Mr. DACEY. I would like to point out again that this is the same basic information both for the GISRA report from OMB, our testimony and all the grades. So the most recent data we have Governmentwide is September 2002 data, and that gets back to the point where there is a consistency. The grades are the way in which the committee assessed and weighted the responses in the GISRA report. What we have presented and what has been included in OMB's report is some of the statistics and averages that are included in there for the same measures. It is a matter of looking at the same information in slightly different ways. It gets back to how do we know from September 2002 until today whether we have made improvements, and the point is we don't really have good reporting processes in place to get that information on a more timely basis. Right now the next set of information we will get is September 2003.

Mr. CLAY. In your testimony last fall, you indicated all 24 agencies had significant weaknesses in program management in both 2001 and 2002, and only 2 agencies improved performance in access control. Would you agree that shows little or no progress?

Mr. DACEY. It shows some progress, but we still have serious problems. Again, we have had general progress at least in reported information across all the categories. The challenge is, as Mr. Forman indicated, whether it is F or D, we still have a long way to go to get to where we need to be. Yes, that is in the report, and that is probably still the case, and that is one of the areas that I think is particularly important that you have these structures in place for the agencies to manage information security.

FISMA started to provide some of that by creating information security officers and coming up with a set of requirements for them in the agencies. And I believe most of the agencies now have a designated information security—if not all—have a designated security information officer.

We also—there's a need to have this process in place to report. Again, we don't have specific information, but I believe a lot of the information for GISRA reporting came from efforts to accumulate that information for the purpose of GISRA reporting and not as part of a routine process that management was getting the information to use to manage their security program. I think that has to change to be effective.

Mr. CLAY. Well, in the OMB report, they list six areas of government-wide security weaknesses and then report that the government shows improvement over 2001. Do you agree with that assessment?

Mr. DACEY. I agree with the characterization in OMB's report with respect to the actions that have been taken. It's consistent with what we have seen in doing our work as well. So there has been action taken in each of those areas.

And five new areas, or five areas that are newly reported, I think those are areas that we knew there were some challenges in the past; but identification of five new areas and action plans, is important to try to address those in going forward.

Mr. CLAY. Mr. Forman, according to your report, there are only 8,000 reporting systems in the Federal Government. Now, I find that difficult to believe. Can you explain to the committee what that number represents and what systems are not included in that count?

Mr. FORMAN. Generally these are combinations of applications that work together to perform a function. So, do we have more than 8,000 systems? Probably. The number of reporting went up in 2002 compared to fiscal year 2001. I suspect it will go up again this year.

But, that said, we know there are many more applications than that number. It's just agencies under the definition in GISRA are allowed to bundle together applications and call that a system. This is the best reporting we've had.

I think, for security purposes, that makes sense, because they are generally used by the same group of people, tied to the same network, and work together to support a business process. At the end of the day, you want to secure all the information around a business process, and you want to make sure that's secure, that business process can keep operating even if it's attacked. So I'm fairly comfortable with the definition that Congress came up with for GISRA. I think it exists fairly the same, except for national security systems, all training in FISMA. But the focus is appropriate.

Mr. CLAY. Thank you both for your answers.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Clay.

Mrs. Miller, do you have another round of questions?

Mrs. MILLER. Just one.

You know, I'm looking at this blue chart over there from the GAO about performance measures and those kinds of things. Mr. Dacey, can you give me a little more specific about what kind of performance evaluations you actually do? I can hardly see the bottom. Give me an example of what kind of performance measures. I mean, we keep talking about this is a management problem, apparently not a financial resource situation; it's a management problem. So just what kinds of things do you actually look at to measure this performance evaluation?

Mr. DACEY. Let me talk about that a minute. And hopefully you have something that looks like this up on your desk area that you can see better.

In any case, these are six of the areas that were included in OMB's report. And what we put together in the chart was to try to really reflect the change from year to year, from 2001 to 2002, and on average for 23 of the largest agencies. Again, as I said before, the information that goes into these is a whole series of performance measures that were required by OMB in reporting on the second year GISRA implementation. And these have been important, because they really are establishing a baseline and a basis for comparison from year to year. And this is the first year we have comparative information government-wide that we can look at.

These are six of the many performance measures that were required to be reported. These particular ones I think are somewhat illustrative because it gets to some of the critical challenges that we have. If you look at the first column on risk assessment, that's whether the agencies have assessed risk in their systems to know what level risk they are accepting and operating them.

The second is a security plan in place——

Mrs. MILLER. Let me just ask you about the risk.

Mr. DACEY. Sure.

Mrs. MILLER. What kind of risk assessments, for instance? I don't want to go through the whole thing, but just in that particular column there. What kind of risk assessments do you actually do? I mean, risk of terrorists? I mean, some guy with a laptop in a cave in Afghanistan being able to get into one of the systems in DOD? And are the evaluations for risk assessments uniform throughout these last two report cards and as we are entering September now?

Mr. DACEY. Well, I think—I guess my observations on risk assessments would be, they're supposed to include the threats to the system. And that's the normal process. We actually have a best practices report we issued on risk assessment; it's something that OMB requires to be done. The format and structure of them has a lot—some flexibility built into how detailed they are. So I couldn't say that every agency does it the same way. But what this number represents is the number of systems that those agencies reported that they had assessed risk for, and that's what those columns represent, both the gold for 2001 and the blue for 2002.

Mrs. MILLER. So risk of the type of information that you are gathering? Risk of the type of access that individuals would have to it? Risk of security of that information, those kind of things?

Mr. FORMAN. And then the final aspect of that is risk that you wouldn't—the agency wouldn't be able to complete its mission if either the information was stolen, disrupted, or the system processing was shut off.

Mr. DACEY. As part of that process, just to point out, one of the provisions of FISMA is to actually come up with risk levels. I think that can help a lot, because that will standardize the process by which agencies assess risks and can communicate more effectively between each other and within the agency as to when they are hooking systems together and what the risk levels are. So I think that would be an important improvement. Right now, the risk assessment is a little more subjective, not that it won't be somewhat subjective, but at least it will have a structure that is proposed by NIST as part of the FISMA law.

Mrs. MILLER. Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mrs. Miller. Now I'd like to ask each of you: does every agency currently have an acceptable business continuity plan?

Mr. FORMAN. Generally we look at that down to the system level. And the answer is, no. That there are big gaps in some agencies and really good success in other agencies. That's part of the data that is tracked and I think was in our report. I would ask you not only to take a look at the agencies that have a valid contingency plan, but also what I think we need to do one step further that has

been tested and validated, very similar to the work that we had to do with the year 2000 contingency plans.

Mr. PUTNAM. OK. While we are talking about that, in Mr. Dacey's testimony, he said that less than 50 percent of the contingency plans at 19 out of 24 agencies have been tested. Less than half have been tested. So does that mean that those plans might not work?

Mr. DACEY. Yeah. I think that really signifies that—until you test it, you don't know it will work, in fact. And there are two issues here. The other number that we have is also the fact that there are a significant number of systems for which they don't have contingency plans. I think it is reported now at about 50 percent, 55 percent, just have the plans to start with; and then the second step is testing those plans to be sure that they would be effective in case of an emergency.

I think that is a critical area, because absent some of these other controls in other areas, particularly for critical systems, it would be very vital to make sure that those systems could be recoverable in case some of these other weakness areas were exploited and the system availability was lost.

Mr. PUTNAM. Nobody ever wants to say that one agency or department is more important than another one. But in terms of the ramifications of having a contingency plan or a disaster management plan, are the agencies that are most at risk and most critical to national security or homeland security the ones who have tested? Has the Social Security Administration tested their contingency plans, and Defense not? Has Homeland Security, has FEMA?

Mr. FORMAN. It's a mix. And you will find the data in the table. You will see, for example, you are absolutely right. Social Security has tested their contingency plans. They are in pretty good shape. By the same token, FEMA did not test their contingency plans.

Mr. PUTNAM. So the Emergency Management Agency has no emergency management plan?

Mr. FORMAN. They have the plans for—as of the end of last year they had some of the plans. They don't have enough plans. And, moreover, they haven't tested the ones they have. There is significant work that needs to be done here.

Mr. PUTNAM. Let's talk about patches very briefly in my remaining time. Then we are going to move to the second panel. Patch management is critical to information security. It goes a long way toward protecting our systems from viruses and other attacks. The PAD-C, the patch authentication and dissemination capability, will provide a system to Federal agencies to manage the patching of their systems. How far along are we in that? How are the agencies participating? Are they responding to OMB's encouragement?

Mr. FORMAN. I don't believe I have the exact numbers on how many agencies have signed up. They continue to get more agencies to sign up. This is, again, part of our concept of buy one, choose many. Patches are obviously to use a software code. And to the extend that people have common software—and we have an awful lot of common software in the government—it's better to buy that patch once and then have an automated way to distribute it. So that's why we invested in this patch management, buy-one, choose-many concept.

I need to get back to you on exactly how many agencies, and I will do that.

Mr. PUTNAM. Do you want to add something, Mr. Dacey?

Mr. DACEY. I don't have the information right in front of me, but a fair number of agencies have signed up for PAD-C. I forget the number. It might be in our testimony. OK. I don't have that with us today. We can certainly get back to you on that. But it is an important area because it does provide a central source for patches that have been tested and authenticated and placed out there. I think one of the key issues in patch management is that even with that, agencies need to have a process to ensure that these patches are installed and installed properly and don't break other parts of the system. And so they need to take efforts to put that in place. And NIST has some draft guidance out in how to do patch management that is very informative.

Mr. PUTNAM. Well, the committee has submitted a letter to the secretaries of the departments, their IGs and CIOs, requesting more frequent updates of information and given them August 1 as a deadline for the update. And we will also be picking up where Mr. Horn left off with the score cards this fall. I think that our first panel will note that this is bipartisan frustration with this, with the inadequate progress on the part of the Federal agencies, and we will continue to monitor this very closely.

My parting question would be this: are the differences in reports due to different interpretations of what the law requires or a genuine disagreement over the level of information security that exists at the agencies?

Mr. DACEY. Just for clarification. Difference in which reports are you referring to, Mr. Chairman?

Mr. PUTNAM. Different interpretations of the FISMA, GISRA requirements, or to a genuine disagreement over the status of information security between the IGs.

Mr. DACEY. Between the IGs and the agencies?

Mr. PUTNAM. Yes.

Mr. DACEY. That's an interesting question. There were a number of IGs that did disagree, and I think OMB in fact in their report pointed out that was one of the new challenges that needs to be really looked at and addressed. And Mr. Forman might speak more to that. That's an area at least that's highlighting where there are differences that go back to the FISMA model and talk about the agency and the IG both working together and the agency providing some validation of that information.

So I think it's good that we are pointing out where there are differences, and it's also a need then to followup on those differences and find out why they exist. I don't know that we have any information on why the differences exist. In some cases it may be just differences of thought or differences in the systems that were looked at. I do know that when we deal with some of these issues from our audit perspective at GAO, there's not always unanimity in how you interpret the results of your reviews. And a lot of our discussion goes around what does this really mean, how serious of an issue is it. So there also—there can be differences of opinion as well.

Mr. PUTNAM. Do you want to add anything, Mr. Forman?

Mr. FORMAN. First of all, let me say that we do have some data in followup to your past question on the patch management contract. There are 37 agencies that subscribe to that today. What I need to do in getting back to you is find out how many are Cabinet-level agencies versus small agencies. Obviously, the small agencies really like to use the shared approaches.

I think that actually the debate is good on what is a covered system and the amount of risk. To have the IG have that independent view and say this system is actually more mission critical or it is more important to the agency's mission than a CIO may say, really reveals to us something about the positioning of the CIO. And generally, as in some of the examples you cited, I notice that the CIO may not have the appropriate status that, sure, maybe in the agency to come forward and say a system is badly performing. They may be kept out because of the differences between the IT organizations and the bureau program offices.

So, I think, first of all, it's not necessarily bad to have the disagreement. And, second, it is very important that the IG stay aggressive in this area so that it can reveal to us where are the areas to look.

Mr. PUTNAM. Thank you very much for your testimony.

At this time we will dismiss panel one and seat panel two and move as quickly as possible. Thank you very much, Mr. Forman and Mr. Dacey. The committee will recess for 3 minutes.

[Recess.]

Mr. PUTNAM. We will go ahead and seat the second panel and reconvene the subcommittee hearing.

I would like to welcome our second panel of witnesses. As is the custom of the subcommittee, we will swear in this panel. I would ask that if you have personnel joining you today who will be assisting you in answering, that they will also rise and be sworn at this time. Please stand and raise your right hands.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all of the witnesses and their supporting cast responded in the affirmative.

We will move right to panelists' testimony. I begin with Johnnie Frazier. Mr. Frazier was appointed to the position of Inspector General at the Department of Commerce in 1999. The Presidential appointment capped more than three decades of distinguished service at the Department in a variety of leadership roles. During his tenure as IG, Mr. Frazier has significantly strengthened that office's strategic agenda to reflect the most pressing priorities for the Department and the Nation. For example, he has directed key audits and investigations of security weaknesses in Commerce's computer networks information systems and personnel policies. He has initiated assessments of emergency preparedness plans at commerce facilities and prompted examinations of export safeguards on sensitive U.S. technology. He has precisely defined the IG's direction for the near future around a set of core priorities that strategically target emerging audit and inspection areas of need.

We welcome you to the subcommittee, and recognize you for 5 minutes for your testimony.

STATEMENT OF JOHNNIE E. FRAZIER, INSPECTOR GENERAL, DEPARTMENT OF COMMERCE

Mr. FRAZIER. Mr. Chairman and members of the subcommittee, I am pleased to appear before you today to provide the IG's perspective on IT security in the Department of Commerce. You know, although IT security and data have long been among the Department's most critical assets, ensuring their security, unfortunately, was not a high priority for the Department before GISRA.

When I first testified on IT security 2 years ago, I had few favorable observations to share. The Department was striving to improve, but our work at that point revealed pervasive security weaknesses that placed sensitive IT security systems at serious risk. As a result, we identified IT security as one of the top 10 management challenges facing Commerce. And while much progress has been made, it still remains high on my top 10 list.

OMB's fiscal year 2002 report to the Congress on Federal IT security noted that progress is evident and that the government is heading in the right direction. I am pleased to report that Commerce, too, has made progress and is heading in the right direction; but this department, like many others I'm sure, must overcome a history of much neglect. As Commerce's CIO put it, the Department has been coming from behind.

Our IG GISRA evaluations over the past few years have often found the same basic weaknesses at Commerce that OMB has found throughout the government. First and probably foremost, we have seen the problems, the progress, and the potential that surround senior management's attention to IT security. Before GISRA, IT security was simply not on the radar screen of senior Commerce management. Through the Secretary and Deputy Secretary's efforts, and quite candidly their bully pulpit, senior managers are increasingly coming to understand that they are responsible for IT security.

Our independent observations on security education and awareness previously highlighted this as an area of neglect. Again, the Department has responded. Today, all employees and contractors receive security awareness training. But specialized training for personnel with significant IT security responsibilities remains inadequate.

A third major area centers on the importance of management religiously integrating funding and IT security into Commerce's capital planning and investment control process. While the Department has substantially increased its control over IT investments, it often still struggles to adequately plan IT security controls and costs for every system.

Our ongoing independent evaluation is also showing that the Department has improved its capability to detect, report, and share information on vulnerabilities. Before GISRA, only 4 of Commerce's 14 operating units had a formal incident response capability. Now, all Commerce operating units have such capability.

Another matter of particular note to us is the importance of ensuring that contractor services are adequately secure. Our review of 40 of the Department's IT service contracts found that contract provisions to safeguard sensitive systems and information were ei-

ther insufficient or nonexistent. Why, you ask? Little Federal or departmental guidance or policy in this area.

On the Federal level, a proposed Federal acquisition clause for IT security is currently under review by the FAR Council. I believe this clause will be beneficial government-wide. And I am personally pleased that our IG contracting expert, Karen DePerini, who first identified the contract problem at Commerce, is co-chair of the OMB issue group that recommended this clause and is identifying methods to improve security in contracts. And last, but by no means least, aggressive schedules for IT performance measures are having an impact on all parties involved in the IT security effort.

It should be noted here, however, that although security plans have been required for Federal IT systems since the Computer Security Act of 1987, when I testified 2 years ago, nearly two-thirds of the Department's systems lacked risk assessments, almost half did not have a security plan, and more than 90 percent were not certified or accredited. The Department is vigorously addressing these serious deficiencies.

The Department's focus can best be seen by looking at its performance measures for system certification and accreditation. According to the Department, between fiscal years 2000 and 2003, the percentage of systems certified and accredited increased from a mere 8 percent to 77 percent of its roughly 600 systems.

At the same time, I must caution that performance measures do not tell the whole story. Overaggressive schedules can actually weaken the process. Our evaluation suggests that aggressive timeframes have often resulted in premature certification and accreditation, where risk assessments, security plans, testing, evaluation, and review have been inadequate or sacrificed altogether.

In closing, I am proud that the independent evaluations required of the IGs play a uniquely valuable role in confirming the substance and quality of critical processes and control and in helping ensure that the job is done right. Unfortunately, our resource limitations have not allowed us to do such things as validate the specific details of the Department's annual IT security report. Likewise, we have not been able to perform vulnerability assessments and penetration testing of nonfinancial systems that would demonstrate whether vulnerabilities exist and intrusions may occur.

I cannot overemphasize how critical it is that the rigor and integrity of IT security processes be maintained; otherwise, we will have paper security but lack true security. Thank you.

Mr. PUTNAM. Thank you very much, Mr. Frazier.

[The prepared statement of Mr. Frazier follows:]

STATEMENT BY

JOHNNIE E. FRAZIER
INSPECTOR GENERAL
U.S. DEPARTMENT OF COMMERCE

BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS
UNITED STATES HOUSE OF REPRESENTATIVES

JUNE 24, 2003

Mr. Chairman and members of the subcommittee, I appreciate the opportunity to appear today to provide the Inspector General's (IG's) perspective on information technology (IT) security in the Department of Commerce.

Commerce's IT systems and the data they process and store are among the most critical assets of virtually all the Department's line offices and operating units. For example, satellite, radar, and other weather forecasting data and systems managed by the National Oceanic and Atmospheric Administration (NOAA) are critical to protecting lives and property; export license data compiled by the Bureau of Industry and Security (BIS) is essential to controlling the export of dual-use commodities to foreign governments and entities; economic indicator data developed by the Economics and Statistics Administration (ESA) has significant policy-making and commercial value and may affect the movement of commodity and financial markets; and data of the U.S. Patent and Trademark Office (USPTO) is essential to administering national and international laws relating to patents and trademarks, promoting industrial and technical progress in the

United States, and strengthening the national economy. Clearly, maintaining the security of Department of Commerce data and systems is of overriding importance to both the agency and the nation. Loss of or serious damage to any one of the Department's critical systems can have far-reaching, long-term, and possibly devastating impacts. Furthermore, without effective IT security, the Department's electronic government initiatives cannot be successful.

State of IT Security at the Department of Commerce

When I first testified on IT security two years ago, I had few favorable observations to share. The Department was striving to improve IT security and make it an integral component of Commerce's business operations. However, our work, augmented at the time by GAO's penetration testing of information systems and networks based in Commerce headquarters, revealed pervasive IT security weaknesses that placed sensitive systems at serious risk. Weaknesses Department-wide prompted us to identify IT security as a top management challenge. Indeed, Commerce exhibited the six common government-wide IT security weaknesses identified by the Office of Management and Budget (OMB) in its FY 2001 report to Congress on government information security reform:

1. Lack of agency senior management attention to IT security.
2. Poor security education and awareness.
3. Failure to fully fund and integrate security into its capital planning and investment control process.
4. Failure to ensure that contractor services are adequately secure.

5. Lack of detecting, reporting, and sharing information on vulnerabilities.
6. Lack of IT security performance measures.

OMB's FY 2002 report to Congress on the state of IT security in the federal government, which was submitted in May, noted that while efforts are still warranted across these six areas, progress is clearly evident, and the federal government is headed in the right direction. I am pleased to report today that Commerce, too, has made progress and is headed in the right direction. But the Department must overcome a history of neglect. In his April testimony before this subcommittee, the Department's CIO, Thomas N. Pyke, aptly stated that Commerce has been "coming from behind" as it strives to implement a comprehensive IT security program. Although significant strides have been made, implementing a comprehensive program to enhance IT security continues to be a top management challenge. As we advised, the Department reported IT security as a material weakness in its *Accountability Report* in both FY 2001 and FY 2002, and we believe it should continue to be reported as such until Commerce systems that are part of the nation's critical infrastructure (national critical systems), as well as those that are mission critical, have been certified and accredited.[1]

USPTO must also address serious IT security issues. As a performance-based organization, USPTO has been submitting its IT security review separate from that of the Department of Commerce. It is also undertaking actions separate from the Department to

[1] Certification denotes that the system's security controls have been tested and found to be adequate; accreditation signifies that the responsible senior manager has formally authorized its operation and accepts any residual risk.

manage IT security, so we reviewed USPTO's IT security program separately in FY 2002. Like the rest of the Department, USPTO is making progress in IT security, but it, too, faces significant challenges. At our urging, USPTO, like the Department, reported IT security as a material weakness in its FY 2002 *Accountability Report*, and we believe it should continue to be reported as such until all USPTO's mission-critical systems are accredited. (We note that USPTO does not have any IT assets identified as part of the nation's critical infrastructure.)

The Six Areas of IT Security Weakness Reported by OMB as They Apply to Commerce

I would like now to address the six areas of weakness reported by OMB as they apply to Commerce, covering their status before GISRA was enacted, the progress that has been made since that time, and the actions Commerce is taking to address its deficiencies. I will then discuss how we perform our evaluations and how our objectivity and independence bring unique insight to this important area.

1. Agency senior management attention to IT security.

Before GISRA was enacted, IT security was not a high priority for senior officials in the Department. This area of responsibility was commonly regarded as belonging solely to the CIOs, who did not treat it as a priority either. And this lack of concern and attention showed. Reflecting a history of neglect, Commerce's IT security program was incomplete, portions that existed were out-of-date, and the program was not enforced. The majority of the Department's IT systems had not been assessed for risk, did not have

security plans, and were neither certified nor accredited. This meant that, more often than not, security controls had not been tested, systems were operating without required management authorization, and management officials lacked an understanding of the risks their organizations were incurring by permitting their systems to operate.

Since the enactment of GISRA, the Department's perspective on IT security has changed completely: senior Department management has become intensely aware of and takes very seriously its IT security responsibilities. Under GISRA, IT security became the explicit responsibility of federal agency senior management—the agency head, senior line managers, and the CIO. GISRA charged the Secretary with ensuring the security of information and information systems by promoting security as an integral component of the agency's business operations. Senior Commerce managers were given specific responsibility for protecting the security of operations and assets they control.

As we reported in our FY 2001 independent evaluation, in the summer of 2001 the Department began a concerted effort to improve IT security and make it an integral component of Commerce's business operations. Specifically, the Secretary of Commerce directed secretarial officers and heads of operating units to (1) give IT security high priority, sufficient resources, and their personal attention, and
(2) restructure, and thus strengthen, IT management by having a CIO at each unit who reports to the unit head or principal deputy and to the Department CIO, and by increasing the unit CIO's authority over IT resources. We noted that these actions—if accompanied

by continued executive-level attention and adequate resources—were important steps in building a more effective IT security program.

Our FY 2002 evaluation confirmed that Department-level executive support for IT security continued. Both the Secretary and Deputy Secretary continued to emphasize to senior Commerce officials the importance of IT security and senior management's responsibility for establishing effective IT security programs in the operating units. They also continued to stress to senior management their leadership role in correcting the problems identified by OIG and GAO evaluations. Our FY 2002 GISRA review found that senior management officials in Commerce's operating units generally were giving IT security their personal attention and were working to ensure that employees understood the responsibilities of their unit's CIO and program officials, as well as their own personal responsibility, for IT security.

However, we still found a need for greater senior management attention in both of the agencies whose IT security programs we reviewed comprehensively in FY 2002—the National Institute of Standards and Technology (NIST) and USPTO. We found that IT security was not receiving adequate senior management attention, and as a result, significant weaknesses existed in planning, budgeting, implementation, review, and oversight. Consequently, we concluded that there had been a lack of follow-through in carrying out such fundamental responsibilities as:

- establishing comprehensive IT security policies and procedures;
- identifying, assessing, and understanding risks to agency IT assets;
- determining IT security needs commensurate with the levels of risk;
- planning, implementing, and testing controls that adequately address risk;
- continually monitoring and evaluating policy and effectiveness of information security practices; and
- developing a capital planning and investment control process and integrating IT security into it.

Since the time of these most recent evaluations, the heads of both of these agencies have stated their commitment to protecting their information assets. In a memorandum to his senior management team, the director of NIST acknowledged his responsibility for the security of NIST's data and IT systems, and directed all members of NIST's upper management to give IT security high priority and to ensure that NIST's policies, procedures, and operational environment are exemplary. NIST has also restructured the CIO's office with the goal of improving its effectiveness.

Regarding USPTO, in response to our evaluation, the Under Secretary of Commerce for Intellectual Property and Director of USPTO began to devote additional attention and resources to this area. In addition to identifying IT security as a material weakness in its FY 2002 *Accountability Report*, USPTO further demonstrated its commitment to improving IT security as part of a new corporate strategy presented in *The 21st Century Strategic Plan*. Referring to the OIG evaluation, the plan states that USPTO is not in compliance with the law and that because IT security has not yet become an integral part

of USPTO's business operations, fundamental IT security responsibilities are frequently not carried out. The plan concludes that the implication of not being compliant with GISRA is that neither internal nor external customers can trust USPTO's automated information systems. It further presents tasks, milestones, and a schedule for correcting this problem that are consistent with our recommendations.

2. Security education and awareness.

In our FY 2001 GISRA evaluation, we reported that security training was not conducted on a rigorous or ongoing basis, and none of the operating units was able to give us the information we requested about the number of employees who had received security training or the cost of providing such training. Our FY 2002 evaluation, however, found that significant progress had been made in providing awareness training to IT users. At the direction of the Department's CIO, operating units had provided such training to all employees and contractor personnel either through programs of their own or via web-based training made available by the CIO. The operating units tracked and reported this training to the Commerce CIO and must continue to do so every year.

Operating units are responsible for identifying positions that require specialized IT security training as well as the specific training requirements for those positions. We found that less progress has been made in this area. Training for personnel with significant IT security responsibilities such as system administrators, IT security officers, and contracting officers appeared to be inconsistent and incomplete at the units we reviewed. The Department CIO is addressing this issue by making training more

accessible: an enterprise license was acquired for web-based IT security training, which makes both specialized and annual awareness training available throughout the Department. In conducting our ongoing independent evaluation this year, we are finding that some IT security officers still lack a sufficient understanding of their duties and responsibilities, thus highlighting the need for the Department to continue to focus on ensuring that specialized security training is provided to those who need it.

In addition, at the end of FY 2002, the Department CIO sponsored and paid for two important on-site training classes—Principles of Certification and Accreditation, and Roles and Responsibilities of the Designated Approving Authority. These classes covered the methodologies NIST is using to update its federal guideline on certification and accreditation. Although the sessions could not accommodate all personnel who needed them, they were an important step in addressing a critical training area.

3. Funding and integrating security into Commerce's capital planning and investment control process.

By controlling IT spending decisions, the Department and operating unit CIOs can ensure that security is planned at the earliest stages of a system's life cycle. In our FY 2002 independent evaluation, we found that the Department CIO's review and concurrence are required for IT investment decisions affecting all major systems, and—with the exception of NIST—all of the operating units we reviewed (BIS, ITA, NOAA, and NTIA) require unit CIO concurrence for smaller IT investments.

At the Department level, the Commerce Information Technology Review Board (CITRB), chaired by the CIO,[2] was established to support this decision-making function. The Department CIO, with input from the board, provides recommendations to the Deputy Secretary and the Office of Budget on the soundness of the planning for each proposed IT initiative, including the extent to which it addresses Department requirements for IT security and IT architecture. The board seeks to conduct a status review, usually once a year, for approved projects. The CIO, in turn, uses these reviews to recommend whether a project should be continued, modified, or terminated. IT projects costing more than $10 million that require a contract, as well as selected smaller projects, must be reviewed by the board in order for the operating unit acquiring the system to receive a delegation of procurement authority, which is the authority to make contractual commitments. In his FY 2004 and 2005 budget guidance to the operating unit CIOs, the Department CIO emphasized that demonstrating effective IT security is an important factor in the board's review of budget requests.

NIST began to implement an IT capital planning and investment control process in FY 2002; however, our evaluation found that investment decisions could still be made

[2] Other members of the board include the Chief Financial Officer and Assistant Secretary for Administration, who serves as co-chair; Deputy CFO; Deputy CIO; the CIOs from NOAA, Census Bureau, NIST, ITA, and, on a rotating term basis not to exceed 2 years, two other operating unit CIOs; selected operating unit executives as designated by the CIO; Director for Budget; Director for Acquisition Management, and Director for Human Resources Management.

without the review and concurrence of NIST's acting CIO. In responding to our evaluation, NIST noted that its capital investment planning process would be fully implemented in FY 2003, at which time CIO concurrence will be required.

As part of our FY 2002 independent evaluation, we examined the FY 2003 capital asset plans for 13 major departmental systems—9 of the systems were from NOAA, 2 were from NTIA, 1 was from NIST, and 1 from BIS—to determine whether each capital asset plan (1) specified the system's projected security costs, (2) detailed how funds would be spent, and (3) adequately described the system's security requirements.
We found that most plans specified projected security costs, but only a few explained how these funds would be spent. Although most plans described the IT security activities that need to be conducted over the system life cycle, some did not detail specific risks and security controls. We concluded that the operating units need to do a better job of identifying security risks and controls throughout a system's life cycle so that security expenditures can be better developed and justified. The Department CIO is addressing this issue by providing training in the preparation of capital asset plans and specific guidance for completing the security and privacy section. As mentioned earlier, IT security is also given special attention during CITRB reviews.

USPTO carries out its capital asset planning and budgeting process separately from that of the Department. Our FY 2002 evaluation found that USPTO needed to make significant improvements in this area. USPTO had not identified security costs for any individual system in its fiscal year 2002 or 2003 budget submissions. Nor had USPTO conducted an accurate, thorough analysis of existing security needs and the cost of

satisfying them in order to develop its budget request. The fiscal year 2002-2007 budget formulation guidance provided by USPTO's Office of the Chief Information Officer did not contain instructions for incorporating security costs into budget requests. In response to this finding, USPTO indicated that the budget system in its CIO office was enhanced to ensure that IT security costs are tracked for each system, and funding for IT security is included in each system's budget plan.

4. Ensuring that contractor services are adequately secure.

This past April, Mark Forman, OMB Administrator for Electronic Government and Information Technology, testified before this subcommittee on the status of the federal government's IT security. While discussing the security of contractor services, he noted that an issue group had been created to review the problem through the Administration's Committee on Executive Branch Information Systems Security of the President's Critical Infrastructure Protection Board. The issue group recommended use of a government-wide security clause, a recommendation currently under review by the Federal Acquisition Regulatory (FAR) Council.

Of course, the need to safeguard sensitive information and information systems when contracting for services increases as outsourcing increases because the risk of security violations by contractors—whether inadvertent or deliberate—also grows. Thus, I share OMB's concern about ensuring the security of contractor services and believe a FAR clause is needed. I am pleased that my office has been able to help address this issue by

having our contracting expert, Karen DePerini, at the invitation of OMB, serve as co-chair of the issue group cited by Mr. Foreman.

Through our FY 2001 independent evaluation, we identified problems with IT security in IT service contracts, resulting, in part, from a lack of sufficient federal and departmental policy and guidance to ensure that contract documents for IT services contain adequate IT security provisions. In FY 2002 we examined this weakness in greater detail: we reviewed 40 of the Department's IT service contracts, including some awarded by USPTO, and found that provisions to safeguard sensitive but unclassified systems and information were either insufficient or nonexistent. Based on the results of this sample, we concluded that the majority of IT service contracts throughout the Department lacked needed IT security provisions. Contracting officers and other acquisition team members need guidance and training, as well as support from technical experts and program officials, to ensure that they prepare and administer IT service contracts in a way that makes clear and enforceable the contractor's responsibility and accountability for safeguarding the government's information assets.

We recommended that the Department of Commerce's Chief Financial Officer and Assistant Secretary for Administration take the necessary actions to ensure that all contracting offices within Commerce include adequate IT security provisions in all IT service contracts to protect the Department's sensitive IT information and assets. Specifically, we urged the Department to establish standard contract provisions for

safeguarding the security of unclassified systems and to disseminate clear, detailed policy guidance for acquiring these systems and services.

We further recommended that such a policy require contracting offices—with assistance from the Department's Office of the CIO—to assess the IT security risk associated with the proposed service or system during the acquisition planning phases; identify and include appropriate IT security requirements in specifications and work statements; monitor contractor performance to ensure compliance with IT security requirements; and terminate the contractor's access to systems and networks once the contract is closed out. We also advised the Department to review all current contracts and solicitations for IT services to determine whether IT security provisions should be added to them, even though such revisions might increase contract costs, and to ensure that all procurement personnel have appropriate training in IT security.

The Department is in the process of implementing our recommendations. Contract provisions have been written and are now undergoing departmental review. After the provisions are approved, Commerce plans to provide appropriate training to acquisition staff. The Department's assessment of current contracts found that more than 350 need modification to address the new security provisions. In January, the Department CIO issued a new security program policy, which addresses IT security in contracts and should help ensure that future contracts include appropriate security provisions prior to being awarded.

5. Detecting, reporting, and sharing information on vulnerabilities.

GISRA requires agencies to have documented procedures for detecting, reporting, and responding to IT security incidents. In our FY 2001 independent evaluation, we found that only 4 of 14 operating units—Census, NIST, NOAA, and USPTO—had a formal incident response capability, and that the Department's policy for reporting IT security incidents needed to be revised to specify notification of OIG and to define what constitutes a reportable incident. In FY 2002, the Department established a computer incident response team to support operating units that did not have their own incident response capability, thus ensuring coverage of the entire Department. The team will also be a focal point for obtaining and exchanging best practices and incident response methodologies.

The Department's new security program policy includes improved guidance on incident identification, handling, response, and reporting. It defines the types of incidents that need to be reported and requires each operating unit to submit its response procedures to Commerce's critical infrastructure program manager, located in the Department CIO's office, for review and approval. This requirement will help ensure that all units have documented procedures for reporting security incidents and sharing information about common vulnerabilities. The policy sets minimum requirements for incident response capabilities and prescribes the system-level processes and incident-handling procedures to be performed, including working with OIG investigators and other law enforcement authorities and reporting incidents to the Federal Computer Incident Response Center (FedCIRC). It also establishes requirements for monitoring and detecting incidents,

including use of network- and host-based intrusion detection systems, logging tools, firewalls, and other devices, as well as review of audit logs, trouble reports, and information provided by intrusion detection tools.

As Mr. Pyke recently told the subcommittee, Commerce has established a capability to transmit IT security alerts Department-wide at any time and to activate Commerce emergency mobilization plans, as appropriate. To maintain up-to-date corrective patches for known vulnerabilities, the Department established a patch authentication and distribution account under the patch management contract awarded by FedCIRC.

6. IT security performance measures.

Although security plans have been required for federal IT systems since the Computer Security Act of 1987, when I testified two years ago, nearly two-thirds of the Department's systems lacked risk assessments, almost half did not have a security plan, and more than 90 percent were not certified or accredited. These were serious deficiencies that the Department has since been addressing zealously. The table below shows the status of these items, based on Department reporting, between FY 2000 and FY 2003.

Percent of Systems with Risk Assessments, Security Plans, and Certification/Accreditation*

	FY 2000 (percent)	FY 2001 (percent)	FY 2002 (percent)
Risk Assessments	28	74	94
Security Plans	54	69	96
Systems Certified and Accredited	8	48	77
*Table excludes USPTO's systems.			

Last fiscal year, the Department CIO set September 30, 2002, as the deadline for having approved security plans for all general support systems and major applications. In its fiscal year 2002 GISRA review, the Department reported that of its 609 systems, 94 percent had risk assessments, 96 percent had security plans, and 77 percent were certified and accredited. OMB has established a goal that by the end of 2003, 80 percent of federal IT systems shall be certified and accredited. The Department's goal is to have all national critical, mission critical, and classified systems certified and accredited by the end of this fiscal year.

Performance Measures Do Not Tell the Whole Story; Aggressive Schedules May Actually Weaken the Process

Achieving certification and accreditation for all systems is imperative, and we support the effort to certify and accredit all systems as soon as possible. Our independent evaluations suggest, however, that the Department's aggressive schedule is causing some systems to be certified and accredited in the absence of adequate risk assessments and security plans and without rigorous and effective testing, evaluation, and review processes. While a

concerted effort toward certification and accreditation must continue, it is equally critical that the rigor and integrity of certification and accreditation processes be maintained. Otherwise, we may have paper security, but lack true security.

Our concern stems from the fact that our 2002 GISRA review, whose fieldwork we completed in July, found numerous systems operating without required risk assessments, approved security plans, or certification and accreditation. Moreover, some with approved security plans could provide no evidence that a risk analysis—a prerequisite for the security plan—had been conducted. Too many operational systems we reviewed had not been accredited, and many lacked up-to-date security plans and risk assessments. Those that were accredited frequently lacked evidence of the requisite security testing and evaluation, thus diminishing the assurance that accreditation is intended to impart. For example,

- NIST had established an ambitious schedule for accrediting all of its systems by September 1, 2002. As of July, none of NIST's 109 operational systems had a documented risk assessment or an approved security plan, and only two had accreditation. Moreover, the dates by which NIST's offices were to receive a risk assessment methodology had passed, yet the methodology had not been provided. All future dates depended on the risk assessments; thus this delay affected the entire schedule. We were concerned that this aggressive schedule would not permit sufficient analysis, documentation, or review to achieve adequate product content or quality or support meaningful certification and accreditation processes.

To address our concern, NIST stated it would have its CIO review all NIST system certifications and accreditations in FY 2003.

- At the time of our evaluation of USPTO, 82 percent of USPTO's 78 operational systems lacked documented risk assessments, and the security plans for 30 percent of those systems were more than 3 years old. None of USPTO's systems had been certified and accredited. In response to our review, USPTO planned to certify and accredit all high-risk systems by the end of FY 2003 and the remaining systems by the end of FY 2004.

- Security plans were provided for all four of BIS systems, which were generally consistent with NIST guidance for content and format, but evidence of a risk assessment was provided for only one system. Although BIS considered the plans approved, it lacked a formal approval process and thus could not validate the approval. None of the systems had undergone security testing and evaluation or been certified or accredited.

- Risk assessments had been performed on the four ITA systems for which we requested documentation. ITA provided two security plans that it considered approved and two draft plans. However, like BIS, ITA lacked a formal approval process. Our review of the two approved plans found them to be generally consistent with NIST guidance for content and format but in need of additional information on rules for using the systems appropriately; they also did not comply

with the Department's password policy. Furthermore, none of the systems had undergone security testing and evaluation or been certified or accredited.

- NOAA's Office of Atmospheric Research (OAR) and National Marine Fisheries Service (NMFS) had performed risk assessments on their systems. With one exception, systems belonging to the National Environmental Satellite, Data, and Information Service (NESDIS) and National Ocean Service (NOS) provided hazard information that did not give enough detail to determine needed security controls or conduct certification activities. All the NOAA offices we reviewed had up-to-date security plans whose content and format were generally consistent with NIST guidance and were approved by an IT security officer. However, some of the plans provided by NESDIS, NMFS, and NOS had been updated after the Department issued a revised password policy but did not comply with that policy. Although all NOAA systems we reviewed had current certifications and accreditations, only one had evidence of security testing and evaluation. The seven NESDIS systems we reviewed were accredited after we requested documentation, and the accreditations appear to have been granted in haste. Because we found no concrete evidence to indicate that the appropriate steps had been taken, including security testing and evaluation, the validity of NESDIS' certification and accreditation process is questionable. Since our review, NOAA reported that it has implemented the Department's new password policy and all security plans will be updated to reflect this by September 2003.

- NTIA had conducted risk assessments on the two systems for which we requested documentation and provided security plans for both systems. The content and format of these plans were generally consistent with NIST guidance, but like ITA and BIS, NTIA lacked a formal plan approval process. Neither system had undergone security testing and evaluation or certification and accreditation.

In this year's evaluations, we have found systems whose documented sensitivity levels are understated; their security controls, therefore, are not commensurate with the level of risk. Similar to last year, security plans were developed without current risk assessments, and essential information required for selecting appropriate security controls was missing. Also similar to last year, systems were certified and accredited without testing of security controls.

When implemented properly, the combination of certification and accreditation is a powerful method for helping to ensure that effective management, operational, and technical controls are in place and functioning as intended. Certification actions may be scaled to the level of IT security being evaluated, but they must be sufficient to confirm that the security features of the systems have been implemented as intended and are performing properly, and that the operational sites comply with requirements for physical, procedural, and communications security. This confirmation cannot be achieved without some amount of testing. Unless the certification and accreditation processes are rigorous, the assurances these credentials are intended to impart will be illusory. It is by confirming the substance and quality of such critical processes and

controls that IGs can play a uniquely valuable role: performance measures focus the Department on getting the job done; our work helps ensure the job is done right.

The Department recognizes the need for credible IT security processes and products. In FY 2002, to address this need, it began an IT security compliance program, which includes quality reviews of certification and accreditation materials for selected systems. This year, the Department plans to review these materials for all national critical, mission critical, and classified systems. This review program is a positive step. Nonetheless, our concern remains that aggressive schedules for certification and accreditation may weaken key processes intended to ensure needed IT security.

How We Perform Our Independent Evaluations

GISRA instructed IGs to perform annual independent evaluations of their agency's IT security programs and practices. The evaluation was to include testing the effectiveness of IT security control techniques for an appropriate subset of the agency's information systems. The Federal Information Security Management Act of 2002 (FISMA) similarly requires IGs to perform an independent evaluation, including testing a representative subset of the agency's information systems. OMB Memorandum M-01-08, *Guidance on Implementing the Government Information Security Reform Act,* January 16, 2001, stated that the Act recognizes that not all systems can be reviewed every year and directs IGs to use a sampling of systems to draw conclusions regarding the effectiveness of the agency's overall security program. This guidance also encourages IGs to use reviews performed by other experts in their evaluations.

We have followed this guidance and found it to be both practical and effective. Our independent evaluations consist of a mix of reviews:

- To assess the effectiveness of policy and oversight, we review the IT security program policies of the Department and selected operating units.

- To evaluate operational, technical, and management controls of nonfinancial systems, we review selected IT systems using NIST's *Security Self-Assessment Guide for Information Technology Systems.*

- To evaluate operational, technical, and management controls of financial systems, we use the results of the general control reviews of financial systems conducted by OIG contractors using GAO's *Federal Information System Controls Audit Manual* (FISCAM), which also include limited vulnerability assessments.

- To obtain additional information regarding the responsibilities of the agency head, training of personnel with significant IT security responsibilities, and integration of IT security into the capital planning and investment control process, we interview the CIO and senior IT security officials from the Department and selected operating units, and review pertinent documentation, including selected capital asset plans.

- To obtain coverage of additional operating units and systems, we review the risk assessment, security plan, security testing and evaluation materials (test procedures and results), and certification and accreditation documents for selected systems.

- To extend our coverage further, our evaluation also includes, when available, the results of IT security reviews performed by other parties—typically contractors engaged by the operating units—if we determine, in accordance with OMB guidance, that they are of sufficient quality, applicability, and independence.

Our independent evaluations are conducted by computer scientists and IT security specialists in our Office of Systems Evaluation, several of whom have security certifications and are active on interagency working groups addressing such topics as network security, certification and accreditation, and procurement. But our resources are very limited: we have about four full-time employees performing this work, not including our FISCAM staff and contractor resources. With 14 Commerce agencies and operating units and approximately 600 IT systems, we offer our perspective on the state of IT security in the Department based on our necessarily selective review. Although we do not have sufficient resources or time to validate the specific details of the annual IT security reports submitted by the Department and USPTO, our approach has not only promoted significant improvements in system and program security throughout the Department and USPTO, but has also served as a check and balance on their annual reporting. Our reviews provide objective and independent insight into the state of IT security Department-wide, and virtually every review we have conducted has prompted a major overhaul of policy, oversight, or system security management.

Our budget request for FY 2004 includes those resources we believe are essential for our office to perform further vital oversight tasks. The requested funding level would allow

us to perform vulnerability assessments and penetration testing of some nonfinancial systems, a compelling mechanism for demonstrating that vulnerabilities exist and intrusions are possible, and a task that OMB, the General Accounting Office, and we believe should be conducted by IGs. OMB guidance directs agencies to develop plans of action and milestones (POA&Ms) to remediate program- and system-level IT security weaknesses and track each deficiency until it is corrected. According to OMB, an IG-verified, agency-wide POA&M process will be one of three criteria necessary for agencies to improve their IT security status on the Expanding E-Government Scorecard. While we can determine whether the Department's POA&M process is sound, the funding we have requested will allow us to also validate the implementation of a sample of the corrective actions contained in the plans. At present, we are able to track the corrective actions only for deficiencies identified in our financial systems reviews. The increase also will allow us to conduct much-needed additional IT system and operating unit security program reviews.

We believe we have focused and leveraged our efforts effectively. We work closely with the Department CIO to ensure our efforts are complementary and mutually supportive. We also work with operating unit CIOs and, increasingly, with program officials. I believe that GISRA established an effective foundation for improving IT security in the federal government and that FISMA will reinforce this goal. It is a privilege to be able to contribute to improvements in this area, and we hope to do more as time goes on.

This concludes my statement. A list of the reports that are part of our independent GISRA evaluations is included as an attachment. Mr. Chairman, I would be happy to answer any questions you or other members of the subcommittee might have.

ATTACHMENT

U.S. Department of Commerce
Office of Inspector General
Evaluation and Audit Reports
on Information Technology Security

	Evaluations
1	Office of the Secretary, *Independent Evaluation of the Department's Information Security Program Under the Government Information Security Reform Act,* OSE-15260, September 2002.
2	United States Patent and Trademark Office, *Independent Evaluation of USPTO's Information Security Program Under the Government Information Security Reform Act,* OSE-15250, September 2002.
3	National Institute of Standards and Technology, *Additional Improvements Needed To Strengthen NIST's Information Security Program,* OSE-15078, September 2002.
4	United States Patent and Trademark Office, *Stronger Management Controls Needed for the Patent Application Capture and Review Automated Information* System, OSE-14926, August 2002.
5	Office of the Secretary, *Information Security Requirements Need to Be Included in the Department's Information Technology Service Contracts,* OSE-14788, May 2002.
6	United States Patent and Trademark Office, *Additional Senior Management Attention Needed to Strengthen USPTO's Information Security Program,* OSE 14846, March 2002.
7	Office of the Secretary, *Independent Evaluation of the Department's Information Security Program Under the Government Information Security Reform Act,* OSE-14384, September 2001.
8	Economics and Statistics Administration, *Additional Security Measures Needed for Advance Retail Sales Economic Indicator,* OSE-12754, September 2001.
9	United States Patent and Trademark Office, *Independent Evaluation of USPTO's Information Security Program Under the Government Information Security Reform Act,* OSE-14384, September 2001.
10	Office of the Secretary, *Program for Designating Positions According to Their Risk and Sensitivity Needs to Be Updated and Strengthened,* OSE-14486, September 2001.
11	Office of the Chief Information Officer: *Use of Internet "Cookies" and "Web Bugs" on Commerce Web Sites Raises Privacy and Security Concerns*, OSE-14257, April 2001.
12	Office of the Chief Information Officer: *Additional Focus Needed on Information Technology Security Policy and Oversight*, OSE-13573, March 2001
13	Office of the Chief Information Officer: *Critical Infrastructure Protection: Early Strides Were Made, but Planning and Implementation Have Slowed*, OSE-12680, August 2000.

Financial Statements Audits [These audits are performed annually; listed below are only the audits covering FY 2000 and FY 2001.]	
14	U.S. Department of Commerce, *Consolidated Financial Statements, Fiscal Year 2001, Improvements Needed in the General Controls Associated with the Department's Financial Management Systems,* Audit Report No. FSD-14474-2-0001, February 2002.
15	Bureau of the Census, *Improvements Needed in the General Controls Associated with Census' Financial Management Systems,* Audit Report No. FSD-14473-2-0001, February 2002.
16	National Technical Information Service, *Improvements Needed in the General Controls Associated with NTIS's Financial Management Systems*, FSD-14476-2-0001/February 2002.
17	National Oceanic and Atmospheric Administration, Improvements Needed in the General Controls Associated with Financial Management Systems, FSD-14475-2-0001/February 2002.
18	Department of Commerce: *Consolidated Financial Statements, FY 2000*, FSD-12849-1, March 2001.
19	National Institute of Standards and Technology, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12859-1, February 2001.
20	Economic Development Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12851-1, January 2001.
21	Bureau of the Census, *Improvements Needed in the General Controls Associated with Financial Management Systems* and *FY 2000 Penetration Test Results*, FSD-12850-1, January 2001.
22	National Technical Information Service, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12857-1, January 2001.
23	Office of the Secretary, *Follow-up Review of the General Controls Associated with the Office of Computer Services/Financial Accounting and Reporting System*, FSD-12852-1, January 2001.
24	International Trade Administration, *Review of General and Application System Controls Associated with the Fiscal Year 2000 Financial Statements,* FSD-12854-1, January 2001
25	National Oceanic and Atmospheric Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12855-1, December 2000.
26	United States Patent and Trademark Office, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12858-1, December 2000.

Mr. PUTNAM. At this time I would like to recognize Robert Cobb. Following nomination by President Bush and confirmation by the Senate, Robert Cobb took office as NASA's Inspector General in April 2002. Mr. Cobb, in his capacity as a member of the President's Council on Integrity and Efficiency, serves as the Chair of that organization's Information Technology Roundtable, which promotes a coordinated approach to information technology issues among inspectors general across the executive branch. He also serves as an observer to the Columbia Accident Investigation Board, which is examining the February 2003 loss of the space shuttle Columbia and her crew.

Mr. Cobb was previously associate counsel to the President. In this role, he handled administration of the White House ethics program under the supervision of the counsel to the President, and was responsible for the administration of the conflict of interest and financial disclosure clearance process for candidates for nomination to Senate-confirmed positions. Prior to joining the Office of the Counsel to the President, Mr. Cobb worked for almost 9 years at the U.S. Office of Government Ethics.

We welcome you. You are recognized for 5 minutes.

STATEMENT OF ROBERT COBB, INSPECTOR GENERAL, NASA

Mr. COBB. Thank you, Chairman Putnam, Ranking Member Clay, Vice Chair Miller. Thank you for the opportunity to discuss information security at NASA and the impact of GISRA and FISMA on the agency's information security program. The Office of Inspector General is committed to helping the agency improve IT security through our ongoing program of IT audits and investigations. I will discuss three areas: the current state of NASA IT security, our audit of the information NASA submitted to OMB under GISRA in fiscal year 2002, and our plans to audit the information submitted by NASA under FISMA in 2003.

First, I want to highlight some of the unique challenges associated with securing NASA's IT resources. The NASA vision and mission concern challenges for scientific exploration and discovery. NASA pursues these challenges with a broad array of programs, including research and development in aeronautics, space exploration, and space flight. Needless to say, these endeavors require a complex range of IT systems.

As context and setting for NASA's IT security challenges, NASA carries out a civilian mission where the distribution of information about scientific exploration, discovery, and achievement is practiced by the agency and expected and desired by the public. NASA is a highly visible agency, with many readily available Web sites, and thus is a natural target for those seeking to illegally access government systems. NASA's IT security program is reliant on the participation and dedication of all employees, contractors, and other partners with access to NASA information. NASA, like every other agency, faces a challenge in convincing its work force that IT security is a primary rather than a secondary responsibility.

The OIG has examined the state of NASA's IT security, and we identified it as a significant management challenge in our December 2002 report to the Administrator. IT's security activities at NASA have historically been carried out on a decentralized basis.

This has resulted in a lack of full interoperability among the systems. NASA is moving toward a one-NASA concept, with a greater centralization and integration. However, as long as NASA's governance structure is such that center CIOs and center security officials report to center directors—who are program officials—rather than to NASA's CIO and chief security officer, a fully integrated approach to IT security will be practically impossible at NASA.

As part of our work, we conduct audits of information security and perform investigations of the criminal misuse of NASA IT systems. Our recent activities have addressed a broad spectrum of security problems. There are examples from our ongoing investigations where inadequate IT security, such as weak password controls, resulted in unauthorized access to significant amounts of NASA data that was sensitive, but unclassified. The agency is aware of these cases and acknowledges that serious compromises have occurred.

In our audit work, we have reported on issues including inadequate security training for system administrators, an inconsistently applied program for ensuring security of sensitive systems, inadequate security plans for NASA's IT systems, and an inadequate incident response capability.

It's important to note that NASA has been responsive to our work and that corrective actions are planned or are underway to address key IT security challenges. Our 2002 GISRA submission reflected the results of 26 final reports and several ongoing assignments related to IT security at NASA. Our submission also reflected IT security-related work performed by the agency's independent accountants as part of their annual review of NASA's financial statements.

Additionally, we verified and validated the status of weaknesses identified in NASA's Fiscal Year 2002 Plans of Actions and Milestones. The agency generally incorporated our suggestions into their final version that they submitted to OMB.

Our fiscal year 2002 GISRA efforts were limited to unclassified systems because NASA did not have the national security information systems reviewed in accordance with GISRA requirements.

During fiscal year 2003, my office continues to conduct a series of IT security-related audits and assessments and will incorporate the results of this work into our FISMA submission. We will also followup on our 2002 GISRA report. Later this year we plan to start an audit of NASA policies to protect sensitive, but unclassified information.

The requirements of GISRA and FISMA are having a positive effect on IT security at NASA. The legislation and related OMB guidance provided NASA with a framework for more effectively managing IT security. Because GISRA, and now FISMA, hold agency heads responsible for IT security, NASA senior management is more focused on it. The legislation also requires the agency to consider the view of the Office of Inspector General and to deal with the issues raised in our independent evaluations, and, in my view, this has also had a positive impact on the agency.

Last, I would like to note that in the NASA OIG, we have an exceptional team of IT auditor, specialists and computer crimes professionals. Because of the investment the OIG has made in this

area, we have been able to provide leadership in the IT area to the IG community through my chairing of the IT Roundtable of the President's Council on Integrity and Efficiency. Through this roundtable, the NASA OIG has sought to promote the sharing of best practices in IT audits and investigations. This concludes my statement.

Mr. PUTNAM. Thank you very much, Mr. Cobb.

[The prepared statement of Mr. Cobb follows:]

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

U.S. House of Representatives

For Release on Delivery
expected at
10:00 a.m. EDT
Tuesday
June 24, 2003

Cyber Security: The Status of Information Security and the Effects of the Federal Information Security Management Act (FISMA) at NASA

Statement of

The Honorable Robert W. Cobb

Inspector General

National Aeronautics and Space Administration

Mr. Chairman, Ranking Member, and Members of the Subcommittee:

Thank you for the opportunity to discuss information security at NASA and the impact of the Government Information Security Reform Act (GISRA) and the Federal Information Security Management Act (FISMA) on the Agency's information security program.

My statement focuses on three areas:

- Key information technology (IT) security challenges faced by NASA and its actions and plans to address them.
- Our audit of the information NASA submitted to the Office of Management and Budget (OMB) under GISRA in fiscal year (FY) 2002.
- Our plans to audit the information submitted by NASA under FISMA in FY 2003.

Before discussing these areas, I want to highlight some of the unique challenges associated with securing NASA's IT resources and how they are inextricably linked to the complex mission and operating structure of the Agency.

The NASA vision and mission concern challenges for scientific exploration and discovery. NASA pursues these challenges with a broad array of science programs, research and development in aeronautics, and space exploration. These endeavors include solar system exploration; Astronomical Search for Origins; Earth Science; Biological and Physical Research; Aerospace Technologies; the Space Launch Initiative; Education Initiatives; Space Flight, including the International Space Station and the Space Shuttle; and the corporate and institutional infrastructure to support these programs.

NASA employs about 19,000 civil servants and has a much greater number of contractor employees working on NASA programs at 11 major installations (including Headquarters, the 9 Centers, and the Jet Propulsion Laboratory). The Centers have diverse roles and historical cultures and, over time, have had substantial operational freedom in fulfilling mission objectives. NASA, like every other agency, faces a challenge in convincing its workforce that IT security is a primary rather than secondary responsibility.

The environment in which NASA IT systems operate provides a context and setting for understanding NASA's IT security challenges. The elements of this environment include:

- NASA has hundreds of programs requiring unique IT solutions.
- NASA's information security program is reliant on the judgment of all persons with access to sensitive information.
- NASA has a responsibility to protect varied types of sensitive and classified information.

- NASA carries out a civilian mission for which distribution of information about scientific exploration, discovery, and achievement is practiced by the Agency and expected and desired by the public.
- Contractors receive 90 percent of NASA dollars.
- NASA is a highly visible agency with many readily available Web sites, making it a natural target for those seeking to illegally access Government systems.
- NASA scientists and engineers focus on meeting specific program objectives and may not give sufficient attention to the IT security environment.
- NASA scientists and engineers often work in "open" educational environments with university scientists where "closed" information systems are an anathema.
- NASA maintains many institutional and mission-critical information systems for which security is critical in carrying out NASA programs and operations.

In my view, IT security comprises two elements: protection of information and protection of the IT resources that support information processing and storage. Information must be sufficiently protected to ensure confidentiality, integrity, and availability. Similarly, IT resources must be protected to ensure that hackers do not compromise them or programs that rely on them.

The requirements of GISRA and the recently enacted FISMA are having a positive effect on the state of IT security at NASA. The most positive impact has resulted from the laws' requirements to view the Agency's IT security posture as a whole, rather than as separate parts. The legislation and related OMB guidance have provided NASA with a framework for more effectively managing IT security. As a result, NASA senior management is increasing the attention given to IT security. The legislation also requires the Agency to consider the view of the Office of Inspector General (OIG) and to deal with issues raised in our independent evaluations.

NASA's unique mission and sophisticated operations present great challenges to those responsible for IT security. My office is committed to helping the Agency improve IT security through our ongoing program of IT audits and investigations.

THE STATE OF INFORMATION SECURITY AT NASA

Our December 23, 2002, report to the Administrator identified IT security as a significant management challenge. IT security activities at NASA have historically been carried out on a decentralized basis. This has resulted in a lack of synchronization in development efforts and a lack of full interoperability among the systems developed. We have reported on issues including inadequate security training for system administrators, an inconsistently applied program for ensuring security of sensitive systems, inadequate implementation of NASA's host and network security policies and procedures, inadequate security plans for NASA's IT systems, and an inadequate incident response capability. The independent public accountant responsible for NASA's FY 2002

financial statement audit identified several IT security deficiencies relating to the general controls environment over NASA's IT architecture that processes financial applications.

The previous NASA Acting Chief Information Officer (CIO) concluded in a briefing to the OIG on September 3, 2002, that NASA's internal systems could not support e-government initiatives as envisioned in the President's Management Agenda. Among the reasons cited were unacceptable security vulnerabilities. OMB reports NASA's status as "red" for e-government, noting among other issues weaknesses in some areas of IT security including program management, implementation, and evaluation.

On the positive side, we believe that NASA's leadership has implemented several IT security improvements and is now formulating plans to address many of the IT security concerns we have raised in past audits and investigations. The most promising overall improvement has been the recognition by the former Acting NASA CIO and the current NASA CIO that IT security is a problem that NASA must effectively address. We believe these positive changes should help to improve NASA's overall IT security posture.

Centralization and Integration of IT Security Is Needed

The implementation of security solutions is individual to NASA Centers and is not enterprise-wide. NASA is moving toward a OneNASA concept, with plans to implement a governance model that moves to a more centralized and integrated method of operating. NASA also plans to revise its IT security architecture. If implemented correctly, centralization and a revised architecture will improve the Agency's information security posture. However, as long as NASA governance structure is such that Center CIOs and security officials report to Center Directors—who are program officials—rather than to the NASA CIO and the Agency's Assistant Administrator for Security Management and Safeguards, a fully integrated approach to information security will be impossible at NASA.

Responsibility for overall IT security at NASA is divided between two organizations. For all unclassified systems, the Office of Security Management and Safeguards has responsibility for IT security policy and oversight, while the Office of the CIO has responsibility for IT security operations, procedures, and guidance. For classified systems, the Office of Security Management and Safeguards has responsibility for IT security policy, procedures, and guidance. These responsibilities for IT security have changed since NASA submitted its FY 2002 GISRA report. The FY 2002 report indicated that the NASA CIO maintained leadership of the entire IT security program.

NASA has established a Competency Center for IT Security (CCITS), currently the Ames Research Center in California. The CCITS is responsible for the technical coordination of information security implementation, the adoption of best security practices, information security consulting, and coordination of security incident reporting and analysis. NASA has integrated IT security into the Agency's capital planning and

investment control process. Furthermore, NASA's IT security program is integrated with its critical infrastructure protection responsibilities and other security programs. A Critical Infrastructure Protection Team is responsible for identifying NASA's critical cyber-based infrastructure assets.

NASA's Center Directors have oversight responsibilities for ensuring that an effective Center IT security program is established and maintained. Directors ensure compliance with Federal, Agency, and Center IT security policies, standards, and practices. Center IT Security Managers are appointed by the Directors to provide organization and direction for implementing the NASA IT Security Program at the Center level. Each Director appoints a Designated Approval Authority to accredit information resources for processing national security information. Centerwide IT security plans are approved by the Center Directors.

Each Center has a CIO responsible for establishing an effective and economical program at the Center. Senior organizational managers (e.g., Directorate Chiefs, Division Chiefs, Program Managers, Chief Financial Officer) have a role in supporting IT security planning, budgeting, and training. Each senior manager appoints a Computer Security Official who serves as a critical communication link to and from the organization for all IT security matters.

IT Security Weaknesses Identified in Recent Reports

We have an exceptional team of IT auditors, specialists, and computer crimes professionals who conduct audits of information security and perform investigations of the criminal misuse of NASA computers and attacks against the Agency's information and communication systems. Our aggressive pursuit of those responsible for illegal cyber activities outside and within the Agency is intended to serve as a deterrent. Because of the investment that the NASA OIG has made, we have been able to provide leadership in the IT and IT security areas to other OIGs. In my role as Chairman of the IT Roundtable for the President's Council on Integrity and Efficiency, I have sought to use my office's resources to promote the sharing of best practices in IT audits and investigations.

The General Accounting Office (GAO) designated computer security in the Federal Government as high risk in 1997. GAO continues to find evidence of pervasive weaknesses Governmentwide. The dramatic increase in computer interconnectivity and dependence on computers has, in part, caused such risks to increase. This year, GAO expanded this risk area to include protecting the information systems that support our nation's critical infrastructures.

During the course of an audit or investigation, our personnel often uncover systemic IT problems that are the root causes of compromises. Our recent activity covers a broad spectrum of security issues and criminal enterprises ranging from security training to

unauthorized access to sensitive information. Some examples of our work involving IT security at NASA follow:

Security Training

We continue to find that system administrators with responsibilities for system security have not received proper technical security training. We have linked inadequate technical training to security implementation problems in critical NASA systems. Individuals responsible for security administration must remain current with ever-changing technology. Without a trained and knowledgeable workforce, security administrators may not understand the vulnerabilities in the systems for which they have responsibility and may not be able to effectively secure them.

Implementation of Host and Network Security

We continue to find inadequate implementation of NASA's computer security policies in major NASA systems, including mission-critical systems. Contractor personnel manage most NASA systems with oversight from NASA. Inadequate security implementation can be attributed to a variety of problems, including unfamiliarity with NASA policy, differing interpretations of policy, inadequate training, and inadequate security tools. We have recently reported inadequate operating system and database security implementations and the need to strengthen firewall filtering, network monitoring, and other network controls.

Particularly noteworthy is our ongoing assessment of the use of wireless networks at NASA. Wireless networks are a versatile and efficient method for transferring data between computer systems. However, their use has several potential security risks. Our assessment to date has identified wireless networks in use at NASA that are not adequately secured. In large part, this was caused by the absence of an Agencywide policy to address wireless network security.

Incident Response Capability

NASA has established formal procedures for reporting security incidents for unclassified systems and for sharing information regarding common vulnerabilities. The procedures require the IT Security Manager at each NASA Center to report most incidents to the NASA Incident Response Center (NASIRC), which provides an Agencywide computer and network systems incident response and coordination capability. In turn, the NASIRC provides incident information to the Federal Computer Incident Response Center (FedCIRC), which is responsible for coordinating an incident response for Federal and civilian agencies.

We found that NASA Centers were not submitting all required reports on IT security incidents to the NASIRC. Thus, senior NASA IT security managers lacked incident information on an Agencywide basis, and NASA underreported and incorrectly reported incidents to the FedCIRC. Additionally, information in the NASIRC incident database

was unreliable for a variety of reasons, and the NASIRC could not produce accurate, complete, and meaningful analyses and reports. NASA agreed to address all OIG recommendations associated with this evaluation. Among the solutions proposed by the NASA CIO is one to shift the responsibility for identifying, reporting, and analyzing hostile probes to a centralized operation during FY 2003.

Unauthorized Access to Sensitive Information

There are examples from our ongoing investigations where inadequate IT security, such as weak password controls, resulted in unauthorized access to significant amounts of NASA data that was sensitive but unclassified. The Agency is aware of the cases and acknowledges that serious compromises have occurred. It would not be appropriate to share the details in any open forum.

Compromise of NASA and Department of Defense (DOD) Systems

Following the compromise of 15 NASA computer systems at 5 separate NASA Centers, we traced the attacks to a hacker in the United Kingdom. When NASA intrusion data was correlated with DOD data, it was determined that this hacker had compromised approximately 90 DOD computers. Based on a request from our office, authorities in the United Kingdom executed a search warrant in London and identified the hacker as Gary McKinnon. The Department of Justice (DOJ) is currently seeking McKinnon's extradition. We have been told that this is the first time DOJ has sought extradition for an alleged computer hacker.

Inconsistencies in Interpretation of NASA IT Security Guidance

On several occasions, we found that security weaknesses may be the result of inconsistent interpretations of NASA IT security guidance by the Centers. Of particular note was unclear guidance regarding IT security incidents and disaster recovery planning and testing. We reported that NASA disaster recovery planning and testing guidance did not define testing or describe the extent to which testing of the disaster recovery plan should be conducted. Without adequate guidance, NASA system managers test their systems to the extent they deem appropriate. We found that plans for mission-critical systems were sometimes tested less stringently than those for less critical systems. As a result, we recommended that certain guidance be clarified. NASA is currently updating and clarifying IT security guidance.

IT Security Performance Measures

We reported that improved performance measures were needed for vulnerability scanning, monitoring security throughout an IT system's life cycle, IT security plans, and incident response.

When performing vulnerability scanning, certain NASA Centers did not scan and obtain results on all IT systems. Some Centers adjusted their scanning results for exemptions

(known system vulnerabilities that were not corrected because the Center CIO had accepted the risk) and did not report them as required. As a result, NASA did not have an accurate vulnerability assessment of its networks.

Due to inadequate performance measures for monitoring security throughout an IT system's life cycle, NASA had limited assurance that its managers had considered specific risks and implemented appropriate controls for each life-cycle phase.

IT officials inaccurately reported to the NASA CIO that they had properly accomplished IT security plans for certain systems in accordance with NASA guidelines and OMB requirements. This decreased the NASA CIO's ability to effectively monitor and manage the Agency's IT security program.

NASA's FY 2002 incident response performance measure did not require the Agency to pass all of its test elements and was not comprehensive enough to fulfill the Agency goal to thwart intrusion attempts.

NASA's Actions and Plans to Address Key IT Security Challenges

NASA is making progress in improving IT security. The plan to establish a OneNASA governance model includes centralizing certain key security services and establishing a control process to ensure uniformity. Consolidation activities under the OneNASA architecture should also provide cost reductions. NASA plans to upgrade and standardize its IT security architecture to provide meaningful and realistic guiding principles and standards to be applied when designing and implementing information services for NASA users. This is a major step in the right direction.

Planning is underway to staff an assurance group within the Office of Security Management and Safeguards to validate that NASA IT security policy is being implemented. Current IT security guidance is being revised for clarity and to address new issues. NASA continues to deploy its Public Key Infrastructure (PKI) technology to perform encryption between applications on its networks and to resolve infrastructure and technical issues. This process has been slow. NASA also plans to enhance system vulnerability scanning and to deploy intrusion detection systems and rapid response capabilities to attempted break-ins.

NASA has also started a new program that requires all system administrators to be certified. This should result in the development of a consistent measure of the knowledge of their workforce. The measure is key to the implementation of appropriate IT security measures. NASA also plans to expand training to address IT security planning and risk analysis and to mandate various IT security courses for users, managers, and system administrators, as well as specialized courses for IT security personnel. Plans are also underway to make IT security and risk management a key component of system development activities. Finally, NASA is making progress in developing metrics for IT security performance and in instituting a comprehensive corrective action program

system to prioritize, track, and manage efforts to close security performance gaps and to support FISMA requirements. Whether all plans come to fruition remains to be seen. My office is committed to continued reviews of IT security. As part of our program, we will monitor and evaluate critical Agency remediation plans and results.

OIG REVIEW OF NASA'S FY 2002 GISRA SUBMISSION TO OMB

We performed numerous reviews relating to the Agency's unclassified IT security and infrastructure protection activities and used the results of those reviews in responding to OMB's FY 2002 reporting instructions. Additionally, we verified and validated the status of weaknesses identified in NASA's FY 2002 Plans of Action and Milestones (POA&M). Based on the results of our work, we suggested various changes to the Agency's draft submission. The Agency generally incorporated our suggestions into the final version submitted to OMB.

Our FY 2002 GISRA submission reflected the results of 26 final reports, 9 draft reports, and 2 ongoing assignments related to IT security at NASA. Our submission also reflected IT security-related work performed by the Agency's independent accountants as part of their annual review of NASA's financial statements. The reports and ongoing assignments addressed the following areas:

- NASA information systems processing national security information.
- The Agencywide IT security program for unclassified systems.
- NASA's planning and implementation for Presidential Decision Directive 63, "Protecting America's Critical Infrastructures," (Phase III).
- Capital planning for IT security.
- IT security requirements in NASA contracts, grants, and cooperative agreements.
- Performance management related to NASA IT security program goals.
- Approvals for accessing IT systems.
- UNIX security and integrity controls (various reports on individual NASA systems).
- Network firewalls.
- NASA's implementation of PKI.
- Internet-based spacecraft command security issues.
- NASA's Advanced Aeronautics Program.
- Removal of data from computer storage devices.
- NASA's incident response capability.
- Penetration testing at NASA.
- Management and control of authentication tokens.
- Operating system controls in a Space Shuttle problem-management system.
- NASA's implementation activities for critical cyber-based infrastructure assets (Phase II).
- IT security controls in NASA's financial management systems.

Our FY 2002 GISRA efforts were limited to unclassified systems because NASA did not provide the documentation that we needed to determine whether the Agency had complied with GISRA requirements pertaining to systems that process national security information. NASA management attributed its nonresponse to increased national security requirements caused by the September 11th terrorist attacks. NASA management stated that the National Security Agency had been unable to conduct its FY 2002 assessments of NASA's national security systems as a result of the increased workload on national security resources.

We also performed unique work to comply with OMB's GISRA reporting instructions including:

- We reviewed Center system inventories to determine whether they included both operational[1] and nonoperational[2] systems and whether the NASA CIO ensured that the Agency implemented its IT security plan throughout the life cycle of IT systems. We also asked the Centers to validate the inventories for completeness. Four of the 11 installations reviewed did not have an inventory of nonoperational systems. Of the remaining Centers that had inventory lists, we could not be assured that three of the system inventories contained all systems.

- We reviewed the Agency's progress in incorporating the NASA Federal Acquisition Regulation (FAR) Supplement 1852.204-76[3] in contractual documents to determine whether program officials used appropriate methods to ensure the security of contractor and other Agency-provided services. We also reviewed contractor operations related to host-based security, firewall[4] capabilities, authentication tokens, and removal of sensitive data from storage devices. We evaluated the Centers' and their contractors' efforts to reduce IT security vulnerabilities and reviewed a third-party's penetration testing activities.

---

[1] NASA Procedures and Guidelines 2810.1, "Security of Information Technology," identifies eight life-cycle phases. We defined operational systems as those in the final three phases: operations, upgrade, and disposal of assets at the end of their useful life.

[2] We defined nonoperational systems as those in the first five life-cycle phases: project initiation, project definition, design, construction, and installation/integration/testing.

[3] NASA FAR Supplement 1852.204-76 states that the contractor shall be responsible for IT security for all systems connected to a NASA network or operated by the contractor for NASA. The supplement also requires the contractor to provide, implement, and maintain a NASA-approved IT security plan; screen personnel requiring privileged access to systems operated by the contractor for NASA or interconnected to a NASA network; ensure its employees receive annual IT security training in NASA's IT policies and procedures; and incorporate the IT security clause in all applicable subcontracts.

[4] A firewall is designed to prevent unauthorized access to or from a private network. The firewall examines messages entering or leaving and blocks those that do not meet specified security criteria.

OIG PLANS TO VALIDATE THE NASA FY 2003 FISMA SUBMISSION TO OMB

During FY 2003, my office continued to conduct a series of IT security-related audits and assessments. As we did in FY 2002, we will incorporate the results of this work into our FISMA submission as well as any unique reporting requirements contained in OMB's FY 2003 reporting instructions for FISMA. We are conducting extensive follow-up work to determine whether weaknesses discussed in our FY 2002 GISRA report have been corrected. Finally, we will continue to review the Agency's POA&M prior to its submission to OMB. Ongoing FISMA-related audit work addresses the following areas:

- Database security and integrity.
- Information assurance controls for International Space Station software development and integration systems.
- Information assurance controls for engineering design systems supporting Space Shuttle ground operations.
- Information assurance controls for Space Shuttle launch test, control, and monitor systems.
- Security controls in NASA's Integrated Financial Management System.
- Information assurance controls in the Hubble Space Telescope Program.
- NT Security in a Center master domain.
- Information category designations in NASA systems.
- Security of wireless networks at NASA Centers.
- IT controls for NASA's FY 2003 Financial Statement Audit.

Also during FY 2003, we plan to start an audit of the adequacy of NASA policies to protect unclassified but sensitive information. We will address the adequacy of policies to prevent the unauthorized compromise of sensitive information, including disclosure, theft, destruction, alteration, and fabrication of information.

This concludes my formal statement. I will be pleased to answer any questions the Subcommittee may have.

Mr. PUTNAM. We have a large panel, and I would ask that everyone be respectful of our 5-minute time limit.

I now introduce Scott Charbo. Agriculture Secretary Ann Veneman named Scott Charbo as Chief Information Officer at the U.S. Department of Agriculture in August 2002. As CIO, Mr. Charbo is responsible for the overall management of USDA's information resources and IT assets, overseeing more than 4,000 IT professionals and $1.7 billion in physical assets. He comes to the CIO position from the USDA Farm Service Agency where he served as director of the Office of Business and Program Integration since July 2002. He was responsible for planning, developing, and administering the agency's programs and policies, and provided direction in the areas of economic and policy analysis, appeals and litigation, strategic management, and corporate operations, outreach programs, and strategic planning and leadership in the agency's citizen-centered E-government initiatives.

Welcome to the subcommittee. You are recognized.

STATEMENT OF SCOTT CHARBO, CHIEF INFORMATION OFFICER, DEPARTMENT OF AGRICULTURE

Mr. CHARBO. Thank you, Mr. Chairman. With your permission, I will submit my testimony.

At the Department of Agriculture, I am responsible for computer systems that support billions of dollars in annual program benefits. Information stored on these systems include Federal payroll data and market-sensitive crop, commodity, and farm data, information on food stamps and food safety and proprietary research data. This information is one of USDA's greatest assets.

Mr. Chairman, we at USDA are doing a better job initiating change and managing information in IT security at USDA; however, our size, decentralized organization, and the wide array of hardware and software in use, combined with the magnitude of today's cyber threats, mean that we have a tremendous amount of work remaining to reduce the risk to our information assets to an acceptable level.

Historically, each USDA agency and office funded and managed its own IT investments independent of other organizations in the department. Likewise, security controls employed to protect these investments have been selected independently. This decentralized management structure has created an environment where some USDA agencies have addressed the issues of security and risk while others have not.

Today, assuring a high level of information security in every USDA agency is a critical issue of USDA's management. Representative of this commitment, we have begun holding our senior executives accountable by including a performance measure in their annual performance plan directly tied to implementing their FISMA plan of action milestones report. With funds from Congress, we are continuing to build a central cyber security program that is providing our agencies with uniformed policies, guidance tools, and program management. We are setting clear cyber security goals and then assisting agencies in meeting them. Through our IT capital planning investment control process, we are also doing a better job integrating security in all phases of our IT project life

cycle, from initial planning to system retirement. This story of good progress and change with much more work to do is representative of our numbers.

In 2004, USDA plans to spend about 68 million to protect our information assets. This represents an increase of 6 percent over the 64 million in securities spending estimates in fiscal year 2003. In the past year, six agencies completed risk assessments of their cyber security programs from qualified security contractors, with an additional four now underway. Similarly, nine USDA organizations created independent security risk assessments on 26 separate systems. Many others are currently in the process of completing assessments. Over the past 2 years, we have deployed intrusion detection and antivirus software across the Department. Just this month we held a training session for agency IT staff on how to deploy the Department's latest patch management software solution. By deploying patch management software, we will ensure the most recent releases of software patches.

Finally, our USDA FISMA and plan of action and milestones report currently shows that we are taking 1,405 distinct actions to address 243 program and system-level weaknesses. While the numbers we report go up and down as threats to our systems change, I am confident we will see progress in our POA&M report.

At USDA, we are fortunate to have a strong senior information security officer and staff who drive our information and IT security efforts. They are the ones who deserve the credit.

Mr. Chairman, in your invitation to this hearing, you asked to discuss the actions that we are taking to remedy the deficiencies in both our GISRA and financial reporting. I will focus my comments on the highest-priority initiatives.

Information assurance starts with employee education and awareness. We are spending—spreading the word across USDA through online courses like the government standard GoLearn.gov classroom training, and numerous technical and management forums.

Recognizing the importance of this issue, the Secretary and I are personally addressing these concerns at our subcabinet meetings and during regular briefings for our agency heads. We are making good progress establishing executable business resumption and recovery plans for critical information systems. At USDA, we are finalizing a standard certification accreditation methodology and process for our agencies to verify and attest that information security functions as required.

As I mentioned earlier, we revised our IT capital planning investment control guidance to ensure system owners address security at all stages of an IT project's life cycle.

I would also like to mention one modernization project that is critical to strengthening cyber security at USDA. We are redesigning our long distance telecommunication network to support the growing demand for E-government services, once implemented. Our

system will greatly improve our ability to verify the integrity and confidentiality of data transmitted over the network.

Thank you for the opportunity to be here, Mr. Chairman. Thank you.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Charbo follows:]

STATEMENT OF
SCOTT CHARBO
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF AGRICULTURE
BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

June 24, 2003

Mr. Chairman and Members of the Subcommittee, thank you for inviting me here today to discuss the challenges and opportunities we face and the progress we are making on protecting the information and systems entrusted by the public to the U.S. Department of Agriculture (USDA). With your permission, I will submit my testimony for the record.

At USDA, I am responsible for computer systems that support billions of dollars in annual program benefits. Information stored on these systems includes: Federal payroll data, market sensitive (crops, farm, commodities, statistical) data, geographical data, information on food stamps and food safety, and proprietary research data. This information is one of USDA's greatest assets. Threats to these assets are numerous, ranging from outright transferring of funds and personal/customer/program information -- to cyber-attacks that leave our information systems crippled or inoperable. Audit reports conducted by both USDA's Office of Inspector General (OIG) and the General Accounting Office (GAO), as well as our own review, have identified significant weaknesses in our overall computer security program.

Mr. Chairman, as you know, our push to deliver more and more services electronically makes protecting these services a high priority. I believe we at USDA are improving in the job we do in this area. Currently, we are implementing significant changes in how we manage information and IT security positions at USDA. However, our size, decentralized organization, and the wide array of hardware and software in use, combined with the magnitude of today's cyber threats, mean that we have a tremendous amount of work remaining to reduce the risk to our information assets to an acceptable level.

The State of Information Security at USDA

USDA's 18 agencies and 12 staff offices together employ over 100,000 people. The Department's fiscal year (FY) 2004 Budget requests about $2.25 billion for IT investments to support the services and products we deliver. Historically, each agency/office funded and managed its own IT investments independent of all other organizations in the Department. Likewise, security controls employed to protect these investments have been selected independently. This decentralized management structure has created an environment where some USDA agencies have addressed the issues of security and risk, while many others have not.

Today, ensuring a high level of information and computer security in every USDA agency is a critical issue for USDA's management. Representative of this commitment, we have begun holding our senior executives accountable by including a performance measure in their annual performance plan related to the security of their information and systems. With funds from Congress, we are continuing to build a central cyber security

program that is providing our agencies with uniform policies, guidance, tools, and program management; we are setting clear cyber security goals and then assisting agencies in meeting them. Through our IT capital planning and investment control process, we are also doing a better job integrating security into all phases of our IT projects lifecycle, from initial planning to system retirement.

This story of good progress and change with much more work to do is represented in our numbers:

- In FY 2004, USDA plans to spend about $68 million to protect our information assets. This represents an increase of 6% over the $64 million in cyber security spending estimated for FY 2003.

- In the past year, 6 agencies completed risk assessments of their cyber security programs from qualified security contractors, with an additional 4 now underway. Similarly, 9 USDA organizations completed independent security risk assessments on 26 separate systems. Many others are currently in the process of completing assessment of their respective programs and systems.

- In the Office of Management and Budget's review of the 51 systems in our FY 2004 Major IT Systems Portfolio, 43% (or 22 systems) received a passing security score. This is the first year we received security scores from OMB.

With the additional planning and training we are conducting this year, I expect all USDA's FY 2004 investments to receive passing scores from OMB.

- Over the past two years, we have deployed intrusion detection and anti-virus software across the Department. Just this month, we held a training session for agency IT staff on how to deploy the Department's latest patch-management software solution. By deploying patch management software we will be able to ensure the most recent releases of software patches are consistently and timely installed across our enterprise.

- Finally, our USDA Government Information Security Reform Act (GISRA) Plan of Actions & Milestones (POA&M) currently shows that we are taking 1,405 distinct actions to address 243 program and system level weaknesses. While the numbers we report will go up or down as the threats to our systems change, I am confident we will see progress in our POA&M reporting.

At USDA, we are fortunate to have a strong information security officer and staff, who drive our information and IT security efforts. They have been instrumental in building our program over the past three years, and deserve much of the credit for the accomplishments and activities I am talking about here today.

USDA Actions to Correct Deficiencies Reported in FISMA and Financial Reporting

Mr. Chairman, in your invitation to this hearing, you asked me to discuss the actions that we are taking to remedy the deficiencies reported in both our GISRA and financial reporting. While USDA's cyber security program covers the full range of technical and management disciplines, I will focus my comments on our highest priority related initiatives.

- Security Awareness: Information Assurance starts with employee education. All employees, from general users to system administrators to senior executives, need to understand the threats to the assets they manage and their cyber security responsibilities. We are spreading the word across USDA through online courses like the government standard GoLearn.gov E-Learning program, classroom training, as well as numerous technical and management forums.

Recognizing the importance of this issue, the Secretary and I are personally raising this issue at our Subcabinet meetings and during regular briefings for our Agency Heads.

- Disaster Recovery and Business Resumption Planning: We are making good progress establishing executable Business Resumption and Disaster Recovery Plans for USDA's most critical information systems. With funding from Congress, we are providing the methods, policy, training, tools, guidance and oversight to agency program and technical managers. By the end of this calendar

year, I expect to see high-quality, consistent, and verified Disaster Recovery and Business Resumption plans for our highest priority systems.

- Certification & Accreditation: The Office of Management and Budget has made it clear that our information systems must be fully certified and accredited. At USDA, we are finalizing a standard methodology and process for our agencies to use to verify and attest that information system security: 1) functions as required, and 2) assures the confidentiality, availability, and integrity of its data and processes. Certification is an intensive, time consuming, and costly process. With this in mind, our goal is to certify and accredit all of our highest priority systems by July 2004.

- Integrating Security into the IT Capital Planning and Investment Control Process: As I mentioned earlier, we revised our IT Capital Planning and Investment Control guidance to ensure system owners address security in all stages of an IT project's lifecycle. In our IT plans, investment owners must demonstrate how they are preparing to secure investments, and provide specific milestones for achieving critical security elements. This year, we are also strengthening our training for agency IT planners to ensure they understand the security and privacy requirements for their IT investments.

USDA Procedures, Processes and Structures to Institutionalize Daily Management of Information Security Risks

Mr. Chairman, you also asked me to discuss the procedures, processes and structures we are putting in place to assist in the transition from once-a-year reporting to institutionalization and daily management of information security risks.

At USDA, the Federal Information Security Management Act of 2002 (FISMA) reporting process has helped us more clearly track specific cyber security weaknesses, which in turn is helping us make better decisions, while holding us more accountable for results.

Currently, our agencies along with my office update all identified information security weaknesses and related corrective actions in a central FISMA POA&M database on a quarterly basis. We use this information in our quarterly and annual reports to OMB. We also use this information as a management tool, verifying and validating agency plans, and analyzing this information in the context of our knowledge of agency progress. When we began this process, there was some uncertainty as to the quality and comprehensiveness of our data. However, as our process matures, we have seen a significant improvement in the quality of information reported. This is moving USDA's security posture from reactive to proactive.

Our goal must be to continue integrating information security planning and reporting into our day-to-day IT management process. The Department's Enterprise Architecture (EA) and IT Portfolio Management initiatives will help us do this. Applying OMB's Federal

Enterprise Architecture guidance, we have begun documenting the EA layers (business processes, data, applications, and technology infrastructure). Analyzing and tracking this information, across all USDA agencies and offices, will enable us to better leverage our information and IT resources. Integrating our security architecture into each layer of the EA will help us ensure we're providing the right level of security for our data, applications, and technology. Similarly, our IT Portfolio Management initiative will allow us to consistently track the achievement of project milestones, including security milestones, for our IT investments.

Finally, I want to mention one modernization project that is critical to strengthening cyber security at USDA. We are redesigning our long distance telecommunications network to support the growing demand for E-Government services. Currently, the mostly decentralized structure of USDA's interconnected data centers and telecommunications networks means that the Department is only as strong as its weakest links. Once implemented, our future Universal Telecommunications Network will greatly improve our ability to verify the integrity and confidentiality of data transmitted over the network.

Mr. Chairman, thank you again for the opportunity to be here today. I am proud of the progress we are making in this area, and look forward to answering any questions you may have.

Mr. PUTNAM. I now recognize Mr. Ladner. Drew Ladner was appointed Chief Information Officer of the U.S. Treasury Department in March 2003. He is responsible for managing the Treasury's $2.5 billion information technology strategy and budget, serving as Treasury's official lead on E-government initiatives, and providing policy direction and oversight of the Department's security programs. Welcome to the subcommittee. You are recognized.

STATEMENT OF DREW LADNER, CHIEF INFORMATION OFFICER, DEPARTMENT OF TREASURY

Mr. LADNER. Thank you, Mr. Chairman.

Mr. Chairman, Ranking Member Clay, thank you for the opportunity to appear today to discuss the state of Treasury's IT security as well as the actions underway for remediating the Department's material weaknesses. The continued leadership of the chairman and the members of the subcommittee is essential if we are to improve IT security and accountability not only at Treasury but across the Federal Government.

The present state of Treasury's IT security requires improvement to achieve our objective: closing all IT-related material weaknesses as identified by GISRA's fiscal year 2002 review process. As of March 31, 2003, the Department had 14 material weaknesses. These included nine at the Internal Revenue Service, three at the Financial Management Service, one at the Mint, and one at the Departmental Offices.

To bolster IT security, Treasury has taken a number of actions to date to resolve outstanding issues addressed by the Treasury Inspector General and the Treasury Inspector General for Tax Administration.

First, Treasury has implemented an aggressive oversight and compliance program for IT security. During fiscal year 2003, reviews will have been completed for all of the bureau's IT security programs to establish a baseline for future annual reviews. This is the first time that the Department has conducted a complete review of the IT security programs.

Second, to maximize implementation success and accountability, Treasury has set specific goals to improve security with the use of performance measures, including the 80 percent to which Mark Forman alluded previously.

Third, a combined Federal Information Security Management Act 2003 data call has just been instituted by the Treasury CIO, IG, and TIGTA. This joint data call is expected to remedy the inconsistency to which the chairman referred earlier in reporting numbers in the last two surveys performed under GISRA.

Fourth, Treasury has taken further action to ensure the protection of our critical infrastructure cyber assets.

Fifth, to augment the FISMA requirement for periodic security training, Treasury has scheduled an IT security conference for the bureau's IT security managers and staffs. This conference will include high-level training sessions and targeted technical sessions focused on Treasury's IT security issues, along with promoting new CD-ROM and Internet-accessible training opportunities.

Treasury is committed to identifying the root causes of unacceptable IT security and putting in place the structures, processes, and

systems that will ensure the Department has a strong security regime. Let me describe several initiatives briefly that are key.

First of all, as soon as I began as Treasury CIO, I decided that my first priority as Treasury CIO would be IT governance. Pursuant to the Clinger-Cohen Act, the CIO's mission is to ensure that the Department wisely steward the funds of our taxpayer citizens on technology systems so that we can deliver ultimately valuable E-government services and other services. Establishing the right structures, processes, and systems of sound IT governance not only provides for sound planning and budget allocation, but also necessitates incorporating security considerations into our capital planning and investment controls. It's a cardinal rule in business operations that the quality of a design has a disproportionate impact on the life cycle cost of the system. If Treasury's systems are not secure when we develop and deploy, the Department leaves itself vulnerable until deficiencies are remediated and taxpayer dollars are not stewarded to boot.

An additional benefit is that Treasury increasingly aligns its IT operations with Department goals and objectives, achieving a more integrated, cohesive, and institutionalized security regime across Treasury.

In short, achieving a strategic, robust, and integrated security regime will be limited if our capital planning investment control process does not share those same characteristics.

In addition to the new IT governance regime, we are working very hard on the enterprise architecture that also achieves the goals that Mark Forman described previously. This will provide us a baseline for planning our security regime as well.

Third, proactive interagency collaboration on IT security provides additional evidence of the institutionalization of Treasury's IT security. The measures thereof are included in my submitted statement.

In the Office of the CIO, our mission is to steward Treasury's information resources with integrity and professionalism. I remain committed to doing that and working on everything we can do to ensure that your goals and this committee's on IT security are stewarded as well. Thank you very much.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Ladner follows:]

U.S. TREASURY CHIEF INFORMATION OFFICER TESTIMONY

BEFORE THE

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

Mr. Chairman and members of the Subcommittee, thank you for the opportunity to appear to discuss the state of Treasury's information technology (IT) security and financial reporting, as well as the actions underway for remediating the material weaknesses. The continued leadership of the Chairman and the members of the Subcommittee is critical if we are to improve IT security and accountability not only at Treasury but across the federal government.

I serve as the Chief Information Officer (CIO) of the Treasury Department. As CIO I provide oversight, strategic management, and policy direction of all information technology security programs within the Treasury Department and its Bureaus. In addition, I have operational responsibility for shared Enterprise services across all

Treasury bureaus, including the cyber protection measures applied to these services.

As articulated by the recent OMB report to the Congress on Federal Government Information Security Reform, IT security is a continuing challenge that warrants the attention of the Congress, the Executive Branch, industry, academia, and the taxpayer-citizens whom we serve. It is vital to our nation's financial institutions, economic prosperity, homeland defense, and E-Government service efforts. It is also crucial to achieving the Treasury's strategic objectives, and the Department continues to make great progress in improving the security of its IT systems. The Department has taken a number of measures to improve the overall IT security posture of the Department and to rectify the identified deficiencies in our GISRA FY 2002 submission to the Office of Management and Budget (OMB).

The present state of Treasury's IT security requires improvement to achieve our objective of closing all IT-related material weaknesses as identified by the Government Information Security Reform Act (GISRA) FY 2002 review process. As of March 31, 2003, the Department had

14 material weaknesses. These included nine (9) at the Internal Revenue Service (IRS), three (3) at Financial Management Service (FMS), one (1) at the Mint, and one (1) at Departmental Offices (DO). These weaknesses can be divided into two main categories: information technology (IT) security weaknesses and financial management weaknesses, with additional general weaknesses at the IRS. First I will address IT security issues, and then I will cover financial reporting.

Central to the IT security material weaknesses is that the Department has not yet achieved the goal of full certification and accreditation (C&A) of mission critical systems and major applications. In addition, specialized IT security training and incorporation of security into the capital investment planning process need improvement. Also included in the list of deficiencies are new and repeated material weaknesses identified by the General Accounting Office (GAO).

To bolster IT security, Treasury has undertaken a number of actions to date to resolve outstanding issues addressed by the

Treasury Inspector General (IG) and Treasury Inspector General for Tax Administration (TIGTA). First, Treasury has implemented an aggressive oversight and compliance program for IT security. Program reviews of each Bureau are conducted to evaluate progress in six areas: 1) security policy and guidance; 2) computer incident handling and response capability; 3) security training; 4) Plan of Actions and Milestones (POA&M) management; 5) integration of security into capital planning; and 6) system C&A. During FY 2003 reviews will have been completed of all Bureaus' IT security programs to establish a baseline for future annual reviews. This is the first time the Department has conducted a complete review of its security programs. Treasury now requires all Bureaus to use the National Institute of Standards and Technology (NIST) Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," for performing self-assessments of both their IT security programs and general support systems and major applications. In addition Treasury has developed and is using a security oversight

methodology and checklist based on NIST 800-26 for conducting department-wide security reviews.

Second, to maximize implementation success and accountability, Treasury has set specific goals to improve security with the use of performance measures. For example, 80% of all Treasury systems must be certified and accredited by the end of FY 2003. This target has been conveyed to the Bureau Heads by the Secretary and to their CIOs by the Assistant Secretary for Management and Chief Financial Officer. Progress of each Bureau is being tracked on a quarterly basis as we move towards reaching the Treasury C&A goal. Our C&A performance measure goal for FY 2004 is 90%.

Third, a combined Federal Information Security Management Act (FISMA) 2003 data call has just been instituted by the Treasury CIO, IG and TIGTA. This joint data call is expected to remedy the inconsistency in reported numbers from the last two surveys performed under GISRA. An enterprise corrective Action Plan and Milestone process for tracking and mitigating each Bureau's material weaknesses and deficiencies has been developed and implemented.

At present this is a manual process but plans are underway - as a cornerstone of Treasury's IT governance reform - to provide an enterprise portfolio management capability by which the Department and all Bureaus will have online access for tracking and will be able to update their status in meeting the established milestones.

Fourth, Treasury has taken further action to ensure the protection of our critical infrastructure cyber assets. We have established a Critical Infrastructure Protection (CIP) Working group consisting of representatives from all its Bureaus. A Project Matrix review to identify key Treasury critical assets is being conducted and a Treasury-wide CIP policy and a Critical Infrastructure Protection (Strategic) Plan with an associated Treasury CIP Implementation Plan have been developed and issued. Treasury has completed and issued to its Bureaus an Interdependency Analysis Guideline/Methodology for completing the next step of the Project Matrix. Treasury is in the process of prioritizing our critical cyber assets and conducting interdependency analyses on those identified as supporting national critical functions and services.

Fifth, to augment the FISMA requirement for periodic security training, Treasury has scheduled an IT security conference for the Bureaus' IT security managers and staffs. The conference will include high-level training sessions and some targeted technical sessions focused on Treasury IT security issues. Additional C&A training is planned for Treasury's senior officials who are Designated Accrediting Authorities (DAA) for IT general support systems and major applications. To share training and awareness information and tools across all Bureaus, the Department has established an IT Security Training Forum which meets quarterly.

The Department is concerned about the new and repeat material weaknesses that have surfaced and continue to remain on the books. Consequently, Treasury is committed to identifying the root causes of unacceptable IT security and putting in place the structures, processes, and systems that will ensure the Department has a strong security regime. Let me describe several key initiatives that I consider essential to our reform.

First, as soon as I began as Treasury CIO, I decided that my number one priority as Treasury CIO would be IT governance. In short, pursuant to the Clinger-Cohen Act, the CIO's mission is to ensure that the Department wisely stewards the funds of our taxpayer-citizens on technology and systems so that we can deliver valuable E-Government and other services. Establishing the right structures, processes, and systems of sound IT governance not only provides for sound planning and budget allocation but also necessitates incorporating security considerations into our capital planning and investment controls. It is a cardinal rule in business operations that the quality of a design has a disproportionate impact on the lifecycle cost of a system; if Treasury's systems are not secure when we develop and deploy, the Department leaves itself vulnerable until deficiencies are remediated, and taxpayer dollars are not stewarded. An additional benefit is that, as Treasury increasingly aligns its IT operations with Department goals and objectives across the Department, achieving a more integrated, cohesive, and institutionalized security regime across Treasury is facilitated. In

short, achieving a strategic, robust, and integrated security regime across the Department will be severely limited if our capital planning and investment control process does not share those same characteristics.

Therefore, Treasury seeks to integrate its security programs both functionally with our capital planning process and organizationally across Bureaus. In addition to the security oversight provided by the Office of the CIO, the Bureaus are required by policy to establish complementary capabilities within their respective bureaus to perform annual self-assessments of their security postures. To ensure that security is consistently implemented across the Department, a set of comprehensive IT security policies, standards and procedures have been developed and issued to all Bureaus. These policies address state-of-the-art technologies and capabilities and provide management, operational and technical controls. A recently established Treasury IT Security Policy Forum meets quarterly to discuss proposed policies and standards which are binding on all Bureaus.

Second, in addition to implementing a new IT governance regime, the Department is working on an enterprise architecture that incorporates a strict IT security regime. This will represent a baseline by providing the security for integration into the performance, business and technical reference models in accordance with OMB's Federal Enterprise Architecture framework. The Bureaus' security architecture will be based on these security models and will provide consistency and interoperability across all platforms and applications where needed. Given Treasury's role in managing Federal Finances and collecting taxes and debts, as well as its role in investigating, tracking and reporting terrorist funding, money laundering, and other financial crimes, it is imperative that data transmissions are secure and private. Without the structure to protect the systems on which information relies, Treasury's ability to carry out its mission will be severely impacted. Owing in no small part to the enterprise architecture effort, the Department is making genuine progress in assuring these objectives are realized.

Third, proactive interagency collaboration on IT security provides additional evidence of the institutionalization of Treasury's IT security. Let me provide a few examples:

- The Treasury Communications System, the Department's nationwide business enabling communications networking infrastructure, is the largest secure and encrypted network in the civilian federal government. It routinely handles over 900 gigabytes of data securely each day and was the model used to establish the initial secure networking capabilities (Customs and Border Protection and Secret Service) of the newly formed Department of Homeland Security. The cyber security protection mechanisms applied to the Treasury Communications System were significantly enhanced in FY 2002. Additionally, a "security in depth" posture was deployed that resulted in a ten fold strengthening of the cyber security countermeasures of these communications services. This centrally managed capability is correlated to the Department of Homeland Security Threat Warning Level system. Any increase in threat level above

yellow results in continuous (24 hours per day) staffing to immediately respond to cyber initiated attacks.

- The Department is one of four agencies (Treasury, Department of Defense, Department of Agriculture, and NASA) to be cross-certified with the Federal Public Key Infrastructure (PKI) Bridge. Therefore, Treasury is positioned to strengthen its secure communications processes in conjunction and in alignment with its development of a common infrastructure.
- Although the missions of the Treasury Bureaus may be diverse, each Bureau is faced with the same challenges of physical, logical and cyber security, the need to improve business processes, the goal to be more resource conscious and the requirement to implement e-government initiatives. The Department determined smart cards and related security technologies, including leveraging its Public Key Infrastructure (PKI) cross-certification with the Federal PKI Bridge and biometrics, would provide the means to authenticate employee identification; secure facilities, systems, and property; and simplify a number of internal business processes.

Treasury, among other selected agencies (e.g., Department of Defense, Transportation Security Administration), is currently deploying smart cards with these technologies enabled at a number of its bureaus, including Departmental Offices.

- As cited previously, the Office of the CIO established a computer security incident response capability to coordinate Treasury efforts with appropriate external Computer Emergency Response Teams and to collect agency-wide information and to disseminate relevant incident reports within Treasury. This security response capability is coordinated with a similar government-wide effort managed through the Federal CIO Council.
- Treasury was recently recognized by the National Communications System (NCS) for enabling a thousand fold increase in circuits designated with the Telecommunications Service Priority (TSP) capability, thereby enhancing its ability to ensure reliable telecommunications during emergency situations - including on September 11, 2001.

- The Treasury CIO is the chairperson for the e-Authentication Steering Committee, the crosscutting government group working to ensure secure financial transactions and communications across the federal government.
- The Financial Management Service bureau continues to provide and expand its robust, reliable, redundant and secure technology infrastructure that issues payments for Social Security Benefits, Tax Refunds, Office of Personnel Management (OPM) Salary, Veterans Administration (VA) Retirement, Railroad Retirement Benefits, and many other forms of payment to the taxpaying public (approximately 900 million payments valued at approximately $1.9 trillion with 99.999% reliability).
- The Department of the Treasury and the entire Finance and Banking Information Infrastructure Committee (FBIIC) have been galvanized and positioned to harness and channel divergent security activities for that entire sector's benefit. To ensure the privacy of any electronic communications associated with the

augmentation of the sector's security improvements, Treasury implemented, and National Security Agency (NSA) approved, secure communications infrastructure specifically designed to support the activities of the FBIIC.

With respect to financial management material weaknesses, Treasury is overseeing remediation at two bureaus: the Internal Revenue Service and the Financial Management Service. Weaknesses at the IRS deal with property management, revenue reporting and financial statement preparation. Weaknesses at the Financial Management Service involve consolidated financial statements and check reconciliation.

The three weaknesses tied to financial reporting for the IRS are not scheduled to be closed this year but are covered in the IRS' Federal Financial Management Improvement Act Remediation Plan that Treasury provides to the Office of Management and Budget on a quarterly basis. In order to address the property management weakness, IRS will acquire and install a fixed asset module to the Integrated Financial System (IFS) that will generate records and record

capital asset acquisition costs in the appropriate general ledger. In the interim, IRS is interfacing the Information Technology Asset Management System (ITAMS) with IFS.

In order to provide support data for the revenue collected for employment and excise taxes, IRS is developing the Custodial Accounting Project (CAP). CAP will be a single, integrated data repository of taxpayer account information, integrated with the general ledger and accessible for management analysis and reporting. IRS intends to correct the lack of accurate general ledger account balances related to financial statement preparation by developing, documenting, and implementing new policies and procedures for monthly reconciliation and developing other steps.

The Consolidated Financial Statement weakness for the Financial Management Service is expected to be carried into 2004. FMS has undertaken a series of steps to improve revenue and net cost reconciliation procedures through implementation of Treasury, Office of Management and Budget, and General Accounting Office task force recommendations for the consolidation process. In the area of check

reconciliation, FMS is undertaking reconciliation as far back as records are reasonably available to investigate the cause of the imbalance and develop and to implement procedures for monthly reconciliation.

In the Office of the CIO, our mission is to "Steward Treasury's information resources with integrity and professionalism." That imperative is what the Clinger-Cohen Act and other statutes require, and it's what our taxpayer-citizens expect. I remain committed to doing that, which requires developing a strong and dynamic IT security program, continuing to work to fulfill our statutory responsibilities in protecting sensitive and classified systems, leading the Bureaus in security policy and standards development, and raising IT security awareness across Treasury. Any weaknesses that threaten to impede our Department's ability to achieve its mission we have aggressively sought to identify, analyze, and aggressively remediate, and we will continue to do so.

Again, I am grateful to the subcommittee for demonstrating leadership in identifying IT security as an issue and for driving reform

across the Federal Government. Mr. Chairman, thank you for the opportunity to appear before you today. This concludes my formal remarks, and I would be happy to respond to any questions.

Mr. PUTNAM. I would like to recognize Bruce Morrison. Mr. Morrison assumed his duties as Acting Chief Information Officer in the Bureau of Information Resource Management in December 2002. Previously Mr. Morrison was Deputy Chief Information Officer for Operations in the Bureau of Information Resource Management. Mr. Morrison is a career senior Foreign Service officer. During his 26-year career, he has held a succession of information management positions, including serving as dean of the School for Applied Information Technology in the Foreign Service Institute. We look forward to your testimony. You are recognized for 5 minutes. Welcome to the subcommittee.

STATEMENT OF BRUCE MORRISON, ACTING CHIEF INFORMATION OFFICER, DEPARTMENT OF STATE

Mr. MORRISON. Thank you, Mr. Chairman, and Ranking Member Clay. I am honored to be here and appreciate the opportunity to discuss information security at the Department of State. While we are not where we would like to be in cyber security, I can report on the initial stages of improving our program.

We at the State Department have the highest level of support and attention from Secretary Powell and Under Secretary for Management Green. Secretary Powell considers information technology to be a strategic component in implementing U.S. foreign policy.

Let me summarize IT security at State. We have long had a strong perimeter defense, with technical, physical, and personnel controls, including an antivirus program, firewalls, intrusion detection, and incident reporting. However, we realize that a sound cyber security program is built upon a defense-in-depth strategy that includes management controls as well as technical and operational measures. What we have lacked in the past is a comprehensive management structure and a serious systems authorization program.

It is a new day at State, with the convergence of several events bringing a fresh approach and commitment to cyber security.

First, GISRA, and then, FISMA focused top management attention on cyber security. Second, we have new cyber security leadership at State. I stepped into the position of acting CIO 6 months ago. Additionally, there is a new Assistant Secretary for Diplomatic Security with whom we collaborate closely.

Finally, OMB very helpfully mandated that we authorize all systems by the fourth quarter of 2004.

Our new organization is giving birth to a new cyber security culture and is producing results. We have a new Office of Information Assurance headed by a senior officer reporting directly to me. This office handles IT security policy, program management, performance measures, risk management, and reporting. There is increased departmentwide cyber security focus, as all offices are now involved to some degree in cyber security through the plans of action and milestones process and awareness programs. As I mentioned, there is an excellent rapport and collaboration between the Chief Information Officer and the Bureau of Diplomatic Security on all aspects of cyber security. Similarly, a cooperative partnership exists with the Chief Financial Officer on Critical Infrastructure Protection and the information technology budget.

We have a senior-level multidisciplinary cyber security advisory group. There is a close working relationship with the Office of the Inspector General. In biweekly meetings with the Inspector General, we discuss a variety of cyber security issues, with FISMA requirements and systems authorization taking center stage.

State has recently established an E-government program board chaired by Under Secretary for Management Green to manage all IT funds. Information assurance experts now review every IT system budget request to assure that appropriate security considerations are budgeted and executed. Very significantly, we have developed a certification and authorization plan. It was submitted to OMB in March, fully funded in mid-April. We are on track with the plan, with 10 percent of our systems done, and a goal of 33 percent by August 2003, and 100 percent by August 2004.

We are taking specific steps to institutionalize cyber security management and practices, enhancing policies, developing a cyber security program management plan, integrating security into planning, and providing training. New systems are addressing security from the outset. Our future budget request will include security costs. Regular awareness sessions for all users, and mandatory training for security practitioners will assist in institutionalizing cyber security.

In summary, we are still at the early stages of creating a comprehensive cyber security program, but we have made great strides over the past few months. This progress contributed to our PMA scores going from red to yellow to green.

I appreciate the opportunity to talk before the committee.

Mr. PUTNAM. Thank you, Mr. Morrison. You timed it perfectly, too.

[The prepared statement of Mr. Morrison follows:]

Statement by
Bruce F. Morrison
Chief Information Officer, Acting
United States Department of State

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

Hearing on
Cyber Security: The Status of Information Security and the Effects of the Federal Information System Management Act (FISMA) at Federal Agencies

June 24, 2003

Good Morning Mr. Chairman and Members of the Committee. I am honored to be here and appreciate the opportunity to discuss with you the solid performance, recognized progress and renewed vigor during the past year in the area of information security at the Department of State. We take seriously the oversight role your Subcommittee provides in ensuring the integrity of cyber security in these challenging times.

Summary

While we are not yet where we would like to be in relation to cyber security, we are pleased to come before you to report on the initial stages of improving our program. Today we will highlight the measurable progress we have made so far.

Traditionally, the world of diplomacy is slow and deliberative by nature. However, in the area of Information Technology, that is not the case. Let me underscore that Secretary Powell considers Information Technology a strategic component in implementing U.S. foreign policy. Protecting our information assets and cyber security is paramount to his agenda. In concert with Under Secretary for Management Green, we have committed substantial resources to meet our challenges. We established an Information Assurance office now headed by a senior officer.

What began as a mandate under the Government Information Security Reform Act (GISRA) has since become a challenge that we now fully embrace. In line with the Federal Information Security Management Act (FISMA) requirements and in close consultation with OMB, we conducted an independent assessment of the Department of State's information security environment. We began by doing something that might sound simple, but which is a major challenge for all USG agencies in the ever-developing E-Government world: clearly defining requirements and objectives. We adhered to OMB's definition of what constitutes a general support system versus a major application versus an application, then we conducted a thorough inventory and analysis of all Department IT assets to categorize them and set priorities for analysis and possible remedial action. Of those, 154 are now categorized as major applications or general support systems.

We are making steady IT security progress through effective management, implementation, evaluation and remediation when necessary. To complement this effort, we meet regularly with the Department's Office of the Inspector General -and address

information security issues and potential problems. Equally critical, we have an enhanced cooperative arrangement with the Bureau of Diplomatic Security, which has delegated responsibilities for significant portions of our information security program. Together, the Assistant Secretary for Diplomatic Security and I have identified our mutually supportive roles and outlined our joint strategy to meet our own critical security enhancement imperatives and OMB's aggressive time schedule.

Measurable Progress

Our recent results in improving information security under FISMA are significant and measurable.

The flagship of our new cyber security efforts is the Systems Authorization Program, more commonly referred to as Certification and Accreditation or simply C&A. In agreement with OMB, our goal is to certify and accredit all existing and emerging systems by September 2004. We have recently embarked on this critical program element and have set monthly targets for authorizations. We plan to have 50 systems, one-third of the total, accredited by the end of FY 2003.

While complex and involved, the quarterly Corrective Action Plan process enables the Department to report on IT security performance indicators and remediation Plans of Action and Milestones (POA&Ms). We have submitted improved POA&Ms the last two quarters.

As you know, these two tools -- C&A and POA&Ms - are major contributors to the President's Management Agenda (PMA) e-Gov score assigned by OMB. I am pleased to report that, over the past three quarters we have moved from "red" to "yellow" to "green" in the progress category and our goal is to move through "yellow" to "green" for status by July 1, 2004.

I. State's Cyber Security Program

The Cyber Security Program at the Department of State is a strategic, layered approach to comprehensive risk management of our information and information assets. In compliance with FISMA, the Department had an independent assessment by the National Institute of Standards and Technology (NIST) review our cyber security program earlier this year and are melding their excellent recommendations into State's security action plans and practices.

Information Assurance has three pillars: - Confidentiality, Integrity and Availability. We recognize that there must be a balance between IT security and business efficiency. Therefore, our approach is based on two tenets:

- Risk must be assessed and reduced to an acceptable level, but cannot be completely -eliminated; and,
- The budget and business needs of the employees must be considered in making risk management decisions.

No single security protection methodology can resist all forms of attack. Using a layered risk management security strategy affords multiple levels of defense and protection -- operational, technical and managerial.

Turning to the operational side, we have made solid strides in operational security and considerable progress in the areas of IT Security Awareness, Training and Education. To heighten cyber security awareness, executive directors report on IT security progress in their quarterly POA&Ms submission to the CIO. According to their reports, approximately 60% of the Department's employees have participated in information security training and/or awareness.

We have maintained a strong perimeter defense by applying standard technical solutions - Firewalls, AntiVirus protection and Intrusion Detection Systems.

I cannot stress enough that cyber threats to the Department are increasing due to the rapid proliferation of technology and the related vulnerabilities created by heavy reliance on emerging technologies and information systems.

In response to the heightened probability of attacks from individuals and groups with malicious intent, including terrorism, State's Virus Incident Response Team (VIRT) has continued to improve technology, process and Department-wide awareness.

Since January of this year, our team has eradicated 155,393 malicious codes. Top viruses included Klez.H, Yaha, Bugbear, Sobig and Lirva. In our VIRT "Home Use Give Away" program, we distributed over 9,000 CDs both domestically and overseas.

The Department of State has played a leading role in the government-wide E-Authentication initiative. Not only will it provide physical access, but also it will be the platform for digital identity and signature. This is a critical element of our forward thinking security and authentication posture and is vital for the protection of our information technology enterprise. To date, approximately 13,000 employee records with photographs have been created while another 10,229 Smart ID Cards are printed and being prepared for distribution by Diplomatic Security. Of those, 2,363 Smart ID Cards with Public Key Infrastructure (PKI) certifications have been distributed to employees.

As part of a continuing effort to ensure the security of the Department's critical infrastructure, the Department deploys a layered defense-in-depth capability. The strategy includes a detect, react and respond approach that emphasizes the analytical capability inherent in the program. Components of this methodology include a 24x7 Network Monitoring Center, a Computer Incident Response Team (CIRT), State's first line of defense, and a Cyber Threat Analysis Cell (CTAC), State's cyber threats think tank.

The Intrusion Detection System (IDS) program enables monitoring and auditing of network and host information systems, thereby, detecting inappropriate, incorrect or anomalous activity. IDS sensors are monitored on a 24x7 basis to protect Department networks against outside penetration, compromise or misuse. Alerts are generated for each possible unauthorized access event. Most recently, the IDS program has been enhanced this fiscal year by the deployment of 298 sensors to the Classified Network at 105 posts.

The Computer Incident Response Team (CIRT) is the focal point for reporting computer security incidents on Department and foreign affairs agency networks. CIRT reports are created and disseminated to senior management as well as security and operations managers. As required, CIRT coordinates with other government agencies to ensure and support needs for criminal prosecution.

CIRT provides computer security incident reports for both internal and external use to be included in the Federal Computer Incident Response Center (FedCIRC). Most recently, on June 17, we signed a Memorandum of Understanding with FedCIRC to formalize our information sharing arrangement. CIRT also participates in the quarterly FedCIRC Partners meetings where federal incident response teams, law enforcement, private sector representatives, academia, and federal agencies responsible for securing the National Information Infrastructure exchange ideas and discuss technical issues.

For example, in the first eight months of FY 2003, the Department had a total of 720 events reported to the CIRT include 557 originating from externally from the Department. Of those 720, 708 of the reports were deemed unsuccessful attempts. The remaining twelve were elevated to "incidents," two were reported to the FedCIRC, as they were of particular interest to the global Federal IT community.

Let me highlight additional accomplishments of the CIRT. During FY 2003, CIRT successfully implemented the use of a hardware/software tool that greatly enhances their ability to analyze network security events. CIRT also provides daily cyber threat information to senior department management and submits a weekly activity report to senior management outlining attempted network intrusions and resolutions.

We are taking a proactive stand as the United States is confronted with increasingly sophisticated computer network attack and information operations capabilities from its adversaries. To address these issues, the Cyber Threat Analysis Cell (CTAC) provides overseas posts and Department management with indications, warnings, descriptions, and diagnoses of threats to the Department's critical cyber infrastructure.

Building out from this strong infrastructure, we have numerous IT programs underway that directly contribute to the security of our information assets. Most recently, we completed "OpenNet Plus," one of our largest IT projects that enables secure desktop access to the Internet to the Department's over 43,000 users. This project was significant from a security point of view in that we ensured all Department domains met basic password and configuration guidelines. In addition, the project routed all Internet access through a central firewall, thereby reducing the risk of having to put individual firewalls in over 300 locations.

Using a similar implementation approach, our Classified Connectivity Program (CCP) provides secure access to our Foreign Service officers and other agency colleagues in over 220 posts around the world. This project is on budget and on schedule for completion by September 30 of this year.

While State has constructed a robust technical defense and solid operational procedures, a number of mechanisms are underway to complement our cyber security program. We have undertaken an ambitious outreach effort.

Senior Agency Information Security Official (SAISO)

The formation, funding and staffing of the Office of Information Assurance is underway. Under the FISMA requirements, I am designating a Senior Agency Information Security Official (SAISO) who will report directly to me. Let me note that the term Chief Information Security Officer (CISO) is used interchangeably with SAISO.

Coordination with the Office of the Inspector General
The cooperation between my office and the Office of the Inspector General is very constructive. - We meet bi-weekly to discuss plans, programs and problems. The meetings over the past six months have revolved around IT systems inventory, systems authorization and FISMA compliance. The OIG has been and continues to be briefed at the various stages of the Systems Authorization Project. The OIG was thoroughly briefed at various stages of the Systems Authorization Plan development. Other presentations have included the CISO's (used interchangeably with SAISO) FISMA mid-term assessment and the POA&Ms process

Cyber Security Advisory Group
For this effort to accomplish its target, a bi-weekly meeting with senior representatives from Management, Management Policy, E-Diplomacy, Resource Management and Diplomatic Security is held. While the initial focus was on C&A, the scope of the session has been broadened to encompass discussions on the
Wide range of information security issues.

IA Forum
For the Cyber Security Program to be effective, everyone at the State Department needs to be involved. We initiated a monthly IA forum to brief Department system managers on Information Assurance plans, programs and processes. Not only has this improved overall awareness and contributed to the participation of agency components in complying with OMB reporting requirements, but also this has served to be a sounding board for potential issues on the horizon.

Internal Synergy
We realize for the Department to succeed, we must work collectively, across Bureau lines, to ensure that the Department's critical infrastructure is protected. We must leverage the full complement of talent available to us to guarantee the Department's critical infrastructure is protected. We have redesigned our processes to align them to E-Government requirements and to ensure that the Chief Financial Officer and the Chief Information Officer speak with one voice on IT security. OIG inspections, audits, and reviews verify that processes in place are performing as expected.

Our existing network monitoring, threat detection and response, cyber analysis, incident reporting and education and awareness suite of services insures strong synergy within the Department. For example, the Computer Incident Response Team (CIRT) must rely on the Bureau of Information Resource Management's (IRM) firewall team to have the capability to identify external threats. Together, they evaluate and block suspicious IP addresses that may

adversely affect the Department's networks. Similarly, the CIRT and Cyber Threat Analysis Center (CTAC) work hand-in-glove with IRM's Virus Incident Response Team to respond to malicious events and to maintain a high state of anti-virus readiness. The DS Training Center has developed a series of computer security training courses for all Information System Security Officers.

Formation of Cyber Security Specialists Corps

We appreciate your support in providing the resources for cyber security. With the increasing requirements for increased cyber security, we believe the role of Information System Security Practitioners is pivotal in supporting the Cyber Security process both here and abroad. As noted in the OIG's report, Information System Security Officers (ISSOs) overseas do not spend adequate time on ISSO functions; rather IT security duties are viewed as collateral.

To help resolve these issues, we are conducting a study on ways to create a corps of cyber security professionals. Regional bureau executive directors welcome the upcoming study. To further encourage sufficient security practitioners with the appropriate skill set, the Skills Incentive Pay for IT security credentials is being raised.

Meanwhile, the Department is working to enhance its field expertise through the Regional Computer Security Officer (RCSO) program. This program provides timely computer security support and "hands-on" assistance to posts worldwide. RSCO are Foreign Service security engineering officers responsible for ensuring that classified and unclassified networks are installed and maintained according to current Department and U.S. Government security regulations. They provide on-site computer security customer support, training, oversight, and revaluations of unclassified and classified networks.

II. Actions to Remedy the deficiencies reported in September 2002 GISRA report

In the interest of fully addressing the issues, the following paragraphs summarize deficiencies identified in OMB's May report to Congress and progress made by the Department in addressing these deficiencies.

1. Security funding.

Last year's report indicated that State's IT security funding amounted to approximately 22% of the IT budget.

This figure, more than double industry figures, is based on estimates. In FY 2003, the Office of Information Assurance (IA) has worked closely with the Office of Architecture and Planning's Capital Investment group to develop guidelines for IT security investments. Training has been provided to those filling out IT submissions and the Office of Information Assurance has reviewed all submissions.

Training, management and oversight of the IT Security aspect of IT Capital planning is underway and will be assessed. Furthermore, IA involvement with the newly formed e-Gov Board Advisory Committee and participation in the e-Gov Board Working Group will ensure that IT security considerations are an important factor - in IT investment decisions.

2. Number of systems reviewed.

Adhering to OMB's definitions, we have created a single inventory of the Department's IT systems.

In close consultation with the OIG, we expect the official inventory number to be 154 for this year's FISMA reporting. Let me caution that the actual number of systems and to which category they belong continues to change as detailed meetings are held with the bureaus in the pre-certification phase of systems authorization.

3. Material weaknesses.

A) In FY 2001, the IG identified a material weakness in the Department's lack of Certification and Accreditation of its information systems.

A C&A plan, with timetable, has been developed, and was presented to OMB in March 2003. Department funding was made available in April.

By the end of June 2003, we expect 18 systems to have undergone the process. Our goal is to authorize one third of major applications and general support systems by August 2003 and 100% by August 2004.

B) According to an IG survey questionnaire, only 15 percent of the Department's systems had security plans.

A requirement of the pre-certification phase is a current Systems Security Plan (SSP). We have developed a template for the SSP development. During the initial C&A cycle, this will help systems managers with SSPs as required as they undergo C&A.

C) The IG found a significant weakness in information security management at overseas missions. Specifically, the IG determined that the information systems security officers (ISSO) generally were not performing all the requisite duties of the position.

IT security work typically constitutes collateral duties of those designated as ISSOs. Many managers place more emphasis on other responsibilities. We believe awareness and training will solve this problem. To alleviate this, the Bureau of Diplomatic Security (DS) training center has developed a suite of role-based IT security courses with distinct audiences in mind such as the security practitioner, the IT professional, and most recently, the manager at all levels. Additionally, cyber security is being added to the Foreign Service Institute's summer training session for Administrative Officers.

D) The IG reported that State had made some progress in assessing information security at missions and bureaus as part of its implementation of OpenNet Plus, the Department's program to provide worldwide desktop Internet access to its employees. Missions must show that they comply with existing security standards prior to receiving Internet services from OpenNet Plus. As of September 3, 2002, 20 bureaus and 84 missions had met the requirements of independent verification and validation (IV&V) of their respective IT infrastructures indicating compliance with the Department's IT security configuration and have subsequently been connected to OpenNet Plus.

The OpenNet Plus project was completed in May 2003 with the connection of over 43,000 users at over 300 overseas posts and domestic offices.

E) Lack of information security performance measures to support strategic goals.

In August 2002, the CIO issued IT security performance measures to the executive directors of all bureaus based on OMB GISRA guidance. New performance measures will be issued when OMB releases FISMA guidance. In FY 2004, the CIO will reformulate and reissue general performance measures and will specifically target overseas missions as well as domestic bureaus.

F) Weaknesses in the critical infrastructure protection program that have not been addressed.

State has adopted an alternative to Project Matrix - the State Secure Infrastructure Management Systems (SSIMS). SSIMS is an efficient, cost effective alternative that meets State's information security and global access requirements. The Department's Critical Infrastructure (CIP) Governance Board has approved the SSIMS project plan and equipment for the pilot. Once tested and relational databases populated, SSIMS will be hosted on SIPRNET where the data can be used and shared at the secret level.

The Undersecretary for Management (M) in April 2002 reinvigorated the Critical Infrastructure Protection (CIP) Governance Board and appointed the Assistant Secretary for Resource Management as chairman. This Board consists of other Assistant Secretaries and Directors under the "M" family (Human Resources, Consular Affairs, Administration, Resource Management, Information Resource Management, Diplomatic Security and the Office of Overseas Building Operations as well as regional and functional bureaus.

The CIP Governance Board has aligned CIP remediation efforts with the Department's budget and planning process to achieve CIP objectives. The board has moved all Tier 1 and 2 CIP remediation priorities from "red" to "green" in just one year. This includes our top priority of establishing redundant communications capabilities at the Department's new alternate communications site. This effort was completed in less than a year and under budget.

The draft CIP plan was presented to the CIP Governance Board in April for review and bureau specific changes. The final plan will be presented to the Governance Board in August.

G. *Financial Systems Reporting*
The Department had its 2001 and 2002 financial statements audited by an independent auditor at the direction of the IG. This independent auditor cited a "material weakness" for the Department's information systems security for networks in domestic operations.

The auditor identified four areas to be addressed to resolve the weakness:

1) Certification and Accreditation
All new systems and applications are thoroughly vetted by the Bureau of Diplomatic Security for security and information assurance before installation and use.

The Department has initiated a comprehensive Systems Authorization Plan, encompassing Certification and Accreditation which subjects all general support systems and major applications to a consistent, standardized, measurable and repeatable systems authorization process, including a thorough review of access controls. This plan was recently presented to the President's Office of Management and Budget (OMB), and OMB advised the Department that from its initial review of this plan, it was pleased with the plan.

2) Penetration Testing
An ongoing, cyclical program of vulnerability assessments for all systems including penetration testing.

Both the general support systems and the major financial systems are categorized at NIST SP 800-37 Security Classification Level 3 which means they will be submitted to penetration testing during C&A.

3) Patch Management
Patches are installed on a real-time basis.

An effective Patch Management program is essential for both IT Security compliance with FISMA and the Department's controls over its financial systems as addressed by the independent auditor.

In January of this year, the CIO took over operation of the Department's Patch Management program from the Bureau of Diplomatic Security. As Department needs to expand and strengthen its patch management capability, we are embracing the use of FedCIRC' s Patch Authentication and Dissemination Capability (PADC) tool as the centerpiece of a new, more robust patch management program. Policy

is being developed, based upon NIST SP800-40, to support this strengthened program and the Office of Enterprise Network Management is planning the operational structure. While an earlier request for supplemental funding to support this initiative was unsuccessful, I intend to revisit this in the near future. Once in place, the improved patch management capability will significantly strengthen our defense-in-depth IT security posture by reducing the vulnerabilities presented by the implementation of defective software.

4) Remediation of Weaknesses

Management respond to and expeditiously corrects findings and weaknesses identified in vulnerability assessments and penetration tests.

As part of the penetration-testing program, rapid mitigation actions have been taken to address several issues in the past, and will continue to be available if appropriate and necessary in the future.

At the June 12, 2003 meeting of the Management Controls Steering Committee - the CIO, at the suggestion of the IG, presented a potential reportable condition on IT security. The Committee determined that there was considerable oversight from the Under Secretary for Management and the OMB on IT security and that one more layer of oversight would not be effective. The issue was tabled until the September meeting when the CIO will provide a status report.

The major financial application Regional Financial Management System (RFMS) has recently completed its certification phase of the C&A process. Five of six critical findings have been corrected and 55 of 60 other findings have been remediated. The application is now in final risk assessment and I expect to make an accreditation decision this month.

4. Systems Authorization

The IG reported on system certification and accreditations. During FY 2002, the Under Secretary for Management mandated the Department-wide implementation of the National Information Assurance Certification and Accreditation Process (NIACAP) in a timely and efficient manner. The Under Secretary approved the DS and IRM roadmap for implementing this plan.

The C&A program was initiated in mid-2003. The roadmap was completely revised and the C&A process is a blend of NIACAP and the emerging NIST guidance.

5. *Critical asset prioritization and protection methodologies. Overall, the IG found that the Department did not specifically comment on critical asset prioritization and protection methodologies.*

The CIP Board-has prioritized remediation of Tier 1 vulnerabilities based on the findings of the 2000 Vulnerability Assessment Report (VAR). The 2000 VAR identified and prioritized our CIP vulnerabilities, which are organized by tiers, Tier 1 being the most critical.

6. *Training*
   The IG did not specifically address the area of training employees in IT security. However, the Department reported that in FY 2002, approximately 2,800 employees had been identified as having significant security responsibilities and that all of them have received specialized training. State indicated that security "awareness" is required of all employees and that as of the close of the FY 2002 third quarter, 9,665 employees out of 31,975 agency employees, including contractors, had received specialized "awareness" briefings, including users of OpenNet Plus.

The Department's IT Security Training program has made specific progress in aligning security training with OMB mandates and establishing processes and procedures to enable necessary tracking of performance. IRM and DS are working closely to provide performance indicators and goals to be reported quarterly in the Corrective Action Plan and annually in the FISMA report to OMB.

State indicated that only some of all known security weaknesses are addressed by the Department's Plans of Action and Milestone (POA&M) reports. POA&Ms were not currently integrated as a complete and comprehensive, single-source for eliminating known and documented vulnerabilities for programs and systems within the Department.

State's POA&Ms process was immature at the time of the September 2002 GISRA report. In fact, in October 2002, only a simple Department-level POA&AM was submitted with the quarterly Corrective Action Report. Since then, the development of a data collection tool, a series of workshops and information messages has elicited the participation of over 90% of bureaus. These introduced bureau-level cyber security performance measures for security documentation, awareness and training, and system and program

assessments. All bureaus are aware of the performance measures and over 90% are participating. These system and program-level documents are monitored throughout the lifecycle and referenced in capital investment decisions.

7. *Agency integration of security and capital planning.*

Top Department of State management is committed to integrating security and capital planning. The Department is overhauling its Capital Planning and Investment Control process and has created a new board called the e-Gov Program Board, chaired by the Under Secretary for Management, aided by the CIO and CFO, to oversee IT investment. The Assistant Secretary-level e-Gov Board is supported by a Deputy Assistant Secretary-level Advisory board, which in turn is supported by a working group. IT security interests are well represented at all levels by the CIO, the SAISO and the Office of Information Assurance, respectively. This effort represents a new culture at State in the awareness of cyber security in decision-making at the most senior levels.

III. Progress

Since the 2002 GISRA submission, the Department has made significant changes to its Cyber Security Program that will provide the cornerstone for managing and enhancing a solid information assurance foundation. To recap,

- At the CIO's invitation, NIST conducted an independent programmatic review to aid in improving the Department's Cyber Security Program. Multiple recommendations were implemented immediately and those requiring longer-term remediation will be incorporated in the Department-level POA&Ms.
- 96% of bureaus are contributing to the quarterly Corrective Action Plan updates and providing system and program level POA&Ms.
- IRM developed a single, agreed-on inventory of Department systems
- Systems Authorization is underway and on schedule. In the first three months, 18 systems have been through the process. Site accreditation will begin in FY 2004.

- We are treating the first C&A cycle as a project although we fully understand that this is a cyclical, recurring activity. Due to the aggressive schedule imposed by OMB (to authorize all systems by the end of FY 2004) we have pooled resources from two bureaus to make one team, funded the project centrally and are providing individual, focused assistance to systems owners and systems managers. A key measure of success of the C&A project will be whether IT security is institutionalized at the end of the project.
- Throughout the first C&A cycle system, owners and system managers are being sensitized to IT security considerations. They are being provided assistance as required to complete security documentation, and concurrently, in an independent initiative, they are receiving training to ensure that appropriate certification and other security cost are part of their life-cycle budgets.
- New systems are addressing security from the outset and will undergo C&A so that they are authorized before being put into operation. Regular awareness sessions for all users, establishing a cyber security corps and mandatory training for the security practitioner will assist in institutionalizing cyber security throughout the Department.
- The patch management program is being revitalized.
- The OpenNet Plus project, in bringing desktop Internet access to all employees, has improved security at bureaus and overseas missions. OpenNet Plus finished under budget and on schedule. CCP is doing the same on the classified side.
- The suite of IT security training courses has been extended, including a course targeting senior management.

As a Department, I believe we have a solid beginning in place and recognize we have a long road to achieving performance based cyber security management. Realizing these challenges, Secretary Powell said it best when he said, "the success of U.S. diplomacy depends in no small measure on whether we exploit the promise of the technology revolution." With the effective management of cyber security, I am confident we will accomplish this.

Mr. PUTNAM. I want to read for you what I read to the first panel out of an article from the Federal Times, from an information security specialist in an anonymous social service agency. They state, "Someone at our parent department told OMB we would have it done in July. We can't get it done right by then, so we will throw together some documentation and make it look like we did."

That never happens in any of your departments. Does it?

Mr. FRAZIER. Of course it happens. Of course it happens. Notwithstanding the anonymity of the person who stated that, we know that people try to meet these artificial deadlines, and in the process, they—haste makes waste. And it happens.

Mr. PUTNAM. Anyone else wish to jump out there?

Mr. COBB. I think that it's not that they are necessarily preparing a fraudulent set of paperwork or that's necessarily occurring. Instead it's a question of thoroughness. Specifically, how thorough are the examinations, planning, testing, and the different elements of the security plans.

Mr. PUTNAM. Mr. Ladner.

Mr. LADNER. My view is that the process will continue to be compromised until there is a plan that not only addresses the objectives that are set out by the statutes which we have to comply with, but that we go the extra mile. And so what we are doing at Treasury is to certainly hit our numbers on CIA, certainly hit the other objectives, but ensure that we actually have a security governance process and plan in place.

Second, I think that the process will continue to be compromised if we view it in static terms instead of dynamic. What I mean by that, is that we need to be able to have real-time visibility into what's happening at, in our case, the bureau level so that we can see on an ongoing basis what the numbers are. And I think over time the data quality will improve, so that we reduce the probability of individuals being able to toss over the wall data and reports that are less than accurate.

Mr. PUTNAM. I'm told that it's been 3 years since agencies were told to complete their inventory of systems, and that has not yet been fully completed. Is that correct?

Mr. MORRISON. One of the first things that I did after taking over as CIO was to complete an inventory of systems using OMB and National Institute of Standards and Technology guidelines. So it is true that was only done at the State Department this year.

Mr. PUTNAM. So we've had 3 years of artificial deadlines. That's fairly dynamic, and it took 3 years to get there.

What about Treasury?

Mr. LADNER. Whether it's ensuring that we have a good security program or ensuring that, for example, Treasury is delivering services at low cost—at high service levels—to our bureaus from our large network, we need to make sure that we understand what infrastructure we have. And so we have directed the bureaus to participate in a Treasury-wide total cost of ownership review, which will enable us to know what we have and therefore be able to drive enterprise architecture and the ability to drive the security programs much more effectively. So we will have that probably within several months, by fall.

Mr. PUTNAM. We look forward to seeing it in the fall. But that will still be substantially beyond when it was to be completed. Correct?

Mr. LADNER. That's my understanding based on what I've learned in the last 3 months. That's correct.

Mr. PUTNAM. OK. What about Ag?

Mr. CHARBO. We are in the process as well of looking at what systems we have and where they are. We have 576 IT projects. Our focus right now is to consolidate those down to a more manageable level. Let's retire those that are legacy, let's retire them, move on, identify those under redevelopment, bring those into the planning and investment process so that security, as Mark discussed earlier, can be placed up front where it is more cost effective and easier to manage.

Mr. PUTNAM. Mr. Charbo, you came from FSA, so I am going to pick on you first. In the article the same unnamed person said, in expressing their frustration not having appropriate authority, "they have their own funding and don't report to us. When I call them and ask for this or that report, they just ignore me."

Is that something that you found in your role at FSA, that you had difficulty getting the different branches around the country to take your requests seriously?

Mr. CHARBO. From a security perspective, that is somewhat better managed at FSA within the Department. Most of that funding is being placed under the common computing environment budget which is a centralized budget for the service center agencies. So we have a better handle on how the security is being done in those agencies within the service center, FSA included.

Mr. PUTNAM. So that's not a problem at FSA. Is it a problem in other parts of the department?

Mr. CHARBO. I won't deny that at times it is difficult to get information out of agencies, yes. And when we experience that, my position is to go to the Deputy Secretary, the administrators, or directly to the Secretary if we need movement. And I've been getting that support when we do that.

Mr. PUTNAM. Anyone else wish to add to that or comment on that?

Mr. MORRISON. I think the State Department made a big step forward this year by organizing an E-government program board that now governs the entire IT budget. That was a very necessary step to carry out the act.

Mr. FRAZIER. Mr. Chair, at Commerce, one of the biggest battles that we've fought, but I think one of the battles that was absolutely essential, was to make certain that all of the individual agency CIOs reported to, at least for part of their management responsibility, to the Department's CIO. And so those individual bureau CIOs now have more authority to override some of the concerns, override even their program head if they disagree with him. So that is something that has, I think been absolutely critical to improving the process at Commerce where you have the individual CIOs reporting to a head CIO at the departmental level.

Mr. LADNER. In my first month at Treasury, we created with the Treasury Budget Office, a Technology Investment Review Board that reviews all IT investments across Treasury. And so I think

that, as bureaus understand both from a statutory standpoint as well as an end-user standpoint that we have to have security considerations integrated into the budget process, that increasingly that close collaborative relationship is being created.

Mr. PUTNAM. Mr. Cobb, you have heard Mr. Frazier's testimony expressing some concern about artificial deadlines or overly aggressive schedules that would cause people to potentially cut corners in their quest to get certified or accredited. NASA has worked rather hard to improve its performance and has made some progress. How did you ensure that the agency's desire to make that progress didn't lead to skimping on the work of correcting vulnerabilities?

Mr. COBB. Well, our audit strategy has been primarily aimed at looking at specific systems, and as I mentioned we've done 26 audits last year of specific systems. Some were agency-wide. And I took note of the biweekly meetings at State.

We don't have those biweekly meetings and we should have them; because, for example, we didn't see NASA's executive summary until a week before they submitted the GISRA report. So we were not on top of the reports of improvement of the NASA programs and NASA's assessments of its systems, by the time we filed our GISRA report. The way in which we are going to get after that is by assessing exactly how thorough NASA was in their systems analyses. In addition, we're going to continue to do our aggressive auditing of NASA systems to determine the thoroughness of their systems' analyses and we will try to verigy their results through sampling.

Mr. PUTNAM. You have heard the recurring theme that this is a management issue or a technology issue, it's not a money issue. Mr. Ladner, your IG stated that there is a general feeling that some bureaus, "appeared to view the GISRA annual reporting process as a pro forma exercise." In your GISRA report to OMB, 8 of the 10 current material weaknesses in IT security were repeats from 2001.

Mr. Morrison, your IG stated that the lack of security planning and missions is the result of, "insufficient guidance from the Department, and a general belief that IT information security is less important than other elements of security."

Mr. Charbo, your IG at USDA said, "'The Department did not have security plans in place for all its major applications and general support systems, had not planned for contingency, had not certified security controls in place and authorized processing for all of its systems. Nor had the Department identified all of its mission-essential infrastructure, conducted risk assessments, or prepared mitigation plans on the identified risks."

What are you all going to do to change the culture at your departments?

Mr. CHARBO. We have been doing this in a process where the first thing is discovery. We feel that we've identified the projects on the IT basis by doing a few things. One is we've lowered our waiver process of how departments and agencies within USDA can spend their dollars for IT so that we can identify where is the money going and what things are being done with this. We've also incorporated that into the investment process with OMB, the 300 business case analysis which now requires two key things for this.

One is project management skills. Even though we have a project identified, that does not mean it's going to get delivered on time, on budget, and meeting the requirements that the system was intended to do.

We now have a process in place that we believe will do that, and that is requiring a name, an accountable person with the skills to deliver that project on time on budget and with the requirements. Security is a major component. Given all the requirements in that document, if security is lacking, it will not go forward. We will not approve that investment moving forward. We have also made our senior executives accountable under a security grading process that we have within the chief information officers. We've started monthly meetings with administrators.

Typically what we do is we have to identify what have you spent on security rather than it being a definite budgeted line item for security. So we are talking more of a proactive than reactive, which, in a lot of the cases, the reports represent. It's just trying to find out what has been done rather than where we are going. We have identified where do we want to be in the next year. Within our office through July, we have identified, on a quarterly basis, where we want to be with security. We have done that with our e-government areas, our network management and several key areas within the IT area of the Department of Agriculture.

Mr. PUTNAM. Mr. Ladner and Mr. Morrison.

Mr. LADNER. At Treasury, I mentioned our focus on the capital planning process. We believe that is absolutely critical if we are going to get change across the Department. One of the actions we've taken in the last 3 months is to create, for the first time, an office of policy and planning that pulls together the IT government's enterprise architecture and our tracking of E-Government services so we can integrate security—not in a silo-like fashion—but truly across all of our functions and across the Department. Second, we have deployed a PKI, a public key infrastructure, and we are looking forward to having a framework with specific examples where we can move the ball forward in improving our security. And I think that where the bureaus see the CIO and the CIO leadership actively engaged in spending time on improving our security, I think that sends a very strong signal.

For example, last week the Bureau of Engraving and Printing affixed, for the first time in our Department, a digital signature to a form. We are actively trying to not only improve security but also essential PKI vehicles. I am very involved in that and I think that sends a very strong signal to the rest of the bureaus.

I would also add, in addition to what Scott said about accountability, that at the IRS where security has been an issue with regard to reports, they are working very hard with my office to address and to fix our exhibit 300's issue. And I think at the end of the day, we can't wave the flag on progress unless we have really made progress and that's the test of fixing the 300's. In addition, the IRS is holding their managers accountable for fixing their security issues on those 300's and I think that's a real sign. Getting to your question on the cultural dimension, we're in fact making progress on the cultural dimension—but there's a long way to go.

Mr. MORRISON. Mr. Chairman, Under Secretary Green is leading aggressively on the IT security issue. I'm engaged directly with the other assistant secretaries. I'm happy to say that in the last two quarters, we now have over 90 percent of the State Department bureaus engaged in the plans of action and milestone process. As my colleagues have mentioned, it's vitally important that security become an integral element of the budget process, which we achieved this spring. So in summary, it's a slow painful process, but we are making progress at changing the culture.

Mr. PUTNAM. Mr. Clay, you're recognized.

Mr. CLAY. Thank you, Mr. Chairman. Mr. Frazier, the Department of Commerce accounts for much of the improvement in the OMB table. The subcommittee's report card shows only modest improvement at the Department between 2001 and 2002. Can you explain the difference, and which do you believe is the more accurate reflection of the situation at the Department?

Mr. FRAZIER. I guess I could start with a quote from something my grandmother used to say to me: "You know, we are not where we should be and where we want to be, but thank God we're not where we used to be." So I think there is a mind-set in the Department that recognizes that we have made tremendous progress. But I have to tell you, we still have a long way to go. I don't want to speak for what GAO says or even what the Department CIO says, I'll just speak for what my systems evaluators have found. Every time they have gone into an area that has supposedly been certified and has been accredited, they have found problems that continue.

Here I will quote Ronald Reagan: "trust but verify." There is usually this mind-set that because somebody tells you something, it must be true, and that is not always the case. And I don't think there is any intent to deceive as much as it is as let's get this done and let's get that done. And as we go back and start to verify and see that there are still gaps, we have also been tremendously impressed with how responsive the Department has been to deal with our issues.

And so now you begin to see that they are saying before we send this forward, maybe we ought to go out and do some testing and do some validating. So I think that the explanation is that we still have a ways to go. We have made progress. But part of it is in the mind-set. I think the Chair has hit it a number of times on the head by saying that the management philosophy has changed. Take this seriously.

The Secretary is making sure that people are held accountable for this. One area that I remain concerned with is that I see that the managers, the CIOs have gotten the message. I still have concerns as to whether the folks on the front lines have gotten the message. I can't tell you how many times we have gone back to tell a CIO of a particular bureau who thinks this is one of their model systems. And I say let me show what we have found. And of course they become very disappointed. So there is still a great deal of work to be done but I have to tell you that significant progress has been made. Being one of the folks that has been around a little while and again when I was here 2 years ago, it was such a dismal

report. So I can take pride in saying that a lot has happened, but we still have a long way to go.

Mr. CLAY. Thank you for that response. Mr. Cobb, NASA accounts for most of the rest of the improvement in the table. The subcommittee's report card shows a decline in performance in that Department between 2001 and 2002. Can you explain that difference and which do you believe is the more accurate reflection of the situation at NASA?

Mr. COBB. Well, I think the variance in the views between the IG's and CIO's may be due to the differences in interpretating of the data. I think that's the same reason that you have a different story between how the subcommittee views the meaing of data and how OMB views the data.

My impression from what I have seen in the 1 year that I have been the NASA IG is that NASA is doing much better than when I came in. The reason is because the senior levels of management and the CIO's office, have acknowledged the fact that they have serious problems. They have had a number of management changes in the CIO's office. They have a lot of plans and programs that are underway. The verdict is out on whether or not they're going to effectively meet the challenges of IT security.

But certainly, in terms of the cultural change and what they have not done, is make the center CIO's report to the CIO's NASA has 10 or so centers that report to the center directors. The CIO doesn't write their evaluation. I think NASA is doing much better. They're focusing on the problems and we keep beating the drum right behind them.

Mr. CLAY. How are the front line workers implementing these applications and systems?

Mr. COBB. NASA has a very large number of systems and related systems' NASA reports. But there may be systems and applications of systems that information managers don't even know about. The scientific community, in terms of the front lines, are very mission-oriented, and I don't think that they view their mission is IT security. I think their mission is doing incredible scientific endeavors. And I would absolutely agree that the biggest challenge that any CIO has is how to get the entire organization inculcated with a concept that IT security is a primary responsibility rather than a secondary responsibility.

Mr. CLAY. Thank you.

Mr. Morrison, the State Department was one of the agencies whose grade went down from 2001 to 2002. Can you explain that decline?

Mr. MORRISON. I wasn't the Chief Information Officer at that time, but I was there. I think that OMB summed it up very well that the Department lost its focus on IT security and allowed itself to concentrate more on other matters. We certainly don't dispute the findings of the OIG or the judgments of GAO or OMB.

Mr. CLAY. Mr. Charbo and Ladner, both of your agencies received failing grades in both 2001 and 2002. Can you explain why your agencies have not adequately addressed computer security over this period? Start with you, Mr. Ladner.

Mr. LADNER. Like Mr. Morrison, I am fairly new, about 3 months, so my understanding from what my briefings have been is

that the structures and processes and systems simply weren't in place to facilitate an enterprise-wide view of security, which is absolutely critical. And so, for example, at the IRS, where a number of the security issues have been, what the IRS has done is to transition more from a facilities based approach to an enterprise wide based approach.

So this is something that now we are pushing both now on a Treasury-wide basis as well as at the bureau level.

Mr. CLAY. Mr. Charbo.

Mr. CHARBO. I guess just this one time we won't say much about consistency in the grades. From my perspective, I am not looking back at those. We are very focused on where we want to go. Using the FISMA report, we have identified over 1,400 tasks that we need to do to correct the 243 weaknesses that we have, rather than just, on a quarterly basis or an annual basis, coming back and trying to say OK, where are we now? We are taking ownership of those to reduce those. We have identified folks in every agency within the Department of who owns responsibility within those systems to correct it. And our vision is to reduce those numbers in half on the next mark if we can, identify the funds that we need in order to do that and move forward with those.

Mr. CLAY. And that process is occurring now.

Mr. CHARBO. That process is occurring right now.

Mr. CLAY. Thank you very much for all of your answers. I appreciate it.

Mr. PUTNAM. Thank you, Mr. Clay. This panel has made several references to personal drive affecting their departments, the leadership, the priority, the sense of urgency that you have brought as fresh leadership in this area. My concern is that we have not institutionalized this as a priority in the departments, and that a year from now, when we have someone else sitting here, they say I have only been on the job 3 months or 6 months. I wasn't here for the last FISMA or GISRA report. And I know different ones of you have alluded to this, but what are the last institutional changes that you are deploying that will guarantee that regardless of who occupies your position, these information security measures will become a part of the culture all the way down to the front line level?

Mr. Frazier, do you want to jump out there?

Mr. FRAZIER. It is an interesting observation. You remember when you started earlier this morning, you read the quote from The Federal Times, and you were talking about documentation and someone had said that we don't think documentation is that important, we can either document something or we can get the work done. Well, here's where I disagree with that: That statement is absolutely wrong. Because when you document something, you leave a record so that it doesn't matter whether I am sitting as the CIO today and John Doe is sitting there next week. You have a base line. When something hasn't been documented, we haven't put it down.

Every time a new CIO comes in, they are starting from scratch, so we don't make the kinds of progress that we should be building upon. Every time a new CIO comes in, there is a new plan that says let's really get this under control. And this is difficult work. One of my staff gave me a cartoon that said IT security is like a

stubborn mule. You know, making progress with it is something that's very difficult but you shouldn't have to reinvent the wheel every time. So it's the documenting it so that you begin to institutionalize the process, so there's a frame of reference that we know where we were and all of us can talk on the same page, if you will.

I think that's one of the important steps that should be taken. So I go back to that and I think that is indicative of the kinds of things that have to happen.

Mr. PUTNAM. What about the attitudes of people you have to work with who think it is an either/or tradeoff?

Mr. FRAZIER. We were lucky. I'll tell you that about 2 years ago when I came up to testify, we were highly critical of the Department. The new Deputy Secretary had just been on the job for less than 3 days and he was dragged before the committee to respond to Bob Dacey's report and my report, and I mean, they just ripped him apart. In the process, he left that meeting, called me into his office, and said, "What do we need to do to get this turned around?" So we have had the kind of cooperation that has made a tremendous difference, and it's because I think that he saw how serious the Congress was about this issue in that it wasn't something that was going to go away.

And in the process he has instilled in his managers—we do some incredible work at Commerce, but people have to understand if you don't have systems and things that are secure, you put all of those programs at risk in the process. That message is out there, and it's out there and making a difference.

Mr. PUTNAM. We are going to make sure that message gets to the FAA who made the comment. Anyone else?

Mr. MORRISON. I think that the FISMA Act itself, as well as OMB's Presidential management agenda process has gone a long ways toward institutionalizing IT security. It certainly has focused top management attention on this matter. We've made fundamental changes in our budget process and frankly, there's nothing like having to report every quarter, or in my case, I have to report to the Under Secretary for management, both in writing and orally every month. And there's nothing like having to report frequently and regularly to focus your attention on correcting problems. And I think that this framework that's provided by the act and by OMB is not going to go away, if I go away.

Mr. LADNER. The reason that change is enduring is that there are structures, processes and systems in place that are hard to change, and that's why our first step was IT governance. So I think that if we want people on the front lines to believe that their actions, or lack thereof, have an impact, we have to tie resource allocation to performance. And that's what IT governance and security governance ensures.

Clearly there's a long way to go on this front, but our goal at the Treasury Department is to articulate a framework which we have, and then pick out instances where we are showing that the lack of performance results in resource reallocation. And that's the kind of change that we believe will be more enduring.

Mr. CHARBO. If I could point out a few of the firsts that we have done that will carry on, regardless of who sits in the Chair that I sit in right now. We have released some governance policy around

security. It's quite a load to the agencies. However, we are putting people in place and contracts in place to help support them in correcting their security needs. We've also started a configuration management and policy board to manage the configurations across the Department. We are testing our business systems, the ability to recover. We're doing that at FSA, at NRCS, Rural Development, the National Finance Center.

First time now we are consistently testing these on a timed basis, so it's not just once when somebody asks whether or not we're doing it, but it's on a regular cycle now that we're testing those, and that's more and more systems that we're doing it as well. We have also initiated a department-wide process to identify what the plans are. Where one system is dependent on another, if that system goes down, others may go down. We're interested in those threats.

So we have initiated some process to connect those dots, identify the trees that we need to initiate in the event of a crisis. We have also changed our investment board around so now that security is a key component in all of the investments within USDA. The CIO owns those projects, positioning those projects within that investment board. On April 1, we released our first enterprise architecture vision of where we would like to see the investments move in the Department of Agriculture as well.

And last, we're training folks in project management. We've initiated a number of classes. Those classes are done in various locations throughout the country to provide us the quality folks that we need to deliver on some of these things. I believe those will continue, whether or not I'm in the chair that I currently sit in.

Mr. PUTNAM. Mr. Cobb, do you have anything to add?

Mr. COBB. I would agree with that. I think that FISMA is providing our IG office with the tools to get after the agency in terms of making sure that their programs are compliant with what you would expect from a robust IT security system. One concern I have about the structure of GISRA and FISMA is the extent to which the act requires independent evaluations of the system as a whole. Also, whether the system, from an umbrella standpoint, is actually accomplishing the objective of protecting information.

I would like to have my office work toward conducting a review of the policies to see whether or not they are substantively working. And the other big point that gets back to that front line is that it is critical to inculcate all Federal employees on the importance of IT security. There may be an avenue for legislating training requirements to make sure that this message is communicated. However, I'll leave that to speculation at this point.

Mr. PUTNAM. We look forward to hearing your conclusion when you reach it, and we'll let that be the final word for the second panel. You know, it seems that the Federal Government never really learned its lesson on physical security or perimeter security and enforced protection until after Beirut, and Oklahoma City and Khobar Towers and the *U.S.S. Cole,* and we never really learned our lessons on aviation security until after September 11. And it seems terribly frustrating that what it would appear is that it will take a digital September 11 or digital Pearl Harbor or some catastrophic cyber attack for people to get the message that this is im-

portant, that this is a priority, not just in some egghead CIO's office, but all the way down to the front line as part of their daily responsibilities.

And I think that is the part that is incredibly frustrating. We hear an awful lot of connecting the dots and learning from the mistakes of the past. As it relates to cyber threats, there is very little indication that anyone takes the threat seriously. I want to thank our witnesses for their contribution to our efforts in understanding this issue better, and I look forward to your continuing cooperation as we move toward greater coordination and more progress in improving our Federal Government's information security. I also want to thank Mrs. Miller, Ms. Watson and Mr. Clay for their participation and leadership on the subcommittee.

In the event that there may be additional questions that we did not get to today, the record will remain open for 2 weeks for submitted questions and answers. Thank you all very much and the subcommittee stands adjourned.

[Whereupon, at 12:25 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

Our Failing Computer Networks Cry Out for Technological Redress

by David M. David*

As Chief Science Officer of DMD Technologies I have observed industry and our Government attempt to solve the problem by continuing to apply network patches and upgrades to an archaic and obsolete architectural infrastructure--an architecture that was never intended to be utilized in the manner that it has, given the advent of the internet as we now know it materialized.

The Need for Network Overhaul

Research to develop the first super computer networks was initiated some 40 years ago, in 1960. The first commercial firewall in the form of Digital Equipment Corporation's SEAL product, achieved security in networking since entity ran an independent network.

The open source networks benefited from Hyper Text Transfer Protocol, which constituted a practical launch into the public arena. Today, these "backbone" networks are a landscape akin to the Wild West where lawlessness prevails in a wide-open panorama fostered by anonymity.

Network Flaws Tolerated

By the time technologists first realized the deficiencies of "open source" networking, it was too late to restructure our networking architecture. Moreover, the cost of major restructuring far outweighed the risks involved. During the 90's, hacking and theft were problems of everyday networking, but for the most part these incursions had little effect upon industry, government or the average citizen.

By 1999, however, things had changed. The estimated cost of attacks of all kinds on the network was $12.1 billion, and growing. The *Boston Herald* reported on July 10, 2000, that the estimated loss from hacking, viruses and criminal penetration of commercial networks was estimated to exceed $1.5 trillion. One notorious attack that year, the "I LOVE YOU" virus, affected an estimated 45 million computer files at a cost to companies of $2.61 billion, as reported by *Reuters* on August 7, 2001. These figures demonstrate an exponential rise in incidents and their costs.

Widespread Reluctance to Undertake Technological Change

These damaging events continue. Why are they tolerated? Many computer security and anti-virus companies began to see a windfall of revenues based upon the insufficiencies of our global information grid architecture. But despite their best efforts the situation continues to remain unchecked.

The RED CODE virus hit the network in 2001, shutting down 341,015 servers globally, at costs above $2.62 billion as of Jan 14, 2002, according to *Wired Magazine*. Code Red and its subsequent spawn represent the very first AI, or Artificial Intelligence-based attacks. Few acknowledged the serious, terrorist-like consequences of this event, one that was predicated on finding the hole in the network security blanket through which to initiate the attack. Even CERT, the government-funded "Computer Emergency Response Team", and one of the internet's leading

network security sites, was sporadically unavailable for three consecutive days due to a distributed denial-of-service attack

Difficulty in Implementing Technological Change to Network Security

We need to grow our security capabilities along with our technological capacities and user demands. Cyberspace should not be a fantasy playground for malicious mischief.

As far back as 1997, my company demonstrated the first media delivery broadcast system to a senior official of a major recording company. The reaction: "No credit card company will ever allow transactions to occur on the Internet. It's just a fad. [For example], why would people listen to music on the internet when they have a perfectly good FM radio?"

Once corporations, financial institutions and government began utilizing the Global Information Grid to conduct business, the virtual reality of cyberspace suddenly became a serious national asset. But it must be protected.

We do have a choice: knowing that we remain vulnerable, we can either continue to stumble forward, blindly pretending that we are safe while nefarious interests plan a time and place for an attack of their own choosing, or we can shake off complacency and take bold action to protect ourselves.

Trillions of dollars in commerce are conducted annually on internet networks. Each year hundreds of billions of dollars are lost due to hacking and crime enabled by our obsolete infrastructure. In the past two years alone, government and industry have spent hundreds of millions of dollars on patches that do not work. We are more vulnerable today than we were a decade ago in terms of proportionate usage growth and vulnerability. There is no easy fix. And the best minds in government, academia and industry have not been able to implement a viable solution to the problem.

Government is slow to respond. The President, Congress or the Senate, along with advisers from outside of government, have relied upon patches to an archaic infrastructure and legacy technologies to find a solution. It is our Declaration of Independence that states the immutable truth: "Mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed."

In the 15 years since November 2, 1988, when the first hacker attack occurred, annual losses due to cybercrime have increased exponentially, and will exceed the national debt within this decade. Networking technology may be in its infancy, as are the means by which these attacks occur. *But with every hostile event, we see how attacks are evolving scientifically at a rate faster than the technology that it targets.* Nor is the assault on fundamental rights and freedoms something to be taken gently: universities have closed their doors, pertinent information is increasingly difficult to find; and pornographers, spammers, thieves, and terrorists have in may ways hijacked or pirated the global information grid.

In place of the green fields of human evolution and knowledge, we now find a scarred, barren landscape of trenches and barbed wire, defenses against an elusive enemy that remains unseen and unidentifiable. Law abiding citizens possess no really effective defenses. Our children receive pornography in their mailboxes; new viruses threaten us constantly; and our daily dose of spam is close to four times the number of our welcome emails.

There are, of course, legitimate concerns regarding privacy and freedom of information. But a free society has never survived terror and lawlessness. Accordingly, we cannot throw away

the construct of freedom itself in order to maintain a battlefield of anonymity in which criminals are able to flourish.

What Is to Be Done

We are a society that has never shrunk from investing in finding technology driven solutions to crises; the collapse of the former Soviet Union in the face of overwhelming US commitment to weapon modernization offers, perhaps, the most contemporary and dramatic anecdotal evidence of this spirit.

Yet, at the moment, even the events of 9-11, and the imminent threats still awaiting us, do not remove the complacency that keeps us in a state of denial, continually attempting to fix the unfixable. We remain unwilling to explore truly innovative approaches to the defense of our critically important information grid in a way that is contrary to both reason and tradition.

Despite the structural reforms, evidenced best, perhaps, by the creation of the Department of Homeland Security (DHS), parochial spasms of self-interest dominate reform attempts: bureaucrats and their unions bicker over even the most marginal adjustments to their workplace environments; the 22 agencies integrated into DHS are joined more in combat than in cooperation over jurisdictional interests that hobble the development of a cohesive homeland security strategy; state and local level first responders lack a role in a desperately needed national emergency communications net as law enforcement and national-level intelligence sources protect rather than share information; and we struggle to protect an enfeebled and increasingly vulnerable system of legacy information networks that serve only the short term economic interests of their managers and providers.

Happily, technology capabilities exist today that provide a scientific solution to this problem. This solution is not another patch; it is not new software or a new firewall. It is a solution comprising an entirely new, comprehensive architecture designed from the ground up and based upon the predicates of information assurance and security.

We have the technology that offers a new foundation for the protection of data networks and data archives from intrusion, theft and malicious attack. These technologies, once integrated, can form an impenetrable data network system with the following capabilities:

- Monitoring global network conditions and traffic in real-time
- Dynamically changeable random addressing
- Dynamically changeable random encryption
- Deployment that is transparent to existing architecture
- Deployment that is transparent to hackers, terrorists and users
- Eliminating 90% of collateral damage from viruses
- Eliminating 90% of damage from hacker or terrorist attacks
- Covert onion-skins to trace routes that identify exact location of attacker(s)
- Absorbing DOS attacks as they occur, prior to penetration of target
- Absorbing any size attack
- Stop AI viruses like Red Code and Nimda
- Instruction sets instantly updateable worldwide
- Instant reports and responses to new threats

This type of "Cyber Shield" infrastructure enables expanded intelligence gathering and law enforcement capacities currently unattainable.

All of these capabilities are patent protected. Many scientists who are currently working with them include founders of the internet, presidential technology advisors, and even top scientific advisors in many high-level federal government positions. Most believe that this solution is the only viable action that will permanently stop network abuse. Yet the motivation to act is crippled by the reluctance to embark on innovations that threaten entrenched interests in government, industry and even in Congress.

This technology is robust, redundant and certain. Further, it provides a platform upon which future technologies, solutions and defenses can be built. We should learn from those who practice the dark art of network corruption that all science has a half-life—intruders have used advances in science to overcome network defenses that employ modest modifications to a collapsing legacy network system.

* David M. David manages DMD Technologies in Los Angeles with offices in Atlanta, Salt Lake City and Washington, D.C. The company is a leader in financial network security thinking.