AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ONCE MORE INTO THE DATA BREACH: THE SECURITY OF PERSONAL INFORMATION AT FEDERAL AGENCIES

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 8, 2006

Serial No. 109–159

Printed for the use of the Committee on Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

28–759 PDF WASHINGTON : 2006

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

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

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

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

BERNARD SANDERS, Vermont (Independent)

DAVID MARIN, *Staff Director*
LAWRENCE HALLORAN, *Deputy Staff Director*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

CONTENTS

	Page
Hearing held on June 8, 2006	1
Statement of:	
Johnson, Clay, III, Deputy Director for Management, Office of Management and Budget; R. James Nicholson, Secretary, Department of Veterans Affairs, accompanied by Tim McClain, General Counsel, Department of Veterans Affairs, and Robert Howard, Senior Adviser to the Deputy Secretary and Supervisor, Office of Information and Technology, Department of Veterans Affairs; David M. Walker, Comptroller General, Government Accountability Office; William E. Gray, Deputy Commissioner for Systems, Social Security Administration; and Daniel Galik, Chief Mission Assurance and Security Services, Internal Revenue Service, Department of Treasury	13
Galik, Daniel	69
Gray, William E.	59
Johnson, Clay, III	13
Nicholson, R. James	18
Walker, David M.	31
Letters, statements, etc., submitted for the record by:	
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	102
Cummings, Hon. Elijah E., a Representative in Congress from the State of Maryland, prepared statement of	100
Davis, Chairman Tom, a Representative in Congress from the State of Virginia, prepared statement of	4
Dent, Hon. Charles W., a Representative in Congress from the State of Pennsylvania, prepared statement of	96
Galik, Daniel, Chief Mission Assurance and Security Services, Internal Revenue Service, Department of Treasury, prepared statement of	71
Gray, William E., Deputy Commissioner for Systems, Social Security Administration, prepared statement of	61
Johnson, Clay, III, Deputy Director for Management, Office of Management and Budget, prepared statement of	15
Nicholson, R. James, Secretary, Department of Veterans Affairs, prepared statement of	22
Schmidt, Hon. Jean, a Representative in Congress from the State of Ohio, prepared statement of	98
Walker, David M., Comptroller General, Government Accountability Office, prepared statement of	33
Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of	8

ONCE MORE INTO THE DATA BREACH: THE SECURITY OF PERSONAL INFORMATION AT FEDERAL AGENCIES

THURSDAY, JUNE 8, 2006

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

The committee met, pursuant to notice, at 10:41 a.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis (chairman of the committee) presiding.

Present: Representatives Tom Davis, Shays, Mica, Gutknecht, Souder, LaTourette, Platts, Marchant, Dent, Schmidt, Waxman, Sanders, Cummings, Kucinich, Clay, Van Hollen, and Norton.

Staff present: David Marin, staff director; Ellen Brown, legislative director and senior policy counsel; Chas Phillips, policy counsel; Rob White, communications director; Andrea LeBlanc, deputy director of communications; Victoria Proctor, senior professional staff member; Teresa Austin, chief clerk; Sarah D'Orsie, deputy clerk; Kristin Amerling, minority general counsel; Adam Bordes and Anna Laitin, minority professional staff members; Earley Green, minority chief clerk; and Jean Gosa, minority assistant clerk.

Chairman TOM DAVIS. The committee will come to order.

Secure information is the lifeblood of effective government policy and management, yet Federal agencies continue to hemorrhage vital data. Recent losses of critical electronic records compel us to ask: What is being done to protect the sensitive digital identities of millions of Americans, and how can we limit the damage when personal data does go astray? In early May, a Veterans Affairs employee reported the theft of computer equipment from his home, equipment that stored more than 26 million records containing personal information. While he was authorized to access those records, he was not part of any formal telework program.

VA leadership delayed acting on the report for almost 2 weeks, while millions were at risk of serious harm from identity theft. And since admitting to the largest data loss by a Federal agency to date, the VA has been struggling to determine the exact extent of the breach. Just yesterday we learned the lost data includes information on over 2 million active duty and Reserve personnel as well as veterans. So the security of those currently serving in the military may have been compromised, and the bond of trust owed to those who served has been broken. And that is just only the latest in a long string of personal information breaches in the public and

private sectors, including financial institutions, data brokerage companies and academic institutions. Just recently, a laptop computer containing information on nearly 300 Internal Revenue Service employees and job applicants, including data such as fingerprints, names, Social Security numbers and dates of birth, was lost while in transit on an airline flight, according to reports. These breaches illustrate how far we have to go to reach the goal of strong uniform government-wide information security policies and procedures.

On this committee, we have been focused on government-wide information management and security for a long time. The Privacy Act and E-Government Act of 2002 outline the parameters for the protection of personal information. These incidents highlight the importance of establishing and following security standards for safeguarding personal information. They also highlight the need for proactive security breach notification requirements for organizations, including Federal agencies that deal with sensitive personal information. I know other committees have been working on the requirements for the private sector. Federal agencies present unique requirements and challenges, and it is my hope that we can work to strengthen personal data protections through regulatory changes and any needed legislative fixes.

The Federal Information Security Management Act of 2002 [FISMA], requires Federal agencies to provide protections for agency data and information systems to ensure their integrity, confidentiality and availability. FISMA requires each agency to create a comprehensive risk-based approach to agency-wide information security management. It is intended in part to make security management an integral part of everyday operations. Some complain that FISMA is a little more than a paperwork exercise, an analog answer to a digital problem. This latest incident disproves that complaint. FISMA requires agencies to notify agency inspectors general and law enforcement among others when a breach occurs, promptly. It appears VA didn't comply with that requirement. Each year, the committee releases scorecards based on information provided by chief information officers and inspectors general in their FISMA reports. This year, the scores for many departments remained unacceptably low or dropped precipitously. The Veterans Affairs Department earned an F the second consecutive year and the fourth time in the last 5 years the department received a failing grade. The Federal Government overall received a whopping D-plus, although several agencies improved their information security or maintained a consistently high level of security from previous years, including the Social Security Administration.

Today the committee wants to discuss how we can improve the security of personal information held or controlled by Federal agencies. In my view, these efforts should include strengthening FISMA and adding penalties, incentives, or proactive notification requirements. OMB will discuss government-wide efforts to improve data security. GAO will highlight areas in which the protection of consumer information can be enhanced. In this context, we will focus on security at the Veterans Affairs, Social Security Administration and the IRS. VA Secretary Nicholson will discuss the details of that department's potentially catastrophic data breach. Officials

from the IRS and Social Security Administration will describe the experiences and efforts of those agencies which stand as guardians of the largest storehouses of taxpayer information. Government information systems hold personal information about millions of citizens, including health records, military service histories, tax returns and retirement accounts. E-commerce, information sharing, online tax filing are commonplace. If the Federal Government is going to be a trusted traveler on the information super highway, critical data on millions of citizens should not be able to go missing after a trip around the Beltway in a back seat of some government worker's car. And that is kind of where we are.

So we appreciate everybody being here.

Secretary Nicholson, you are new to the VA, and I know this has come up, and you are trying to deal with it. We appreciate your being here today and sharing your thoughts.

Mr. Waxman.

[The prepared statement of Chairman Tom Davis follows:]

Statement of Chairman Tom Davis
Government Reform Committee Hearing,
"Once More Into the Data Breach:
The Security of Personal Information at Federal Agencies"
June 8, 2006

Secure information is the lifeblood of effective government policy and management, yet federal agencies continue to hemorrhage vital data. Recent losses of critical electronic records compel us to ask: What is being done to protect the sensitive digital identities of millions of Americans, and how can we limit the damage when personal data does go astray?

In early May, a Department of Veterans Affairs employee reported the theft of computer equipment from his home, equipment that stored more than 26 million records containing personal information. While he was authorized to access those records, he was not part of any formal telework program.

VA leadership delayed acting on the report for almost two weeks, while millions were at risk of serious harm from identity theft. And since admitting to the largest data loss by a federal agency to date, the VA has been struggling to determine the exact extent of the breach. Just yesterday, we learned the lost data includes information on over 2 million active duty and reserve personnel, as well as veterans. So the security of those currently serving in the military may have been compromised, and the bond of trust owed to those who served has been broken.

And that is only the latest in a long string of personal information breaches in the public and private sectors, including financial institutions, data brokerage companies, and academic institutions. Just recently, a laptop computer containing information on nearly 300 Internal Revenue Service employees and job applicants – including data such as fingerprints, names, Social Security numbers, and dates of birth – was lost while in transit on an airline flight, according to reports.

These breaches illustrate how far we have to go to reach the goal of strong, uniform, government-wide information security policies and procedures.

On this Committee, we've been focused on government-wide information management and security for a long time. The Privacy Act and the E-Government Act of 2002 outline the parameters for the protection of personal information. These incidents highlight the importance of establishing – and following -- security standards for safeguarding personal information. They also highlight the need for pro-active security breach notification requirements for organizations -- including federal agencies -- that deal with sensitive personal information.

I know other Committees have been working on requirements for the private sector. Federal agencies present unique requirements and challenges, and it is my hope

that we can work to strengthen personal data protections through regulatory changes, and any needed legislative fixes.

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to provide protections for agency data and information systems to assure their integrity, confidentiality, and availability. FISMA requires each agency to create a comprehensive risk-based approach to agency-wide information security management. It is intended, in part, to make security management an integral part of everyday operations.

Some complain that FISMA is little more than a paperwork exercise, an analog answer to a digital problem. This latest incident disproves that complaint. FISMA requires agencies to notify agency Inspectors General and law enforcement, among others, when a breach occurs. It appears VA has not complied with that requirement.

Each year, the Committee releases scorecards based on the information provided by Chief Information Officers and Inspectors General in their FISMA reports. This year the scores for many departments remained unacceptably low or dropped precipitously.

The Veterans Affairs Department earned an F, the second consecutive year and fourth time in the past five years the department receiving a failing grade. The federal government overall received a D+, although several agencies improved their information security or maintained a consistently high level of security from previous years, including the Social Security Administration.

Today, the Committee wants to discuss how we can improve the security of personal information held or controlled by federal agencies. In my view, these efforts should include strengthening FISMA, and adding penalties, incentives, or pro-active notification requirements.

The Office of Management and Budget will discuss government-wide efforts to improve data security. GAO will highlight areas in which the protection of consumer information can be enhanced. In this context, we'll focus on security at Veterans Affairs, the Social Security Administration, and the IRS. VA Secretary Nicholson will discuss the details of that department's potentially catastrophic data breach. Officials from the IRS and the Social Security Administration will describe the experiences and efforts of those agencies, which stand as guardians of the largest storehouses of taxpayer information.

Government information systems hold personal information about millions of citizens, including health records, military service histories, tax returns, and retirement accounts. E-commerce, information sharing, on-line tax filing, are commonplace. If the federal government is going to be a trusted traveler on the information superhighway, critical data on millions of citizens should not be able to go missing after a trip on the Beltway in the back seat of a federal employee's car.

Mr. WAXMAN. Thank you, Mr. Chairman.

I'm pleased you are holding this hearing on Federal data security. Last month, the sensitive data on 26.5 million veterans and active duty members of the military were stolen from the Department of Veterans Affair. Everybody has heard about this, but I think we need to examine it carefully and learn from this experience. The administration needs to provide the public with a thorough accounting regarding the VA incident, and it must detail how it will ensure that no future breaches will occur with respect to the tremendous volume of information the Veterans Administration and other Federal agencies maintain on Americans across the country.

The recent VA data breach represents a violation of trust of remarkable magnitude. The administration's failure to protect against such an incident and its delayed response may have made millions of men and women who currently serve or have served in uniform vulnerable to identity theft and other potentially costly misuse of their information.

Unfortunately, this breach does not come as a surprise. Consider for example GAO's July 2005 assessment of information security in the Federal Government. GAO stated: Pervasive weaknesses threaten the integrity, confidentiality, and availability of Federal information and information systems. These weaknesses exist primarily because agencies have not yet fully implemented strong information security management programs. These weaknesses put Federal operations and assets at risk of fraud, misuse and destruction. In addition, they place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure and critical operations at risk of disruption. So we had a warning as of July 2005, and indeed in this year, March of this year, in its annual scorecard evaluation, this committee gave the Federal Government a government-wide grade of D-plus, and the VA received a grade of F.

Well, remarkably and regrettably, the Bush administration has repeatedly shown questionable commitment to protecting the privacy of American citizens. For example, last December, we learned that the President had authorized warrantless eavesdropping on Americans' e-mails and phone calls despite Federal laws prohibiting this practice. Just this week, the Washington Post reported that, "since the Federal medical privacy requirements went into effect in 2003, the administration has received nearly 20,000 complaints alleging violations but has not imposed a single civil fine and has prosecuted just two criminal cases."

Well, I hope the administration will view the VA data breach as impetus for placing higher priority on privacy issues relating to the sensitive data it collects and maintains on Americans. You would think that the General Accounting Office report in July 2005 which was so damning should have been a wake-up call. Now we have another wake-up call where the data has actually been surreptitiously available to others that could do harm to the veterans whose data may be used against them. Well, I hope we will give a higher priority on privacy issues because technology advances facilitate the sharing of information, and as we develop new ways to use data on individuals to further important goals such as terrorism preven-

tion, we must be vigilant about protecting Americans' privacy rights. In the short term, the government must do everything possible to address expeditiously, any harm resulting to the individuals whose data was stolen. The VA Secretary has taken several steps to provide information to veterans about the breach, but the administration should be doing more to support the affected veterans and active service members.

I recently joined Representative Salazar and over 100 other colleagues in urging President Bush to request emergency funding for free credit monitoring and additional free credit reports for veterans and others whose information was compromised. For our part, Congress should consider measures, such as the Veterans Identity Protection Act of 2006 which Representative Salazar has introduced. This bill would require the Department of Veterans Affairs to certify that it has notified all affected individuals. It would also direct the VA to provide free credit monitoring services and reports to each affected individual. We must also determine exactly what went wrong at the VA, not only to know what happened but to prevent future breaches. To that end, there is an ongoing joint investigation by the inspector general, the Department of Justice and local law enforcement, and I hope that today's hearing will advance our understanding of this issue.

Finally, the VA data breach should underscore the importance of ensuring implementation of sound information-security practices government-wide. The reports from the Office of Management and Budget and the Government Accountability Office show that some agencies, some agencies are making progress on this front. The A-plus grade this committee gave the Social Security Administration this year underscores that large agencies with aging systems and vast amounts of sensitive data can comply with Federal information security requirements.

I want to thank all the witnesses for taking time to appear before the committee today. I look forward to hearing from them about the issues raised by the VA data breach. I hope this will not just be another hearing, another wake-up call that is ignored and that we find ourselves with similar breaches of privacy as we unfortunately have seen with the veterans in this country.

Chairman TOM DAVIS. Thank you.

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

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

Statement of Rep. Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
Hearing on the Security of Personal Information
at Federal Agencies
June 8, 2006

Mr. Chairman, I am pleased that you are holding this hearing on federal data security.

Last month, sensitive data on 26.5 million veterans and active duty members of the military was stolen from the Department of Veterans Affairs. The Administration needs to provide the public with a thorough accounting regarding the VA incident. And it must detail how it will ensure that no future breaches occur with respect to the tremendous volume of information the VA and other federal agencies maintain on Americans across the country.

The recent VA data breach represents a violation of trust of remarkable magnitude. The Administration's failure to protect against such an incident – and its delayed response – may have made millions of men and women who currently serve and have served in uniform vulnerable to identity theft and other potentially costly misuse of their information.

Unfortunately, this breach does not come as a surprise.

Consider, for example, GAO's July 2005 assessment of information security in the federal government. GAO stated:

> Pervasive weaknesses … threaten the integrity, confidentiality, and availability of federal information and information systems. … These weaknesses exist primarily because agencies have not yet fully implemented strong information security management programs. These weaknesses put federal operations and assets at risk of fraud, misuse, and destruction. In addition, they place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

Indeed, in March of this year, in its annual scorecard evaluating agency information security practices, this Committee gave the federal government a governmentwide grade of D+. The VA received a grade of F.

Regrettably, the Bush Administration has repeatedly shown questionable commitment to protecting the privacy of American citizens.

For example, last December, we learned that the President has authorized warrantless eavesdropping on Americans' e-mails and phone calls, despite federal laws forbidding this practice. Just this week, the *Washington Post* reported that since the federal medical privacy requirements went into effect in 2003, the Administration has received nearly 20,000 complaints alleging violations but "has not imposed a single civil fine and has prosecuted just two criminal cases."

I hope that the Administration will view the VA data breach as impetus for placing higher priority on privacy issues relating to the sensitive data it collects and maintains on Americans. As technological advances facilitate the sharing of information and as we develop new ways to use data on individuals to further important goals such as terrorism prevention, we must be vigilant about protecting Americans' privacy rights.

In the short term, the government must do everything possible to address expeditiously any harm resulting to the individuals whose data was stolen. The VA Secretary has taken several steps to provide information to veterans about the breach. But the Administration should be doing more to support the affected veterans and active service members.

I recently joined Rep. Salazar and over 100 other colleagues in urging President Bush to request emergency funding for free credit monitoring and additional free credit reports for veterans and others whose information was compromised. For our part, Congress should consider measures such as the Veterans Identity Protection Act of 2006, which Rep. Salazar has introduced. This bill would require the Department of Veterans Affairs to certify that it has notified all affected individuals. It would also direct the VA to provide free credit monitoring services and reports to each affected individual.

We must also determine exactly what went wrong at the VA to prevent future breaches. Toward that end, there is an ongoing joint investigation by the Inspector General, the Department of Justice, and local law enforcement, and I hope that today's hearing will advance our understanding of this issue.

Finally, the VA data breach should underscore the importance of ensuring implementation of sound information security practices governmentwide. The reports from the Office of Management and Budget and the Government Accountability Office show that some agencies are making progress on this front. The A+ grade this Committee gave the Social Security Administration this year underscores that large agencies with aging systems and vast amounts of

sensitive data can comply with federal information security requirements.

I want to thank the witnesses for taking the time to appear before the Committee today, and I look forward to hearing from them about the issues raised by the VA data breach.

Chairman TOM DAVIS. We will move to our panel.

We have the Honorable Clay Johnson III, the Deputy Director for Management, Office of Management and Budget; the Honorable R. James Nicholson, Secretary of the Department of Veterans Affairs, accompanied by Tim McClain, who is the General Counsel of the Department of Veterans Affairs, and Robert Howard, the senior adviser to the Deputy Secretary and Supervisor, Office of Information and Technology, Department of Veterans Affairs; the Honorable David Walker, the Comptroller General, Government Accountability Office; William E. Gray, the Deputy Commissioner for Systems, Social Security Administration; and Mr. Daniel Galik, Chief Mission Assurance and Security Services for the IRS, Department of Treasury.

It is our policy to swear all witnesses in before they testify. So, including Mr. McClain and Mr. Howard, if you would rise and raise your right hands.

[Witnesses sworn.]

Chairman TOM DAVIS. We will start with you, Mr. Johnson, and we will move straight down. Thank you very much.

STATEMENTS OF CLAY JOHNSON III, DEPUTY DIRECTOR FOR MANAGEMENT, OFFICE OF MANAGEMENT AND BUDGET; R. JAMES NICHOLSON, SECRETARY, DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY TIM MCCLAIN, GENERAL COUNSEL, DEPARTMENT OF VETERANS AFFAIRS, AND ROBERT HOWARD, SENIOR ADVISER TO THE DEPUTY SECRETARY AND SUPERVISOR, OFFICE OF INFORMATION AND TECHNOLOGY, DEPARTMENT OF VETERANS AFFAIRS; DAVID M. WALKER, COMPTROLLER GENERAL, GOVERNMENT ACCOUNTABILITY OFFICE; WILLIAM E. GRAY, DEPUTY COMMISSIONER FOR SYSTEMS, SOCIAL SECURITY ADMINISTRATION; AND DANIEL GALIK, CHIEF MISSION ASSURANCE AND SECURITY SERVICES, INTERNAL REVENUE SERVICE, DEPARTMENT OF TREASURY

STATEMENT OF CLAY JOHNSON III

Mr. JOHNSON. Mr. Chairman and members of the committee, thank you. I'm here to speak about the adequacy or inadequacy of existing laws, regulations and policies regarding privacy, information security and data breach notification. I'm here because we have had an unprecedented security breach causing the loss of personal data concerning millions of people.

Generally, at OMB, we believe we have sound laws, policies and standards related to this topic. But we can and must do a much, much better job of implementing them. We have policies and standards that call for encryption and passwords to protect data taken offsite via laptops, for instance. But we obviously need to do a better job of abiding by them. We must do a better job of holding ourselves accountable for implementing existing policies and holding each employee accountable for performing their assigned responsibilities.

In the short term, as the Deputy Director for Management, I have instructed agencies to remind each employee of their specific responsibilities for safeguarding personally identifiable information

and the relevant rules and penalties. I have instructed them to review and appropriately strengthen the means by which they hold their bureaus and people accountable for adhering to existing security guidelines, and I have instructed them to ensure that they are reporting all security incidences as required by law.

Our inspectors general are already reviewing the adequacy of their data security oversight. As chair of the PCIE and the ECIE, the two inspector general associations. I will make sure that IG oversight is consistent with the high level of accountability called for in this matter.

Longer term, the Federal Government is already implementing a 2004 Presidential Directive to develop and utilize information cards that will be used to control access to government computer systems and physical facilities. It will take several years to implement this new initiative.

OMB, all executive branch agencies and employees, and the inspectors general community have a shared responsibility to minimize the risk of harm associated with our use of this type of data. I am committed to working with Congress to ensure our information security policies and procedures are what they need to be and, most importantly, that we are all held accountable for following them. Thank you.

[The prepared statement of Mr. Johnson follows:]

STATEMENT OF THE HONORABLE CLAY JOHNSON III
DEPUTY DIRECTOR FOR MANAGEMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
June 8, 2006

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to speak about the adequacy of existing laws, regulations, and policies regarding privacy, information security, and data breach notification.

Unfortunately, I am here today in the wake of an unprecedented security breach causing the loss of personal data concerning millions of people. Clearly we have a problem. Losing any type of government data is bad enough, but losing personal data is especially troubling as it undermines the public's trust and confidence in our ability to protect them as individuals and keep them from harm.

As your invitation requested, I will describe our review of existing laws and policies, the lessons we have learned from the recent incident and steps for improving our response in the future. You will note the steps we are taking include a focus on better understanding how security programs are actually performing to help avoid breaches in the first place.

Over the past several weeks since the incident, we have reexamined the law and policies designed to prevent problems such as this. We have looked for weaknesses in the policies themselves and in our oversight and measurement of agency performance in implementing them. While we believe the law and policies are generally sound and this incident would not have occurred had elementary and long-standing security procedures been followed, this is a hollow victory and we are left with the same unacceptable results – a breach placing the data concerning millions of people at risk and from which each individual may have to recover.

Our review has identified four specific, but related issues. First, the recent incident makes painfully obvious a long-known security risk – a single trusted individual can mistakenly or intentionally and very quickly, undo all of the sophisticated and expensive controls designed to safeguard our information and systems from attack. To safeguard against this risk, the agencies themselves must be held accountable for implementing existing policies such as segregating personnel duties so one person cannot cause such damage.

Second, good security and privacy are shared responsibilities. As you know, within a framework of laws developed by Congress and through direction from the President, the Office of Management and Budget (OMB) develops policies for and oversees agencies' programs to protect security and information privacy. Agencies are responsible for implementing the policies based upon the risk and magnitude of harm that would result from a breach in their security, ensuring their programs are managed to

maintain risk at an acceptable level, and Inspectors General must independently evaluate effectiveness. Each individual, from rank and file employees and their supervisors to independent evaluators and overseers, must be held accountable for performing their assigned responsibilities. The American public expects and deserves positive results from all of us.

Third, while we have seen significant improvements in agency security planning more than 80% of government systems are certified and accredited, 17 Inspectors General rate agency planning processes as satisfactory or better and 12 Inspectors General indicate their agency has put this planning into practice improving their security performance – our view of the state of government security is much the same as reflected in your Committee's annual security report card – it is not nearly where it must be.

Of course we all know good planning is not enough. Plans must be executed and agency employees must be instructed in clear and unambiguous terms on how to use them, the rules they must go by, and what will happen if the rules are not followed. Equally and perhaps more importantly, managers must oversee execution, ensure their employees are in fact doing what the plans say must be done, and continually monitor operational effectiveness in an ever-changing risk environment. Finally, as the Federal Information Security Management Act says, Inspectors General must independently evaluate their agencies' programs. To get a better picture of how agencies are executing their plans, I am directing each agency head to describe in their annual Federal Information Security Management Act report the specific actions they take to ensure their plans are in fact being implemented.

Fourth, security and privacy are commonly seen as separate responsibilities and programs. They are not. We see them as separate pieces of the same puzzle – personally identifiable information is an example of <u>what to protect</u>, while security is a program for <u>how to protect it</u>. At least in part due to this program separation, agencies also characterize differently how and when to report incidents and breaches involving privacy and security. There are also differences in how agencies characterize and report incidents and breaches stemming from physical or cyber incidents.

Correcting this problem involves both near and mid-term efforts. We have begun reviewing these issues using both the Identity Theft Task Force established by Executive order on May 10, 2006, and an OMB-led working group of agency privacy experts. Additionally, we will begin working with the Department of Homeland Security, designated by law as the government's central cyber incident coordination organization, to combine incident reporting. Without prejudging the results of these efforts, we will remove any artificial and unnecessary barriers or differences between various reporting practices for security and privacy incidents, and make clear to all agency employees what they must report, to whom, and within what specific timeframe.

In taking these actions, we will certainly continue to apply our current policy of immediate reporting of the highest-impact incidents such as the recent loss of personally identifiable information. We will also see if revisions are needed to the current reporting

requirements and schedules for lower impact incidents. Also, to ensure a more timely picture of all agencies' operational security, I have directed my staff to work with the Department of Homeland Security, the Chief Information Officers Council, and Senior Agency Officials for Privacy to identify the appropriate level of detail and a schedule for distributing a periodic government-wide incident report to agency officials, Inspectors General, and other interested parties such as the Government Accountability Office. This may be a quarterly report – our current annual report to Congress is not timely enough.

At my direction, Senior Agency Officials for Privacy are now reviewing the effectiveness of their security programs and will report to OMB their findings early this fall with their agency's annual reports under the Federal Information Security Management Act. These reports will help us identify the extent to which additional actions are necessary.

I also would like to mention longer-term steps we are taking to increase the security of our sensitive information, computer systems, facilities, and employees. In response to an August of 2004 Presidential directive, OMB led the development of a common identification standard for several million Federal employees and contractors. This directive requires all Executive branch agencies to conduct background checks on their employees and contractors before issuing them permanent government identification. The agencies are now conducting these checks and in October of this year, will begin issuing new identification cards. These cards have built-in security features to control access to government computer systems and the government's physical facilities.

I have outlined above a number of actions we are taking to demonstrate the Administration takes its information privacy and security responsibilities very seriously. These will help prevent a recurrence of an incident such as we just experienced, permit us to better respond if prevention fails, and provide us a more complete and timely view of the security performance of the agencies. Agencies spend more than $4.5 billion each year on controls to protect information and computer systems and we will use the budget process to ensure this money is wisely spent and re-emphasize new spending on information technology will not be approved if sound security is not already in place for existing systems and programs. We are prepared to take more action as necessary and I look forward to working with you to improve our security and privacy programs and welcome any suggestions you have.

Chairman TOM DAVIS. Thank you very much.

Secretary Nicholson, thanks for being with us.

STATEMENT OF R. JAMES NICHOLSON

Secretary NICHOLSON. Mr. Chairman, ranking member, members, I want to thank you for holding this hearing. I think it is very timely, and I thank you for the invitation to appear here before you to provide you with a report and an assessment of current events at the Department of Veterans Affairs.

In that context, I will also present a brief overview of VA security policies along with the Department's views on the adequacy of current regulation legislation, regulations and policies regarding privacy, information security and data breach notification. Facts surrounding the recent data breach at VA are well known to you through their coverage in the media. I will briefly recap them, though, before reviewing with you the actions that I have taken in response and what we have learned and are learning as a result and what we need to be doing as we go forward.

A 34-year VA employee, a VA analyst, took home electronic data files from the VA. He was not authorized to do so, but he had been in the practice of doing it for 3 years. On May 3, that employee's home was broken into in what appears to local law enforcement to be a routine breaking and entering. His laptop computer and hard drive containing the VA data were stolen. These data contained identifying information on up to 26.5 million veterans, some spouses and dependents. It is important to note that the data did not include any of the VA's electronic health records.

On June 1, independent forensic experts that we retained, confirmed that there was some data pertaining to active duty, Guard and Reserve troops. On June 5, we learned through ongoing analysis and through data matching and discussions with the Department of Defense that private information on over 2 million active duty, Guard and Reserves may have also been included. As I stated in my testimony before the House and the Senate Committees on Veterans Affairs recently, I am totally outraged at the loss of this data and the fact that an employee would put so many people at risk by taking it home in violation of existing VA policies.

I'm also gravely concerned about the timing of the Department's response once the burglary did become known. I accept responsibility for this. I am in charge of this Department. I have never been so disappointed and angry at people, but it is my responsibility also now to fix this. And just as the health care system, the VA has risen to be a paradigm of integrated health care in our country and it has done so in a relatively short period of time, I think that we can make the same of the VA and data security, and I'm committed to doing that because it's doable. It won't be easy, and it won't be overnight because we are going to have to change a culture.

Full-scale investigations into this matter remain ongoing. Authorities believe it's unlikely the perpetrators targeted the items stolen because of any knowledge of the data contents. We remain hopeful that this was a common random theft and that no use will be made of this data. However, certainly we cannot count on that. And because we are committed to keeping our veterans and our service members informed, we have established call centers with

call numbers to provide information which we have promulgated in many different ways, including a letter to each of the known affected people. We've dedicated a Web site that provides answers to any concerned veteran, service member or family member. These are updated as additional information becomes available to us regarding this theft and what it might entail.

From the moment I was informed, the VA began taking all possible steps to protect and inform our veterans. On May 31st I named Maricopa County District Attorney Richard Romley, formerly district attorney, as my new special adviser for information security reporting directly to me. Mr. Romley shares my commitment to cutting through the bureaucracy to provide the results our Nation's veterans and service members deserve and expect. I have initiated several actions to strengthen our privacy and data security programs. On May 24th, we launched the Data Security Assessment and Strengthening Program, a high-priority focus plan to strengthen our data privacy and security procedures. On May 26th, I directed my top leadership to reenforce each VA manager of their duty to protect sensitive information. I've instructed all employees to complete privacy and cyber security training by June 30th. Further, I have convened a task force of VA senior leadership to review all aspects of information security, inventory all positions requiring access to sensitive VA data and ensure that personnel have the appropriate current security clearances. On June 6th, 2 days ago, I issued a VA information technology directive entitled, Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations. I also issued a separate directive under the under secretary of benefits suspending the practice of permitting veterans' benefits employees to remove files for claims from their regular work stations in order to adjudicate claims from alternative work locations, including their homes.

During the week of June 26th, VA facilities across the country and including Guam, Manila and the Puerto Rican islands at every hospital, clinic, regional office, national cemetery, field office and our central office will stand down for Security Awareness Week. Managers throughout the VA will review information security and reenforce privacy obligations and responsibilities with their staff. I've also ordered that every laptop in the VA undergo a security review to ensure that all security and virus software is current. The review will include removal of any unauthorized information or software. I have also ordered that no personal laptop or computer equipment will be allowed to access the VA's virtual private network or be used for any official business.

You asked that I review the VA's data security policies and procedures. I believe these have been shared with you and your staff and they are discussed in my written testimony. They include: VA Directive 6502, issued on June 30, 2003 on our privacy program; Directive 5011 dated September 22, 2005, providing specific policies and procedures for the approval of alternative workplace arrangements and teleworking.

One existing guideline, Security Guideline for Single-User Remote Access, will be published very soon as a VA directive. This document sets the standards for access, use and information security including physical security, incident reporting and responsibil-

ities. I believe that the policies we have and the legislation under which they are promulgated is generally adequate. But it is, Mr. Chairman, too hard in my opinion to discipline people in the Civil Service. It is too hard to impose sanctions. I have multiple examples of that I can give you of people at each strata of leadership in the VA who, due to the cultural lapses, have violated the existing policies. I think something that this committee and the Congress should look at is HIPA, the Health Information Portability Accounting Act, which has teeth in it for violations of health information breaches, and I think we should consider putting the same kind of teeth into an enforcement mechanism for the compromising and the careless and negligent handling of personal information, putting it under the same category of enforcement.

Another that I think needs to be considered is that while we have a system in the government of doing background investigations for people to whom we will give access to classified information, we do not have a similar screen for those to whom we will give enormous amounts of data. And I will use—this is my wallet. This is a hard drive that holds 60 gigabytes; 60 gigabytes will hold 12 times the information that was compromised in our data breach. This will hold the personal information of the population of the United States, and it fits very easily into my vest pocket.

So obviously what we need to do is know more about the people who have access. This employee who took this home, as I said, worked for 34 years with the VA. He has not had a background check for 32 years. He did, by the way, this year sign the annual requirement for security awareness.

So it is clear that we need to put some teeth behind the obvious needs that also exist at the VA for more training, education and enforcement and the ascertainment of the culture of the people that we are giving access. This has been a painful lesson for me at the VA.

Ultimately our success in changing this is going to depend on changing the culture, and that depends on our ability to change the attitudes of our people. It is our obligation to do this, to ensure that they have the right training, that they are instilled with the sense of discipline and the commitment to be careful in their trusteeship of this data, and we have an obligation on, collectively, I believe, at the governmental level to ensure the character and the vulnerability of people that have access in important work for caring for our veterans and all of the other people in this government. This is a personal priority of mine. Indeed, I believe it needs a crusade. This is an emergency. It is an emergency at the VA, and it should be an emergency in our society.

Last night I was approached by a university president who recognized me to tell me about a data breach that they'd just had—I can't divulge—but a very prestigious university and its recommendations. So this is unfortunately rampant and we need to have better tools in the way of approaching it. Significant change in the way the VA manages its infrastructure ironically was put into place by me last October. Part of the reason the VA I think has gotten so lapse is that it is decentralized and it is spread all over this country, as you know. I made a major policy decision and we are centralizing information technology, and that is undergoing

significant cultural resistance but we are going to do that and that was underway and that will also assist us in this broader goal and it will include both cyber and information security and privacy. We will stay focused on these problems until they're fixed and we will take direct and immediate action to address and alleviate people's concerns.

With greater control comes greater accountability. Mr. Chairman, I remain cognizant that we are accountable not only to you, the Congress, but also to our Nation's veterans and our service members. And, Mr. Chairman, that concludes my statement. Thank you for this opportunity.

[The prepared statement of Secretary Nicholson follows:]

Statement of
The Honorable R. James Nicholson
Secretary of Veterans Affairs

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

June 8, 2006
******

Mr. Chairman, Ranking Member Waxman, and members of the Committee.

Thank you for your invitation to appear before you this morning to provide you with a report and assessment of current events at the Department of Veterans Affairs. In that context, I will also present an overview of VA privacy and security policies and procedures, along with the Department's views on the adequacy of current legislation, regulations and policies governing privacy, information security and data breach notification.

The facts surrounding the recent data breach at VA that now rightfully draw the spotlight of Congressional oversight to government-wide information security policies and procedures are well known to you. I will briefly recap them before reviewing with you the actions that VA has taken in response, and what we have learned—and are learning—as a result.

A VA analyst took home electronic data files from VA. He was not authorized to do so. On May 3rd, that employee's home was broken into in what appears to local law enforcement to have been a routine breaking and entering. His laptop computer and hard drive containing the VA data were stolen. Initial analysis performed by both VA and its Inspector General indicated that these data contained identifying information, including names and dates of birth, for up to 26.5 million veterans and some of their spouses. In addition, that information, plus social security numbers, was available for some 19.6 million of those veterans. Also possibly included were some numerical

disability ratings and the diagnostic codes which identify the disabilities for which the veteran is being compensated. It is important to note that none of the data included the VA's electronic medical records.

As part of our ongoing effort to better determine what information was compromised, in addition to deploying our own internal technical experts, VA hired its own independent forensic experts, Internet Security Services, to analyze data on some 17 disks that were in the possession of the analyst. On June 1st, we learned that there was some information pertaining to active duty, Guard and Reserve troops among the individuals whose data had been compromised. On June 5th, we learned through ongoing analysis, and through discussions with the Department of Defense, that private information – the names, social security numbers and dates of birth – of as many as 1.1 million active-duty personnel from all the armed forces, along with 430,000 members of the National Guard, and 645,000 members of the Reserve force, may have been included. We are working with the Department of Defense to match data and verify, to the greatest extent possible, those potentially affected. Individualized notification letters are being sent to all those whose personal information may have been included among the stolen data. We are working with the Internal Revenue Service and the Social Security Administration to assure that we have their most current addresses.

As I stated in my testimony before both the House and Senate Committees on Veterans' Affairs last month, I am outraged at the theft of this data and the fact an employee would put it at risk by taking it home in violation of VA policies. I am also gravely concerned about the timing of the Department's response once the burglary became known. Full-scale investigations into this matter remain ongoing. Authorities believe it is unlikely the perpetrators targeted the items stolen because of any knowledge of the data contents. We remain hopeful that this was a common theft, and that no use will be made of the VA data.

However, because we are committed to keeping our veterans and service members informed, VA, working with our Federal government colleagues, established call centers (800-FED-INFO) and a dedicated website (www.firstgov.gov) on May 22nd to provide answers to any concerned veteran, service member, or family member. These are updated as additional information becomes available to us regarding this data theft and what it might imply. Those tools will remain active for as long as they remain necessary for communicating with all affected persons.

From the moment I was informed, VA began taking all possible steps to protect and inform our veterans. Last week, I announced a series of personnel changes in VA's Office of Policy and Planning, the division in which the breach occurred. I have detailed current Assistant General Counsel for Management and Operations, Paul Hutter, to provide leadership to this office while the recent nomination of Patrick W. Dunne as Assistant Secretary for Policy and Planning is considered by the United States Senate. Mr. Hutter replaced the Acting Assistant Secretary for Policy and Planning, a long-time career employee, who has been placed on administrative leave. In addition, the Deputy Assistant Secretary for Policy resigned effective Friday, June 2, 2006.

I assure you that my commitment to changing the way we do business at VA is not limited to personnel actions. Moving forward, and emphasizing our commitment to improving our information security procedures, on May 31, 2006, I named former Maricopa County (Phoenix, AZ) District Attorney Richard M. Romley as my new Special Advisor for Information Security, reporting directly to me.

Mr. Romley will evaluate the current state of VA's information security procedures and processes, and will make recommendations for improvement in VA's information security systems. Rick Romley is a well-respected prosecutor and combat veteran who will bring a critical outsider's perspective to this effort. Mr. Romley shares my commitment to cutting through the bureaucracy to provide the results our nation's veterans and service members deserve and expect.

I have initiated several actions to determine how to best strengthen our privacy and data security programs. On May 24, 2006, we launched the *Data Security-Assessment and Strengthening of Controls* program, a high priority, focused plan to strengthen our data privacy and security procedures. This program will minimize the risk of a re-occurrence of incidents similar to this recent breach, and seeks to remedy material weakness that could place sensitive information at risk.

On May 26, 2006, I issued a directive to my top leadership to reinforce in each VA manager, supervisor, or team leader their duty and responsibility to protect sensitive and confidential information. In this memo, I instructed all employees to complete privacy and cyber security training by June 30, 2006. Further, I have convened a task force of VA's senior leadership to review all aspects of information security and to make recommendations that will strengthen our safeguarding of sensitive information. As an initial step, I charged this Task Force to complete an inventory of all positions requiring access to sensitive VA data by June 30, 2006. In conjunction with this, we will conduct a review of sensitivity levels and ensure that personnel at all levels have the appropriate and current National Agency Check and Inquiry (NACI), Minimum Background Investigation (MBI), or Background Investigation (BI) investigations and that these are documented in their respective personnel records.

On June 6, 2006, two days ago, I issued VA IT Directive 06-2, *Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations*. This Directive recommits both the Department, and our employees, to protecting the personal data of all individuals, including veterans, dependents and employees, while informing all concerned parties that failure to comply with VA policy may violate Federal law and could result in administrative, civil or criminal penalties. It further provides direction on proper notification procedures should a breach occur, and directs all VA senior management officials to ensure that employees under their supervision fully comply.

Also on June 6th, I issued a separate directive that the Under Secretary for Benefits suspend the practice of permitting Veterans Benefits Administration (VBA) employees to remove claims files from their regular work stations in order to adjudicate claims from alternative work locations (i.e. their homes.) This suspension will remain in place until I am satisfied VBA has in place adequate policies and procedures, and the necessary physical means to safeguard those files from theft, loss, or other unauthorized disclosure.

These initiatives will culminate across VA nationwide during the week of June 26, 2006, when VA facilities across the country – every hospital, CBOC, regional office, national cemetery, field office and VA's Central Office – will "stand down" for Security Awareness Week. Managers throughout VA will review information security and reinforce privacy obligations and responsibilities with their staff. I have also ordered that every laptop in VA undergo a security review to ensure that all security and virus software is current. The review will include removal of any unauthorized information or software. Importantly, I have ordered that no personal laptop or computer equipment be allowed access to VA's Virtual Private Network (VPN) or be used for official business. VPN settings will be changed every 30 days, forcing laptop users to return the laptop to VA for updating and security screening. We are in the process of conducting an inventory of all positions in VA with access to VPN or to any sensitive information.

You asked that I review VA's data security policies and procedures. The Department has several policies, procedures, and guidelines that govern the privacy and security of sensitive information.

VA Directive 6502, dated June 30, 2003, *Privacy Program*, establishes a Department-wide program for the protection of the privacy of veterans, their dependents and beneficiaries, as well as the privacy of all VA employees. This directive provides for the safeguarding and security of all privacy-protected data stored or transmitted in VA information systems for which VA is responsible, as well as those systems shared with, or operated by, other Federal agencies, contractors, or outside organizations.

Specific policies and procedures for the approval of alternative workplace arrangements, or telework, are governed by VA Directive 5011, dated September 22, 2005, *Hours of Duty and Leave.* This directive requires the completion of the User's Remote Computing Security Agreement between the Supervisor and the employee. The employee must complete a safety checklist and notify his organization's Information Security Officer (ISO) of the telework arrangement. The organization sponsoring telework must also ensure that adequate technological security protections are in place on all electronic devices issued to telework participants.

The FY 2001 Department of Transportation and Related Agencies Appropriations Act, Public Law 106-346, Section 359, states that, "Each executive agency shall establish a policy under which eligible employees of the agency may participate in telecommuting to the extent possible without diminished employee performance." Under that law telecommuting is defined as "any arrangement in which an employee regularly performs officially assigned duties at home or other work sites geographically convenient to the residence of the employee," and an eligible employee is "any satisfactorily performing employee of the agency whose job may typically be performed at least one day per week at an alternative workplace." Telework is not unique to VA, and is, in fact, an alternative work arrangement promoted by federal government policy. The Office of Personnel Management (OPM) encourages telework as a means of making reasonable accommodation to persons with disabilities and as a critical factor in the implementation of continuity of operations plans.

One existing Security Guideline, *Security Guideline for Single-User Remote Access,* describes appropriate security measures for mobile or fixed computers used to process, store, or transmit information or connect to VA IT systems when such computers are housed in an alternate work location. It identifies and recommends the minimally acceptable security controls when VA personnel use anything other than a direct connected, VA-controlled local area network (LAN) connection to perform VA information processing. Examples include people that are on travel, telecommuting or working from alternate work locations. This document requires that any data not stored on our systems be encrypted and password protected. I have directed the Office of

Information & Technology to publish this guideline as a VA Directive. This document sets the standards for access, use, and information security, including physical security, incident reporting and responsibilities.

Finally, we will continue to require all VA employees and contractors to complete annually both Cyber Security Awareness Training and Privacy Awareness Training. This training is designed to help VA employees understand the importance of protecting sensitive information and making them aware of their responsibilities in this regard. Normally, employees are required to complete this training by September 30th of each year. However, as I noted earlier, given the recent data breach at VA, I directed all employees to complete both courses by June 30, 2006.

As any Federal agency, VA's privacy and security policies and procedures implement all pertinent laws, regulations, Executive Orders. These laws include the Privacy Act, the Health Information Portability and Accountability Act, the Federal Information Security Management Act, and the Information Technology Management Reform Act. We establish our policies and procedures to implement Federal Information Processing Standards Publications developed by the National Institute of Standards and Technology, the Office of Personnel Management, the Office of Management and Budget and any other oversight agency in these program areas. I believe that we should have policies and legislation, government wide, that would enable us to discipline employees and, possibly bring criminal actions, against those who willfully disregard the safeguards needed to protect veterans and other sensitive data.

I am committed to working with Congress to create a plan for the federal government to improve this situation, and at the same time, I have asked the President's ID Theft Task Force to assist us in developing this policy.

There are many lessons to be learned from the recent data breach at VA. I do know, as I have stated previously, that the time to determine that a loss had occurred

and to assure that proper individuals within the chain of command were notified was too protracted. There was also a breakdown in communications in the notification process once the incident occurred.

Mr. Chairman, in his testimony this morning, Clay Johnson, III, Deputy Director for Management of the Office of Management and Budget, stated that

> "the recent incident makes painfully obvious a long-known security risk – a single trusted individual can mistakenly or intentionally, and very quickly, undo all of the sophisticated and expensive controls designed to safeguard our information and systems from attack."

This has been a painful lesson for us at VA, and I am committed to assuring that we have the people, adequately trained, policies and procedures in place to assure that this could not happen again. Moreover, I am strongly committed to ensuring that VA seize on this moment to change the status quo, to break the "as is" model of doing business, and to make VA an exemplary federal agency in the area of information security and privacy protection, just as it has become in the area of health care.

A significant change in the way VA manages its information technology infrastructure was already well underway before this incident. In October, 2005 I issued a directive reorganizing IT at VA through the centralization of many functions, to include cyber and information security and privacy. As we continue to centralize the control of our IT systems, our ability to meet our information security and privacy obligations will be greatly enhanced. We will stay focused on the problems until they are fixed, and we will take direct and immediate action to address and alleviate affected people's concerns. With greater control, comes greater accountability. Mr. Chairman, I remain cognizant that we are accountable not only to Congress, but also to our nation's veterans and our men and women who are wearing the uniform today. It is my pledge to you that I am, and will remain, guided in my leadership of VA by what is best for our veterans.

Mr. Chairman, that concludes my statement. Thank you for the opportunity to appear before you today.

Chairman TOM DAVIS. Thank you, Mr. Secretary. And now we'll hear from General Walker.

STATEMENT OF DAVID M. WALKER

Mr. WALKER. Thank you, Mr. Chairman. I assume that the entire statement will be included in the record and therefore I will move to summarize.

I appreciate the opportunity to be here today to discuss the key challenges that Federal agencies face in safeguarding certain personal and sensitive information that's in their custody and taking action when that information is compromised.

As we've just heard, there have been circumstances in the past where such information has been compromised, and I think it is important to note that this is a matter of increasing concern both in the public and the private sector and breaches have occurred all too frequently in the private and the public sector. As we look forward, I think it is important to keep in mind that Federal agencies are subject to security and privacy laws that are aimed in part at preventing security breaches, including breaches that could result in identity theft.

The major requirements of the protection of personal privacy by Federal agencies come from two laws: The Privacy Act of 1974 and the E-Government Act of 2002. The Federal Information Security Management Act of 2002, FISMA, also addresses the protection of personal information in the context of securing Federal agency information and information systems.

Federal laws to date have not required agencies to report security breaches to the public, although breach notification has played an important role in the context of security breaches in the private sector. A number of actions can and should be taken in order to help safeguard against the possibility that personal information maintained by government agencies is inadvertently compromised.

First, agencies should conduct privacy impact assessments and, second, agencies should ensure that they have a robust security program in place. In the course of taking a more strategic approach in adopting these two particular measures to protect privacy and enhance security over personal information, agencies should also consider several other specific actions, including limiting the collection of personal information, limiting data retention, limiting access to personal information and conducting appropriate training of persons who do have access, and considering using technological controls such as encryption when data needs to be stored on mobile devices, and other measures.

Irrespective of the preventative measure that James put in place data breaches are possible and may occur. However, in the event that an incident does occur agencies must respond quickly in order to minimize potential harm that could be imposed by identity theft. Applicable law such as the Privacy Act currently do not require agencies to notify individuals of security breaches involving their personal information. However, doing so allows those affected the opportunity to take steps to protect themselves against the dangers of identity theft. Breach notification is also important in that it can help an organization address key privacy rights of individuals and in the government notifying somebody like OMB, helps to obtain a

better understanding of the government-wide challenges associated with this area.

Public disclosure of major data breaches is a key step to ensuring that organizations are held accountable for personal protection of information. At the same time, care needs to be taken to avoid requiring agencies to notify the public of trivial security incidents.

In summary, agencies can and should take a number of actions to help guard against the possibility that data bases of personal, sensitive information aren't inadvertently compromised. Furthermore, when such compromises do occur, it is important that appropriate notification steps be taken.

We at GAO are attempting to lead by example as well, and I must note, Mr. Chairman, that I met with my own CIO about these issues and am comfortable that we are taking appropriate steps, but I have also instructed them to take a couple of additional steps in light of some of the recent events that have occurred.

I would also note that with the additional proliferation of teleworking and with the additional use of laptop computers in the government that this becomes an increasing challenge and one of significant concern and interest. As Congress considers legislation requiring agencies to notify individuals or the public about security breaches, we think it is important to ensure that there are specific criteria that are defined for the incidents that merit public notification. Congress may also want to consider a two-tier reporting requirement in which all Federal Government security breaches are reported to OMB and affected individuals regarding the nature of the violation and the risk imposed.

Furthermore, Congress should consider requiring OMB to provide guidance to agencies on how to develop programs and remedies to affected individuals.

And last, Mr. Chairman and members of the committee, I would say on listening to the two colleagues who presented before myself, you may want to think about whether or not there should be additional requirements for restricting access to sensitive information or conducting mandatory training and monitoring with regard to those who do have access for requiring reporting to OMB to the extent there is a significant breach within the Federal Government, and as the Secretary mentioned, make sure that there are tough sanctions for violators.

We need to have incentives. We need to have transparency, and we need to have an accountability mechanism, and if we don't have all three of those the system won't work.

Thank you very much.

[The prepared statement of Mr. Walker follows:]

United States Government Accountability Office

GAO

Testimony

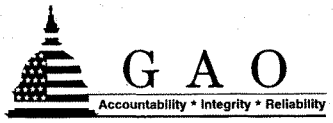
Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10 a.m. EDT
Thursday, June 8, 2006

PRIVACY

Preventing and Responding to Improper Disclosures of Personal Information

Statement of David M. Walker
Comptroller General of the United States



GAO-06-833T

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-833T, a testimony before the Committee on Government Reform, House of Representatives

June 8, 2006

PRIVACY

Preventing and Responding to Improper Disclosures of Personal Information

Why GAO Did This Study

The recent security breach at the Department of Veterans Affairs, in which personal data on millions of veterans were compromised, has highlighted the importance of the federal government's processes for protecting personal information. As the federal government obtains and processes information about individuals in increasingly diverse ways, it remains critically important that it properly protect this information and respect the privacy rights of individuals.

GAO was asked to testify on preventing and responding to improper disclosures of personal information in the federal government, including how agencies should notify individuals and the public when breaches occur. In preparing this testimony, GAO drew on its previous reports and testimonies, as well as on expert opinion provided in congressional testimony and other sources.

What GAO Recommends

GAO has made recommendations previously to agencies and to the Office of Management and Budget (OMB), which provides guidance to agencies on implementing federal privacy and security laws, to ensure that they are adequately addressing security and privacy issues.

In addition, in considering security breach notification legislation, the Congress should consider setting specific reporting requirements for agencies.

www.gao.gov/cgi-bin/getrpt?GAO-06-833T

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised. Two key steps are as follows:

- Develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed—whenever information technology is used to process personal information. These assessments, required by the E-Government Act of 2002, are a tool for agencies to fully consider the privacy implications of planned systems and data collections before implementation, when it may be easier to make critical adjustments.
- Ensure that a robust information security program is in place, as required by the Federal Information Security Management Act of 2002 (FISMA). Such a program includes periodic risk assessments; security awareness training; security policies, procedures, and practices, as well as tests of their effectiveness; and procedures for addressing deficiencies and for detecting, reporting, and responding to security incidents.

More specific practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal information, limiting the time that such data are retained, limiting access to personal information and training personnel accordingly, and considering the use of technological controls such as encryption when data need to be stored on mobile devices.

When data breaches do occur, notification to the individuals affected and/or the public has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft. Although existing laws do not require agencies to notify the public when data breaches occur, such notification is consistent with agencies' responsibility to inform individuals about how their information is being accessed and used, and it promotes accountability for privacy protection. That said, care is needed in defining appropriate criteria for incidents that merit notification. Notifying individuals of security incidents that do not pose serious risks could be counterproductive and costly, while giving too much discretion to agencies could result in their avoiding the disclosure of potentially harmful breaches. Care is also needed to ensure that notices are useful and easy to understand, so that they are effective in alerting recipients to actions they may want to take to minimize the risk of identity theft. Among other things, it is important to provide context in the notice—explaining to recipients why they are receiving a notice and what to do about it. It is also important the notices be coordinated with law enforcement to avoid impeding ongoing investigations. Given that individuals may be adversely impacted by a compromise of their personal information, it is critical that they fully understand the nature of the threat and the options they have to address it.

Mr. Chairman and Members of the Committee:

I appreciate the opportunity to be here today to discuss key challenges federal agencies face in safeguarding personally identifiable information[1] in their custody and taking action when that information is compromised. As the federal government obtains and processes personal information about individuals in increasingly diverse ways, it remains critically important that this information be properly protected and the privacy rights of individuals respected. Recently, as you know, personal data on millions of veterans was stolen from the home of an employee of the Department of Veterans Affairs, who had not been authorized to have the data at home. Compromises such as this raise important questions about what steps agencies should take to prevent such compromises and how they should notify citizens when breaches do occur.

As requested, my statement will focus on preventing and responding to improper disclosures of personal information in the federal government, including notifying the public about such security breaches. After a brief summary and discussion of the federal laws and guidance that apply to agency use of personal information, I will discuss potential measures that federal agencies can take to help limit the likelihood of personal information being compromised and then highlight key benefits and challenges associated with effectively notifying the public about security breaches.

To address measures that agencies can take to help limit the likelihood of personal information being compromised, we identified and summarized issues raised by experts in congressional testimony and in our previous reports, including our recent work regarding the federal government's use of personal information from

[1] For purposes of this testimony, the term *personal information* encompasses all information associated with an individual, including both identifiable and nonidentifying information. *Personally identifiable information*, which can be used to locate or identify an individual, includes such things as names, aliases, and Social Security numbers. *Nonidentifying personal information* includes such things as age, education, finances, criminal history, physical attributes, and gender.

companies known as information resellers.[2] We conducted the work for these reports in accordance with generally accepted government auditing standards. To identify benefits and challenges associated with effectively notifying the public about security breaches, we summarized expert opinion from congressional testimony as well as key practices identified at a Department of Homeland Security (DHS) privacy workshop, by the state of California, and by the Federal Trade Commission. To provide additional information on our previous privacy-related work, I have included, as an attachment, a list of 20 pertinent GAO publications.

Results in Brief

Agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised. Two key steps are (1) to develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed in a federal information system—whenever information technology is used to process personal information and (2) to ensure that a robust information security program is in place, as required by the Federal Information Security Management Act of 2002 (FISMA). More specific practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal information, limiting data retention, limiting access to personal information and training personnel accordingly, and considering using technological controls such as encryption when data need to be stored on mobile devices.

When data breaches do occur, notification to the individuals affected and/or the public has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft. It is also consistent with agencies' responsibility to inform individuals about how their information is being accessed

[2] GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421, (Washington: D.C.: Apr. 4, 2006).

and used and promotes accountability for its protection. At the same time, concerns have been raised that notifying individuals of security incidents that do not pose serious risks could be counterproductive and costly. Care is needed in defining appropriate criteria if agencies are required to report security breaches to the public, including coordinating with law enforcement. Care is also needed to ensure that notices are useful and easy to understand so that they are effective in alerting individuals to actions they may want to take to minimize the risk of identity theft.

We have made recommendations previously to OMB and agencies to ensure they are adequately addressing privacy issues, including through the conduct of privacy impact assessments. We have also recommended that OMB implement improvements in its annual FISMA reporting guidance to help improve oversight of agency information security programs. In addition, the Congress should consider setting specific reporting requirements for agencies as part of its consideration of security breach legislation. Further Congress should consider requiring OMB to provide guidance to agencies on how to develop and issue security breach notices to affected individuals.

Background

The recent theft of personally identifiable information on millions of veterans is only the latest of a series of such data breaches involving the loss or theft of information on magnetic tapes, computer hard drives, and other devices, as well as incidents in which individuals gained unauthorized access to large commercial databases of such information. Concerns about possible identity theft resulting from such breaches are widespread. The Federal Trade Commission (FTC) reported in 2005 that identity theft represented about 40 percent of all the consumer fraud complaints it received during each of the last 3 calendar years. Identity theft generally involves the fraudulent use of another person's identifying information—such as name, address, Social Security number, date of birth, or mother's maiden name—to establish credit, run up debt, or take over existing

financial accounts. According to identity theft experts, individuals whose identities have been stolen can spend months or years and thousands of dollars clearing their names. Some individuals have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft.

Several Key Laws Govern Agency Privacy Practices

Federal agencies are subject to security and privacy laws aimed in part at preventing security breaches, including breaches that could enable identity theft. The major requirements for the protection of personal privacy by federal agencies come from two laws, the Privacy Act of 1974 and the E-Government Act of 2002. FISMA also addresses the protection of personal information in the context of securing federal agency information and information systems.

The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by a "system-of-records notice": that is, a notice in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personal information.[3] Among other provisions, the act also requires agencies to define and limit themselves to specific predefined purposes.

The Office of Management and Budget (OMB), which is responsible for providing guidance to agencies on how to implement the

[3] Under the Privacy Act of 1974, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

provisions of the Privacy Act and other federal privacy and security laws, recently issued a memorandum reminding agencies of their responsibilities under the Privacy Act, other laws, and policy to appropriately safeguard sensitive personally identifiable information and train employees on their responsibilities in this area.[4] The memo called on agency senior privacy officials to conduct a review of policies and processes to make sure adequate safeguards are in place to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.

The provisions of the Privacy Act are largely based on a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices, which were first proposed in 1973 by a U.S. government advisory committee;[5] these principles were intended to address what the committee termed a poor level of protection afforded to privacy under contemporary law. Since that time, the Fair Information Practices have been widely adopted as a standard benchmark for evaluating the adequacy of privacy protections. Attachment 2 contains a summary of the widely used version of the Fair Information Practices adopted by the Organization for Economic Cooperation and Development in 1980.

The E-Government Act of 2002 strives to enhance protection for personal information in government information systems by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to OMB guidance,[6] a PIA is to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements

[4] Office of Management and Budget, *Safeguarding Personally Identifiable Information*, M-06-15 (Washington, D.C.: May 22, 2006).

[5] Congress used the committee's final report as a basis for crafting the Privacy Act of 1974. See U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: July 1973).

[6] Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. To the extent that PIAs are made publicly available,[7] they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

FISMA also addresses the protection of personal information. FISMA defines federal requirements for securing information and information systems that support federal agency operations and assets; it requires agencies to develop agencywide information security programs that extend to contractors and other providers of federal data and systems.[8] Under FISMA, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure to protect personal privacy, among other things. Your committee has issued annual report cards on federal government information security based on reports submitted by agencies as required by FISMA.

Interest in Data Breach Notification Legislation Has Increased

Federal laws to date have not required agencies to report security breaches to the public,[9] although breach notification has played an important role in the context of security breaches in the private sector. For example, California state law requires businesses to notify consumers about security breaches that could directly affect

[7] The E-Government Act requires agencies, if practicable, to make privacy impact assessments publicly available through agency Web sites, publication in the *Federal Register*, or by other means. Pub. L. 107-347, § 208(b)(1)(B)(iii).

[8] FISMA, Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002).

[9] At least one agency has developed its own requirement for breach notification. Specifically, the Department of Defense instituted a policy in July 2005 requiring notification to affected individuals when protected personal information is lost, stolen, or compromised.

them. Legal requirements, such as the California law, led ChoicePoint, a large information reseller,[10] to notify its customers in mid-February 2005 of a security breach in which unauthorized persons gained access to personal information from its databases. Since the ChoicePoint notification, bills were introduced in at least 44 states and enacted in at least 29[11] that require some form of notification upon a security breach.

A number of congressional hearings were held and bills introduced in 2005 in the wake of the ChoicePoint security breach as well as incidents at other firms. In March 2005, the House Subcommittee on Commerce, Trade, and Consumer Protection of the House Energy and Commerce Committee held a hearing entitled "Protecting Consumers' Data: Policy Issues Raised by ChoicePoint," which focused on potential remedies for security and privacy concerns regarding information resellers. Similar hearings were held by the House Energy and Commerce Committee and by the U.S. Senate Committee on Commerce, Science, and Transportation in spring 2005.

Several bills introduced at the time of these hearings, such as the Data Accountability and Trust Act,[12] would establish a national requirement for companies that maintain personal information to notify the public of security breaches. While many of these proposals were focused on private sector companies rather than the federal government, they could be applied to any organizations that collect and maintain significant amounts of personally identifiable information. The Notification of Risk to Personal Data Act[13] would

[10] Information resellers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers, which include both private-sector businesses and government agencies. For additional information, see GAO-06-421.

[11] States that have enacted breach notification laws include Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Washington, and Wisconsin.

[12] H.R. 4127; introduced by Representative Clifford B. Stearns on October 25, 2005.

[13] S. 751; introduced by Senator Dianne Feinstein on April 11, 2005.

explicitly include federal agencies, requiring them as well as any "persons engaged in interstate commerce" to disclose security breaches involving unauthorized acquisition of personal data.

Agencies Can Take Steps to Reduce the Likelihood That Personal Data Will Be Compromised

A number of actions can be taken to help guard against the possibility that personal information maintained by agencies is inadvertently compromised. I will focus my remarks today on key strategic approaches for safeguarding personal information as well as a few practical measures that could be critical in preventing data breaches. I will not discuss at length the broader topic of information security in the federal government, which both the committee and GAO have addressed extensively in the past.[14] Key strategic approaches include the following:

Conduct privacy impact assessments (PIAs). It is important that agencies identify the specific instances in which they collect and maintain personal information and proactively assess the means they intend to use to protect this information. This can be done most effectively through the development of PIAs, which, as I previously mentioned, are required by the E-Government Act of 2002 when using information technology to process personal information. PIAs are important because they serve as a tool for agencies to fully consider privacy implications of planned systems and data collections before those systems and collections have been fully implemented, when it may be relatively easy to make critical adjustments.

In prior work we have found that agencies do not always prepare PIAs as they are required. For example, our review of selected data

[14] See, for example, GAO, *Information Security: Department of Health and Human Services Needs to Fully Implement Its Program*, GAO-06-267 (Washington, D.C.: February 24, 2006) and *Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program*, GAO-05-700 (Washington, D.C.: June 17, 2005).

mining efforts at federal agencies[15] determined that PIAs were not always being done in full compliance with OMB guidance. Similarly, as identified in our work on federal agency use of information resellers,[16] few PIAs were being developed for systems or programs that made use of information reseller data because officials did not believe they were required. Complete assessments are an important tool for agencies to identify areas of noncompliance with federal privacy laws, evaluate risks arising from electronic collection and maintenance of information about individuals, and evaluate protections or alternative processes needed to mitigate the risks identified. Agencies that do not take all the steps required to protect the privacy of personal information risk the improper exposure or alteration of such information. We recommended that the agencies responsible for the data mining efforts we reviewed complete or revise PIAs as needed and make them available to the public. We also recommended that OMB revise its guidance to clarify the applicability of the E-Gov Act's PIA requirement to the use of personal information from resellers. OMB stated that it would discuss its guidance with agency senior officials for privacy to determine whether additional guidance concerning reseller data was needed.

Ensure that a robust security program is in place. FISMA requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Key elements of this program include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;

[15] GAO, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866 (Washington, D.C.: Aug. 15, 2005).

[16] GAO-06-421, pp. 59–61.

- risk-based policies and procedures that cost-effectively reduce risks to an acceptable level and ensure that security is addressed throughout the life cycle of each information system;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies through plans of action and milestones; and
- procedures for detecting, reporting, and responding to security incidents.

In prior reviews we have repeatedly identified weaknesses in almost all areas of information security controls at major federal agencies, and we have identified information security as a high risk area across the federal government since 1997. In July 2005, we reported that pervasive weaknesses in the 24 major agencies' information security policies and practices threatened the integrity, confidentiality, and availability of federal information and information systems.[17] These weaknesses existed primarily because agencies had not yet fully implemented strong information security management programs, as needed to fully meet FISMA requirements. We recommended that OMB implement improvements in its annual FISMA reporting guidance to help improve oversight of agency information security programs. In March 2006, we reported that OMB had taken several actions to improve reporting and could further enhance the reliability and quality of reported information.[18]

[17] GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

[18] GAO, *Information Security: Federal Agencies Show Mixed Progress In Implementing Statutory Requirements*, GAO-06-527T (Washington, D.C.: March 16, 2006).

In the course of taking strategic approaches to protecting the privacy and security of personal information, agencies will likely consider a range of specific practical measures. Several that may be of particular value in preventing inadvertent data breaches include the following:

Limit collection of personal information. One item to be analyzed as part of a PIA is the extent to which an agency needs to collect personal information in order to meet the needs of a specific application. Limiting the collection of personal information, among other things, serves to limit the opportunity for that information to be compromised. For example, key identifying information—such as Social Security numbers—may not be needed for many agency applications that have databases of other personal information. Limiting the collection of personal information is also one of the fair information practices, which are fundamental to the Privacy Act and to good privacy practice in general.

Limit data retention. Closely related to limiting data collection is limiting retention. Retaining personal data longer than needed by an agency or statutorily required adds to the risk that the data will be compromised. In discussing data retention, California's Office of Privacy Protection recently reported an example in which a university experienced a security breach that exposed 15-year-old data, including Social Security numbers. The university subsequently reviewed its policies and decided to shorten the retention period for certain types of information.[19] Federal agencies can make decisions up front about how long they plan to retain personal data as part of their PIAs, aiming to retain the data for as brief a period as necessary.

Limit access to personal information and train personnel accordingly. Only individuals with a need to access agency databases of personal information should have such access, and controls should be in place to monitor that access. Further, agencies can implement technological controls to prevent personal data from being readily transferred to unauthorized systems or media, such as

[19] State of California Department of Consumer Affairs, *Recommended Practices on Notice of Security Breach Involving Personal Information* (April 2006), p. 6.

laptop computers, discs, or other electronic storage devices. Security training, which is required for all federal employees under FISMA, can include training on the risks of exposing personal data to potential identity theft, thus helping to reduce the likelihood of data being exposed inadvertently.

Consider using technological controls such as encryption when data needs to be stored on mobile devices. In certain instances, agencies may find it necessary to enable employees to have access to personal data on mobile devices such as laptop computers. As discussed, this should be minimized. However, when absolutely necessary, the risk that such data could be exposed to unauthorized individuals can be reduced by using technological controls such as encryption, which significantly limits the ability of such individuals gaining access to the data. While encrypting data adds to the operational burden on authorized individuals, who must enter pass codes or use other authentication means to decrypt the data, it can provide reasonable assurance that stolen or lost computer equipment will not result in personal data being compromised, as occurred in the recent incident at the Department of Veterans Affairs. A decision about whether to use encryption would logically be made as an element of the PIA process and an agency's broader information security program.

While these suggestions do not amount to a complete prescription for protecting personal data, they are key elements of an agency's strategy for reducing the risks that could lead to identity theft.

Public Notification of Data Breaches Has Clear Benefits as Well as Challenges

I just discussed some preventive measures agencies can take to avoid a data breach. However, in the event an incident does occur, agencies must respond quickly in order to minimize the potential harm associated with identity theft. Applicable laws such as the Privacy Act currently do not require agencies to notify individuals of security breaches involving their personal information; however, doing so allows those affected the opportunity to take steps to protect themselves against the dangers of identity theft. For

example, the California data breach notification law is credited with bringing to the public's notice large data breaches within the private sector, including at information resellers such as ChoicePoint and LexisNexis last year. Although we do not know how many instances of identity theft resulted from last year's data breaches, the Federal Trade Commission has previously reported that the overall cost of an incident of identity theft, as well as the harm to the victims, is significantly smaller if the misuse of the victim's personal information is discovered quickly.[20] Arguably, the California law may have mitigated the risk of identity theft to affected individuals by keeping them informed about data breaches and thus enabling them to take steps such as contacting credit bureaus to have fraud alerts placed on their credit files, obtaining copies of their credit reports, scrutinizing their monthly financial account statements, and taking other steps to protect themselves. The chairman of the Federal Trade Commission has testified that the Commission believes that if a security breach creates a significant risk of identity theft or other related harm, affected consumers should be notified.[21]

Breach notification is also important in that it can help an organization address key privacy rights of individuals. These rights are based on the fair information practices (see attachment 2); these principles have been widely adopted and are the basis of privacy laws and related policies in many countries, including the United States. In particular, the *openness* principle states that the public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information. Breach notification is one way that organizations—either in the private sector or the government—can meet their responsibility for keeping the public informed of how their personal information is being used and who has access to it. Equally important is the *accountability* principle, which states that individuals controlling the collection or use of personal information

[20] Synovate, *Federal Trade Commission Identity Theft Survey Report* (McLean, Va.: September 2003).

[21] Federal Trade Commission, *Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft* (Washington, D.C.: June 16, 2005), p. 10.

should be accountable for taking steps to ensure the implementation of the other principles, such as use limitation and security safeguards. Public disclosure of data breaches is a key step in ensuring that organizations are held accountable for the protection of personal information.

Concerns Have Been Raised About the Criteria for Issuing Notices to the Public

Although the principle of notifying affected individuals (or the public) about data breaches has clear benefits, determining the specifics of when and how an agency should issue such notifications presents challenges, particularly in determining the specific criteria for incidents that merit notification. In congressional testimony, the Federal Trade Commission[22] raised concerns about the threshold for which consumers should be notified of a breach, cautioning that too strict a standard could have several negative effects. First, notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion. Second, a surfeit of notices, resulting from notification criteria that are too strict, could render all such notices less effective, because consumers could become numb to them and fail to act when risks are truly significant. Finally, the costs to both individuals and business are not insignificant and may be worth considering. The FTC points out that, in response to a security breach notification, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on credit files, or obtain a new driver's license number. These actions could be time-consuming for the individual and costly for the companies involved. Given these potential negative effects, care is clearly needed in defining appropriate criteria for required breach notifications.

While care needs to be taken to avoid requiring agencies to notify the public of trivial security incidents, concerns have also been raised about setting criteria that are too open-ended or that rely too heavily on the discretion of the affected organization. Some public advocacy groups have cautioned that notification criteria that are

[22] Federal Trade Commission, *Prepared Statement on Data Breaches and Identity Theft*, p. 10.

too weak would give companies an incentive not to disclose potentially harmful breaches. This concern could also apply to federal agencies. In congressional testimony last year, the executive director of the Center for Democracy and Technology argued that if an entity is not certain whether a breach warrants notification, it should be able to consult with the Federal Trade Commission.[23] He went on to suggest that a two-tiered system may be desirable, with notice to the Federal Trade Commission of all breaches of personal data and notice to consumers where there is a potential risk of identity theft. The Center for Democracy and Technology's comments regarding the Federal Trade Commission were aimed at commercial entities such as information resellers. A different entity—such as OMB, which is responsible for overseeing security and privacy within the federal government—might be more appropriate to take on a parallel role with respect to federal agencies.

Effective Notices Should Provide Useful Information and Be Easy to Understand

Once a determination has been made that a public notice is to be issued, care must be taken to ensure that it does its job effectively. Designing useful, easy-to-understand notices has been cited as a challenge in other areas where privacy notices are required by law, such as in the financial industry—where businesses are required by the Gramm-Leach-Bliley Act to send notices to consumers about their privacy practices—and in the federal government, which is required by the Privacy Act to issue public notices in the *Federal Register* about its systems of records containing personal information. For example, as noted during a public workshop hosted by the Department of Homeland Security's Privacy Office, designing easy-to-understand consumer financial privacy notices to meet Gramm-Leach Bliley Act requirements has been challenging. Officials from the FTC and Office of the Comptroller of the Currency described widespread criticism of these notices—that they were unexpected, too long, filled with legalese, and not understandable.

[23] Center for Democracy and Technology, *Securing Electronic Personal Data: Striking a Balance between Privacy and Commercial and Government Use* (Apr. 13, 2005), p. 7.

If an agency is to notify people of a data breach, it should do so in such a way that they understand the nature of the threat and what steps need to be taken to protect themselves against identity theft. In connection with its state law requiring security breach notifications, the California Office of Privacy Protection has published recommended practices for designing and issuing security breach notices.[24] The office recommends that such notifications include, among other things,

- a general description of what happened;
- the type of personal information that was involved;
- what steps have been taken to prevent further unauthorized acquisition of personal information;
- the types of assistance to be provided to individuals, such as a toll-free contact telephone number for additional information and assistance;
- information on what individuals can do to protect themselves from identity theft, including contact information for the three credit reporting agencies; and
- information on where individuals can obtain additional information on protection against identity theft, such as the Federal Trade Commission's Identity Theft Web site (www.consumer.gov/idtheft).

The California Office of Privacy Protection also recommends making notices clear, conspicuous, and helpful, by using clear, simple language and avoiding jargon and suggests avoiding using a standardized format to mitigate the risk that the public will become complacent about the process.

The Federal Trade Commission has issued guidance to businesses on notifying individuals of data breaches that reiterates several key elements of effective notification—describing clearly what is known about the data compromise, explaining what responses may be appropriate for the type of information taken, and providing information and contacts regarding identity theft in general. The

[24] State of California, *Recommended Practices on Notice of Security Breach.*

Commission also suggests providing contact information for the law enforcement officer working on the case as well as encouraging individuals who discover that their information has been misused to file a complaint with the Commission.[25]

Both the state of California and the Federal Trade Commission recommend consulting with cognizant law-enforcement officers about an incident before issuing notices to the public. In some cases, early notification or disclosure of certain facts about an incident could hamper a law enforcement investigation. For example, an otherwise unknowing thief could learn of the potential value of data stored on a laptop computer that was originally stolen purely for the value of the hardware. Thus it is recommended that organizations consult with law enforcement regarding the timing and content of notifications. However, law enforcement investigations should not necessarily result in lengthy delays in notification. California's guidance states that it should not be necessary for a law enforcement agency to complete an investigation before notification can be given.

During a recent public workshop on "Transparency and Accountability: The Use of Personal Information within the Government," hosted by the DHS Privacy Office, a panelist discussed the concept of "layering" notices to foster greater understanding and comprehension by consumers. Layering involves providing only the most important summary facts up front—often in a graphically oriented format—followed by one or more lengthier, more narrative versions in order to ensure that all information is communicated that needs to be. The panelist noted the pros and cons of lengthy, detailed notices versus brief, easier-to-understand notices. Specifically, long notices have the advantage of being complete, but this is often at a cost of not being easy to understand, while brief, easier-to-understand notices may not capture all the detail that needs to be conveyed. Multilayered notices were cited as an option to achieving an easy-to-understand yet complete notice.

[25] Federal Trade Commission, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business* (June 2004).

In addition, DHS workshop panelists from the Federal Trade Commission and the Office of the Comptroller of the Currency discussed the major findings of an interagency research project[26] concerning the design of easy-to-understand consumer financial privacy notices. The study found, among other things, that providing context to the notice (explaining to consumers why they are receiving the notice and what to do with it) was key to comprehension, and that comprehension was aided by incorporating key visual design elements, such as use of a tabular format, large and legible fonts, and appropriate use of white space and simple headings.

Although these panel discussions were not focused on notices to inform the public of data breaches, the multilayered approach discussed and findings from the interagency research project can be applied to such notices. For example, a multilayered security breach notice could include a brief description of the nature of the security breach, the potential threat to victims of the incident, and measures to be taken to protect against identity theft. The notice could provide additional details about the incident as an attachment or by providing links to additional information. This would accomplish the purpose of communicating the key details in a brief format, while still providing complete information to those who require it. Given that people may be adversely affected by a compromise of their personal information, it is critical that they fully understand the nature of the threat and the options they have to address it.

In summary, agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised, among which developing PIAs and ensuring that a robust information security program is in place are key. More specific practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal information, limiting data retention, limiting

[26] Kleimann Communication Group, Inc., *Evolution of a Prototype Financial Privacy Notice: A Report on the Form Development Project* (Feb. 28, 2006).

access to personal information and training personnel accordingly, and considering using technological controls such as encryption when data need to be stored on mobile devices. Nevertheless, data breaches can still occur at any time, and when they do, notification to the individuals affected and/or the public has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft. Care is needed in defining appropriate criteria if agencies are to be required to report security breaches to the public. Further, care is also needed to ensure that notices are useful and easy-to-understand so that they are effective in alerting individuals to actions they may want to take to minimize the risk of identity theft.

As Congress considers legislation requiring agencies to notify individuals or the public about security breaches, it should ensure that specific criteria are defined for incidents that merit public notification. It may want to consider creating a two-tier reporting requirement, in which all security breaches are reported to OMB, and affected individuals are notified only of incidents involving significant risk. Further, Congress should consider requiring OMB to provide guidance to agencies on how to develop and issue security breach notices to affected individuals.

Mr. Chairman, this concludes my testimony today. I would happy to answer any questions you or other members of the committee may have.

Contacts and Acknowledgements

If you have any questions concerning this testimony, please contact Linda Koontz, Director, Information Management, at (202) 512-6240, or koontzl@gao.gov. Other individuals who made key contributions include Idris Adjerid, Barbara Collier, John de Ferrari, David Plocher, and Jamie Pressman.

Attachment I: Selected GAO Products Related to Privacy Issues

Privacy: Key Challenges Facing Federal Agencies. GAO-06-777T. Washington, D.C.: May 17, 2006.

Personal Information: Agencies and Resellers Vary in Providing Privacy Protections. GAO-06-609T. Washington, D.C.: April 4, 2006.

Personal Information: Agency and Reseller Adherence to Key Privacy Principles. GAO-06-421. Washington, D.C.: April 4, 2006.

Information Security: Federal Agencies Show Mixed Progress In Implementing Statutory Requirements. GAO-06-527T. Washington, D.C.: March 16, 2006.

Information Security: Department of Health and Human Services Needs to Fully Implement Its Program. GAO-06-267. Washington, D.C.: February 24, 2006.

Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain. GAO-05-866. Washington, D.C.: August 15, 2005.

Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public. GAO-05-864R. Washington, D.C.: July 22, 2005.

Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements. GAO-05-552. Washington, D.C.: July 15, 2005.

Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights are Under Way. GAO-05-710. Washington, D.C.: June 30, 2005.

Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program. GAO-05-700. Washington, D.C.: June 17, 2005.

Electronic Government: Federal Agencies Have Made Progress Implementing the E-Government Act of 2002. GAO-05-12. Washington, D.C.: December 10, 2004.

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards. GAO-05-59. Washington, D.C.: November 9, 2004.

Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges, GAO-04-823. Washington, D.C.: July 21, 2004.

Data Mining: Federal Efforts Cover a Wide Range of Uses, GAO-04-548. Washington, D.C.: May 4, 2004.

Privacy Act: OMB Leadership Needed to Improve Agency Compliance. GAO-03-304. Washington, D.C.: June 30, 2003.

Data Mining: Results and Challenges for Government Programs, Audits, and Investigations. GAO-03-591T. Washington, D.C.: March 25, 2003.

Technology Assessment: Using Biometrics for Border Security. GAO-03-174. Washington, D.C.: November 15, 2002.

Information Management: Selected Agencies' Handling of Personal Information. GAO-02-1058. Washington, D.C.: September 30, 2002.

Identity Theft: Greater Awareness and Use of Existing Data Are Needed. GAO-02-766. Washington, D.C.: June 28, 2002.

Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards. GAO-02-352. Washington, D.C.: May 31, 2002.

Attachment 2: The Fair Information Practices

The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Ways to strike that balance vary among countries and according to the type of information under consideration. The version of the Fair Information Practices shown in table 1 was issued by the Organization for Economic Cooperation and Development (OECD) in 1980[27] and has been widely adopted.

Table 1: The Fair Information Practices

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.

[27] OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980). The OECD plays a prominent role in fostering good governance in the public service and in corporate activity among its 30 member countries. It produces internationally agreed-upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in the global economy.

Principle	Description
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organization for Economic Cooperation and Development.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

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

STATEMENT OF WILLIAM E. GRAY

Mr. GRAY. Chairman Davis, Representative Waxman and members of the committee, thank you for inviting me here this morning to discuss government data security at the Social Security Administration. As SSA Deputy Commissioner for Systems, I appreciate the opportunity to talk about the ongoing challenge of safeguarding the personal information that the public counts on us to protect.

As you know, Mr. Chairman, the Social Security Board's first regulation published in 1937 dealt with confidentiality of SSA's records. Our policies predate and are consistent with the Privacy Act, and while the technologies we employ to ensure the safety and privacy of our records has changed dramatically over the 70-year history of our program, our commitment to the American people and maintaining the confidentiality of our records has remained constant.

We nurture a security conscious culture throughout the agency from the executive level down. Every time an SSA employee logs on to his or her work station, and that includes the Commissioner of Social Security, a banner pops up warning that unauthorized attempts to access, upload or otherwise alter SSA's data are strictly prohibited and subject to disciplinary and/or criminal prosecution. In effect, every SSA employee sees that message every day he or she comes to work.

We use state-of-the-art software that carefully restricts our employees' access to data. Using this software, we ensure the employees only have access to the information they need to perform their jobs. The software allows us to audit and monitor the actions of individual employees, and it provides us with the means to investigate allegations of misuse.

Every year every SSA employee must read the Sanctions for Unauthorized Systems Access Violations, which we developed to secure the integrity and privacy of personal information contained in the computer systems. This memorandum advises SSA employees of the category of security violations and the minimum recommended sanctions. Annually, all employees are required to read and sign the acknowledgment statement indicating that they have read and understood the sanctions.

Our Flexiplace agreements require adherence to our information management in the electronic security procedures for safeguarding data and data bases. While each Flexiplace agreement is different, they share different basic requirements. The agreements generally contain provisions that require participating employees to maintain lockable storage for securing files at the alternate duty site. They also require participating employees to protect government records from unauthorized access, theft and damage in addition to requiring protection from unauthorized disclosure in accordance with the Privacy Act and other Federal laws restricting disclosure of the information we maintain.

A violation of the conditions set forth in the agreements results in disciplinary action. Penalties may range from reprimand to removal, depending on the seriousness of the violation.

Despite our best efforts in establishing policy and procedures and enforcing these procedures, no system of safeguards is immune from human error. We use these rare occurrences to review and strengthen our security precautions.

At SSA, our approach to data security is multi-faceted. It involved numerous policy and hardware and software safeguards. Even with all of the measures and safeguards we use, we cannot rest and be satisfied that we've plugged every hole. We continue to monitor, test, and evaluate what we are doing to prevent, detect and mitigate any potential threat. We strive to create and maintain a security conscious culture. We continue to try to stay abreast of all threats and vulnerabilities associated with emerging technologies, and our goal is to keep up with best practice approaches related to information security.

We have recently reemphasized with all employees the critical importance of safeguarding personal information, and we've directed managers to reinforce this point with their employees. In light of recent events, we are also conducting the review of our response procedures and protocols.

Mr. Chairman, Commissioner Barnhart and I recognize that data security is an ongoing challenge and critical component of our mission. We look forward to continuing to work with the committee to assure the American people that we are doing all that we can to maintain the security of the information entrusted to us.

Thank you for the opportunity to speak before this committee, and I am happy to answer any questions.

[The prepared statement of Mr. Gray follows:]

Statement of William E. Gray
Deputy Commissioner
Office of Systems
of the
Social Security Administration
Before the
Committee on Government Reform
June 8, 2006

Mr. Chairman and Members of the Committee, thank you for inviting me here today to discuss government data security at the Social Security Administration (SSA). Commissioner Barnhart and I place the highest importance on our information security program and are committed to securing and protecting Federal information. As SSA's Deputy Commissioner for Systems, I appreciate the opportunity to discuss our data security policies and procedures with you this morning.

At SSA we have always recognized the importance of protecting the security and privacy of the people we serve and ensuring the integrity and accuracy of the records we maintain. As you know, Mr. Chairman, the Social Security Board's first regulation, published in 1937, dealt with the confidentiality of SSA records. Our policies predate and are consistent with the Privacy Act. For more than 70 years, since long before the advent of computers and the technology age, SSA has honored its commitment to the American people in maintaining the confidentiality of our records. Our emphasis on privacy has led to a strong commitment in data security.

At SSA, we use a variety of inter-related, proactive measures to protect the information that the American public entrusts with us. These include physical security measures, Information Technology (IT) security measures, and training

and security protections for our employees. We have tried to put in place the authorities, the personnel, and the software controls to prevent penetration of our systems and to address systems security issues as they surface.

Prevention of Unauthorized Access

We use state-of-the-art software that carefully restricts user access to data. Using this software, only persons with a "need to know" to perform a particular job function are approved and granted access to specific kinds of data. All access to our mainframe computer is controlled through this matrix access process, also known as "Top Secret Services".

These systems controls not only register and record access, but also determine what functions a person can do once access is authorized. SSA security personnel assign a computer-generated personal identification number and an initial password to persons who are approved for access (the person must change the password every 30 days). This allows SSA to audit and monitor the actions individual employees take when using the system. These same systems provide a means to investigate allegations of misuse and have been crucial in prosecuting employees who misuse their authority.

Additionally, we have implemented processes to scan, at least once a month, every SSA workstation (over 100,000), every telephone, and every systems platform for compliance with Agency standards. I believe that our record in preventing intrusions demonstrates our success in implementing an Enterprise-wide security program that is second to none.

Prevention of unauthorized access is enhanced by risk assessments, systems penetration testing, physical safeguards, and independent audits and reviews.

Human Capital

We nurture a security-conscious culture throughout the agency from the executive level down.

For instance, every time any SSA employee, and that includes the Commissioner of Social Security, logs onto his or her workstation, a banner pops up warning that only authorized users can access the system; that the system is a United States government computer system subject to Federal law, and that unauthorized attempts to access, upload, or otherwise alter SSA's data or programming language are strictly prohibited and subject to disciplinary and/or civil action and criminal prosecution. In effect, every SSA employee sees that message every day he or she comes to work.

And as you may know, every year, every SSA employee must read the Sanctions for Unauthorized Systems Access Violations (Sanctions) which we developed to secure the integrity and privacy of personal information contained in the Agency's computer systems. This memorandum advises SSA employees of the categories of systems security violations and the minimum recommended sanctions. These sanctions apply for all SSA employees who use or have access to computer systems containing personal data about workers, claimants, beneficiaries, SSA employees or other individuals. Annually, all employees are required to read and sign the Acknowledgment Statement indicating that they have read and understand the sanctions. The Sanctions and Acknowledgment Statement have both been incorporated into the Information Systems Security Handbook.

We are also very serious about training. We provide security awareness training to all of our employees (including contractors) and specialized in-depth training for those with significant IT security responsibilities. Contractors are required to possess security credentials, and have the expertise and training appropriate to the functions they will be performing before they are permitted to perform services under a contract.

In addition, we have networks of full-time staff devoted to systems security stationed throughout the Agency. These front-line employees provide day-to-day oversight and control over our computer software in headquarters and centers for security and integrity in each SSA region.

IT Security Measures

We closely follow Federal guidelines including security standards and guidelines issued by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget. We incorporate these standards and guidance into Agency policy for information security and the related Certification and Accreditation (C&A) of our major IT systems. The C&A process is a major part of our efforts to maintain and strengthen our systems controls.

And as we reported to you this past March, we use the Federal Information Security Management Act (FISMA) reporting process as an important indicator of how the agency's information technology assets and resources are being protected. SSA submitted our report for fiscal year 2005 to OMB on October 7, 2005. A few of the major highlights of our report are especially relevant to today's discussion. For example, we reported to you that
all twenty of our major information systems are currently certified and accredited. We follow documented policies and procedures for identifying and reporting incidents of security weakness and use a combination of automated tools, system monitoring tools and network-penetration type reviews to protect all 20 of our information systems. And, as required by NIST, SSA provides monthly incident reports to the United States Computer Emergency Readiness Team.

Flexiplace at SSA

Consistent with May 2003 guidance from the Office of Personnel Management (OPM), we have a flexiplace program in place at SSA that we are now obligated to maintain under our collective bargaining agreements. All participating employees are required to sign, and abide by, their individual component's negotiated Flexiplace Program Participant Agreement. Of our current workforce of 64,000 employees, 4,400 have signed flexiplace agreements. These agreements require adherence to applicable government regulations in place at SSA governing information management and electronic security procedures for safeguarding data and data bases. While each flexiplace agreement is different, they share certain basic requirements. Regarding security, the agreements generally contain provisions that:

- require participating employees to maintain lockable storage for securing files at the alternate duty site;

- require participating employees to protect government records from unauthorized access, theft, damage in addition to requiring protection from unauthorized disclosure in accordance with the Privacy Act and other federal laws restricting disclosure of the information we maintain; and

- allow for management inspection of the alternate duty station with 24 hours advance notice to the employee.

A violation of the conditions I have just laid out results in disciplinary action. Penalties may range from reprimand to removal, depending on the seriousness of the violation. Despite our best efforts in establishing policy and procedures and in enforcing these procedures, no system of safeguards is immune from human error. We use these rare occurrences to review and strengthen our security precautions. Recently a laptop computer owned by an SSA employee

was stolen from a conference the employee was attending. The laptop contained copies of decisions the employee had written as part of his assigned work when he worked at home. There were approximately 200 files on the laptop that were stolen and these files contained the names, Social Security numbers and other personal information pertaining to these individuals. While the investigation is still underway, we have taken steps to notify the individuals whose files were contained on the laptop and to monitor the SSNs to ensure no suspicious activity has occurred on SSA's records. This employee, although authorized to work at home, violated SSA security procedures by failing to properly secure sensitive information on the laptop, and by taking it to a non-secure location.

Detection of SSN Misuse

As recent experience makes clear, despite government's best efforts to protect data, breaches do occur. So I would like to turn now to a discussion about detecting SSN misuse.

One way that a person can find out whether someone else is misusing their number to work is to check his or her earning records. About three months before their birthday, anyone 25 or older and not already receiving Social Security benefits, automatically receives a Social Security statement each year. The statement lists earnings posted to their Social Security record and provides an estimate of benefits and other Social Security facts about the program. If there is a mistake in the earnings posted the individual is asked to contact us right away, so the record can be corrected. We investigate, correct the earnings record and if appropriate, we refer any suspected misuse of a Social Security number to the appropriate authorities.

SSA may learn about misused SSNs in a variety of other ways including alerts from our computer systems while matching Federal and State data, processing wages, claims or post entitlement actions, reports from individuals contacting our field offices or teleservice centers and inquiries from the Internal Revenue Service concerning two or more individuals with the same SSN on their income tax returns.

We have another tool that has been used successfully to detect instances of fraud and abuse. This tool, called the Comprehensive Integrity Review Process (CIRP), is a review and anomaly detection system. Known fraudulent patterns are first identified and then transactions that fit these fraudulent patterns are provided to SSA managers for their review. If upon investigation, the SSA manager believes that fraud or misuse has occurred, they prepare a referral to the Inspector General (IG).

As I have tried to make clear today, our approach to data security is multi-faceted, and involves numerous policy, hardware and software safeguards. However, even with all the measures and safeguards we use, we cannot rest and be satisfied that we have plugged every hole. The challenge is to keep ahead of threats with an intense and responsive security program. We continue to monitor, test and evaluate what we are doing to prevent, detect, and mitigate any potential threat. We strive to create and maintain a security conscious culture; we continue to try to stay abreast of all threats and emerging technologies and vulnerabilities associated with those technologies, and our goal is to keep up with "best practice" approaches related to information security. We have recently reemphasized with all employees the critical importance of safeguarding personal information, and we have directed managers to reinforce this point with their employees. In light of recent events, we are also conducting a review of our response procedures and protocols.

Conclusion

Mr. Chairman, Commissioner Barnhart and I, along with all of the senior executives at the Social Security Administration, recognize data security is an ongoing challenge and critical component of our mission. We know we must be vigilant in every way to assure that an individual's personal information remains secure, taxpayer dollars are protected, and that public confidence in Social Security is maintained. We look forward to continuing to work with the Committee to assure the American people that we are doing all we can to maintain the security of the information entrusted to us.

Thank you for the opportunity to speak before this committee and I am happy to answer any questions.

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

STATEMENT OF DANIEL GALIK

Mr. GALIK. Good morning, Mr. Chairman, Mr. Waxman and members of the committee. I am pleased to be with you this morning to discuss IRS's efforts relative to information technology security and the privacy of both employee and taxpayer information. Commissioner Everson regrets that he could not be here today as he is out of the country on travel that was scheduled several weeks ago.

Taxpayer and employee privacy is of foremost concern to the IRS. We are charged with protecting the most critical information about virtually every American. Taxpayer data is subject to much higher statutory protection and safeguards. IRS's security policy guidance requires the mandatory use of encryption to protect all taxpayers and other sensitive, personally identifiable information that may be contained in IRS's computer systems. We continue to update our systems and our training so that employees who have access to sensitive information are aware of the steps they must take to prevent that information from being compromised.

This job has never been tougher, specifically in an agency like the IRS. We have more than 82,000 full-time and 12,000 part-time employees. We also have a large mobile work force that utilizes laptops and other portable storage devices, and they are authorized to have taxpayer and sensitive information with themselves at locations outside of IRS office space.

By focusing on both privacy and security, we have made significant progress in upgrading our system to respond to the security challenges we face in this new age. Consider the following: We have achieved the green status on the President's management agenda fiscal year 2000 scorecard with over 90 percent of our major systems having successfully completed security certification and accreditation. In early 2004, very few of the IRS's major information systems had not completed security accreditation.

We make use of a defense and security approach with over 100 firewalls and several intrusion detection devices on our computer systems. We operate our own computer security incident response center that monitors all network activity 24 hours per day. There is no evidence that any IRS systems, including the master files of all taxpayer data, have ever been successfully penetrated or compromised by external attacks. Cracking our system requires more than bypassing a single barrier. All IRS computers are equipped with multiple data protection tools that allow IRS users to encrypt all IRS taxpayer data and all other sensitive information that they may have on their computers, including their laptops.

In light of the incident at the VA, the IRS is aggressively reviewing all policies, processes and training to ensure IRS users know how to use the encryption tools and are aware of the penalties of violation of policies. It is important to note that the laptops used by all IRS personnel working in the field are equipped with software applications that automatically encrypt all taxpayer and other personal and sensitive information.

We have also been proactive not only in the area of security but also on our commitment to privacy. Almost 1 year ago we implemented OMB to designate senior officials to privacy. Despite all of this we know that we are still vulnerable to computer theft and loss, especially since our agents need to use laptops in the performance of their duties outside of IRS premises.

For example, recently an IRS employee checked a laptop as checked baggage on a commercial air flight. The laptop did not make it to the proper destination. We determined that the laptop contained the names, Social Security numbers and dates of birth of 291 IRS job applicants and employees. We reported this security breach to our Inspector General and law enforcement, which are currently conducting an investigation. We have attempted to call each of the individuals as information was on the laptop, and we also sent a letter to inform them of the missing data and to guide them on how to watch for suspicious activity. We are also taking additional steps to ensure this does not happen again.

In summary, Mr. Chairman, we at the IRS take privacy and security of both taxpayer and employee information as one of our highest priorities. We have taken numerous steps to make sure that our systems are not breached, but because so much of our work is done offsite we have a heavy reliance on laptops and other portable mass storage devices. While we remain vulnerable to one of those devices being lost or stolen, we are making every effort to ensure that any data on such a device is encrypted and of no use to anyone.

The Treasury Department and IRS look forward to continuing to work with the committee to ensure we are doing everything possible to protect taxpayer information and privacy.

I appreciate the opportunity to appear today. I'll be happy to answer any questions.

[The prepared statement of Mr. Galik follows:]

Testimony of Daniel Galik
Chief, Mission Assurance and Security Services
Internal Revenue Service
Before the
House Committee on Government Reform
June 8, 2006

Good morning Chairman Davis, ranking Member Waxman and members of the Committee on Government Reform. My name is Dan Galik. I am the Chief of Mission Assurance and Security Services (MA&SS), and serve as the Chief Security Officer for the Internal Revenue Service. I am pleased to be with you this morning to discuss IRS's efforts relative to information technology (IT) security and the privacy of both employee and taxpayer information.

Taxpayer and employee privacy is a foremost concern of the IRS. We are charged with protecting the most critical information about virtually every American. In recognition of this responsibility, we continue to update our systems and our training so that employees who have access to sensitive information are aware of the steps they must take to prevent that information from being compromised.

This job has never been tougher. According to the FBI, identity theft is one of the fastest growing White Collar crimes. There has been a 4,600 percent increase in computer crime since 1997. Nearly 20 million Americans lost their identities over the past two years, according to the Federal Trade Commission. Deloitte-Touche recently reported that financial institutions and U.S. banks have also experienced a significant increase in the number of computer based attacks and attempted intrusions into financial systems.

Contrast that with the job of the IRS. Every year, we process approximately $2 trillion in revenues to fund the U.S. operating budget. Although the majority of this is collected in an automated banking system throughout the year, about $300 billion is collected through 8 IRS campuses where taxpayers send their tax returns for processing. We house computing systems that hold data on all taxpayers and also process enormous volumes of paper data in our more than 500 offices across the country. We have more than 82,000 full time and 12,000 part-time employees across the U.S.

As a result, protecting all of this information has simultaneously become both more important and more difficult. Imagine if you will a chain with each link representing some element of information security such as security policies and processes, training, or the use of encryption mechanisms. It is a cliché to say we are no stronger than our weakest link, but it is true. Those seeking to unlawfully access this data have the ability to attack our weakest link. Perhaps the strongest asset that IRS deploys in trying to counter information security breaches is our layered "defense in depth" concept. In short, attackers must defeat multiple security protection layers to get to our data.

I would be disingenuous if I did not say that what happened at the Department of Veterans Affairs (VA) has probably caused everyone in my position in the Federal government to take a second look at all of the policies and procedures in place to prevent a similar incident for our agency. And, regardless of how rigorous our programs or how much training we conduct, it can still happen.

We recently had an incident at the IRS where an employee, heading to a job fair, checked a carrying case as luggage on a commercial flight. The carrying case contained a laptop computer and an accompanying finger print scanner. The laptop contained the fingerprints and some personal data on 291 IRS employees and job applicants. The information contained on the laptop was limited to information job applicants provide and included the name, date of birth, social security number, and physical characteristics of the applicant (height, weight, hair color, etc.). There were no electronic tax records or financial information on the laptop. The laptop was lost in transit and has not been recovered.

According to our procedures, this was reported to the Treasury Inspector General for Tax Administration (TIGTA), which is currently conducting an investigation. The airlines and other federal officials are also investigating. In addition, we contacted each of the individuals whose information was on the laptop by phone and by letter to inform them of the missing data and to guide them on how to watch for suspicious activity. We are now reviewing and refining our procedures for handling fingerprint equipment to reduce the possibility of this happening in the near future. We are also working with the provider of the fingerprint equipment in installing encryption capabilities. Later in my testimony, I will discuss the encryption procedures we plan to implement for laptops. This morning, I want to describe to you the steps we have taken and are taking to protect sensitive data. First, however, I think it is important for you to better understand the security environment in which the IRS operates.

Mission Assurance and Security Services

Under the IRS Restructuring and Organization Act of 1998 (RRA), our agency was essentially divided into two distinct units. One unit focuses on service and enforcement and represents the primary point of contact between the IRS and all taxpayers. The other unit focuses on operations support for the agency. In essence, the Operations Support unit, of which MA&SS is a part, provides the tools for the Services and Enforcement division to do its job. As the chief of MA&SS, I report directly to the Deputy Commissioner for Operations Support.

MA&SS is a service and support organization. It assists all IRS Operating Divisions in maintaining secure facilities, technology, and data. We provide the operational support to enable an integrated approach to information protection by combining physical, information technology, and personnel security as well as privacy. We do so by providing overall IRS security and privacy leadership and promoting collaborative security planning and decision-making with all IRS organizations.

MA&SS brings together previously separate security functions to enable a consistent and unified approach to security and privacy. The MA&SS organization is matrixed to enable an integrated approach to meeting security needs. Five core programs – Information Technology Security, Physical Security, Emergency Preparedness, Personnel Security, and Privacy – shape the direction of services and initiatives.

For the purposes of this hearing, I will focus my attention on two of these programs: Information Technology (IT) and Personal Security and Privacy.

Information Technology Security

Our Information Technology Security Program Office is charged with identifying and mitigating threats, establishing policy and standards, determining strategy and priorities, and monitoring program implementation. In addition, the office provides customers with the tools, advice, security engineering, and tactical guidance necessary to ensure IT security is properly addressed in the development and operations of all IRS information systems.

Title III of the E-Government Act, entitled Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information systems that support the operations and the assets of the agency. As required by FISMA, the IRS has implemented an agency-wide information technology security program which includes following key elements:

- Periodic assessments of risk;
- Policies and procedures that are based on risk assessments;
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems as appropriate;
- Security awareness training to inform personnel (including contractors) of the information security risks associated with their activities and their responsibilities in complying with IRS policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices and security controls;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures and practices of the IRS;
- Procedures for detecting, reporting and responding to security incidents; and

- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets.

The IRS IT Security Program efforts in 2004 and 2005 were focused on the accomplishment of security certification and accreditation of the IRS network infrastructure systems, which was achieved at the end of FY 2005. The top priority in FY 2006 has been on achieving security certification and accreditation for our major applications, using new process guidance issued each year by the National Institute of Standards and Technology (NIST). As a result, over 90 percent of our major systems having successfully completed security certification and accreditation. (Of note, in early 2004, very few of the IRS' major information systems had completed security accreditation). The IRS will continue to aggressively pursue the correction of the computer security material weaknesses and implementation of the corrective plans that address those weaknesses. The IRS is implementing an enterprise-wide risk management approach that cost-effectively focuses resources on major systems and assets that directly support the most critical business processes supporting tax administration. While we have made significant progress towards implementation of a FISMA compliant IT Security program at the IRS, we anticipate that progress continuing in 2006 and 2007 as we transition to high quality certification and accreditation packages for all IRS systems. With the increased recent attention on privacy and identity theft, the IRS is ensuring that proper management, operational, and technical security and privacy controls are enhanced for existing legacy infrastructure systems, and also built into the designs for all new tax modernization systems.

The day-to-day security status of the entire IRS network and computer operations are continuously monitored by a world class 24X7 Computer Security Incident Response Center (CSIRC). The IRS CSIRC provides proactive prevention, detection, and response to computer security incidents targeting the IRS' enterprise IT assets. The CSIRC is equipped to identify, contain and eradicate cyber threats targeting IRS computing assets. The four major CSIRC operational functions of prevention, detection, response and reporting meet FISMA requirements for incident response and reporting. IRS IT security technical efforts have focused on "hardening" computer and network infrastructure systems to make them resistant to external attacks. We believe there have been no successful penetrations into any IRS systems by hackers. The IRS has deployed the security "defense-in-depth" approach with over 100 firewalls and several hundred intrusion detection devices, with all of these devices monitored by the CSIRC. Anti-virus software is deployed throughout the network, and the latest security patches and required updates are aggressively pushed out to all desktops.

All IRS computers are equipped with multiple data protection tools that allow all IRS users to encrypt all taxpayer data, personally identifiable information, and all other sensitive information. In light of the incident at the VA, the IRS is aggressively reviewing all policies, processes, and training to ensure IRS users know how to use the encryption tools, are familiar with the associated data protection and privacy policies, and are aware of the penalties for violation of the policies. The primary focus right now is on the large IRS mobile workforce that utilizes laptops and other portable storage devices

working at locations outside of IRS office space. Currently available encryption tools on all IRS computers provide the capability for at least double encryption, and double password protection. The IRS also has the capability to encrypt all sensitive emails. This ultimately provides triple encryption capability and triple password protection for users who utilize both secure email and the other available encryption solutions that are installed on IRS computers. The use of multiple security protection mechanisms enables the IRS to focus increased attention on our internal security controls, to prevent any potential compromises that could occur from an attack by an "insider." The use of the multiple encryption capabilities also prevents or effectively mitigates the loss of any sensitive data, should the user's laptop be stolen, lost, or misplaced. It is important to note that IRS revenue agents in the field utilize software programs that automatically encrypt taxpayer data on the hard drives of their laptops.

The IRS is pursuing the deployment of an enterprise-wide automated security encryption solution for use by all IRS staff. By automatically encrypting all user data files, it removes the challenges faced by typical computer users who may often forget to encrypt sensitive data, or who may not realize that the data they are working with is in fact sensitive. With all taxpayer data files and files that may contain sensitive and personally identifiable information all being encrypted, the IRS will be in a position to mitigate any threats posed by insiders.

The IRS also utilizes a number of software programs that monitor and audit the behavior of the authorized users of IRS tax processing systems. The Integrated Data Retrieval System (IDRS), the System Audit Analysis System (SAAS), and the IRS Internet Misuse and Monitoring Program, all monitor the activities of our users with specific focus on any unauthorized activities, such as attempts to improperly access any taxpayer data.

Office of Privacy and Information Protection

The mission of the Office of Privacy and Information Protection (OP&IP) focuses on enabling taxpayer and employee confidence by ensuring the right people, see the right data, in the right places, for the right reasons. OP&IP achieves this mission by incorporating taxpayer and employee privacy controls and privacy principles of Notice, Choice, Access, Business Purpose, and Data Minimization into IRS systems and business processes. These principles can be generally summarized as "*any information collected about an individual should be the minimum necessary to complete the business at hand and individuals should have access to and notification and choice of the use to which their information is put in order to prevent data inaccuracy and misuse*." This office also ensures that the public is aware of IRS privacy business practices and that IRS programs and projects only gather the taxpayer and employee data necessary to accomplish the Service's objectives. It creates, promotes, and supports privacy awareness Servicewide. The IRS OP&IP begins where the law leaves off, by going the extra step to protect privacy by embedding privacy into IRS systems and business processes and establishing privacy as an agency core value.

Within OP&IP there are a number of subordinate organizations, the IRS Privacy Program the UNAX Program, the Safeguards Program, and the Homeland Security Presidential Directive-12 (HSPD-12) Program Management Office. Today, I will speak on the Privacy, UNAX, and the Safeguards Programs.

The Privacy Program ensures the legal and regulatory privacy requirements are not only met, but exceeded by operationalizing privacy principles through policy, assurance, and awareness programs. The IRS created the Privacy Impact Assessment (PIA) in the early 1990's as a means of identifying privacy risks and vulnerabilities imbedded in IRS systems. The PIA process was identified by the Federal Chief Information Officer Council as a best practice and adopted into law as part of the e-Gov Act of 2002 as the government-wide standard on how to ensure privacy controls throughout the business lines. Specifically, the PIA:

- Ensures handling of personally identifiable information (PII) conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determines the risks and effects of collecting, maintaining and disseminating PII in an electronic information system; and
- Examines and evaluates protections and alternative processes for handling PII to mitigate potential privacy risks

We integrate the multiple privacy and confidentiality requirements of the Privacy Act, the e-Gov Act, and Internal Revenue Code into a single program area to increase taxpayer and employee confidence in the way IRS handles personal information.

The OP&IP has expanded its scope to include the Unauthorized Access (UNAX) Program. The mission of the UNAX Program is to provide awareness to all IRS employees to ensure that employees do not compromise public confidence in our protection of tax account information in accordance with the Taxpayer Browsing Protection Act of 1997. The UNAX Program also tracks allegations of violations and works with the Human Capital Office, business program areas, and the Treasury Inspector General for Tax Administration (TIGTA) to investigate and take appropriate action, which can range from no finding of violation to termination and potential criminal charges. All IRS employees must receive the UNAX briefing and certify that they received the briefing annually. New employees must do the same within the first 30 days of their Entry on Duty (EOD) date or before being given access to taxpayer information, whichever is sooner. Seasonal employees and employees returning from extended leave, who did not certify to having received the briefing during the mandatory briefing period (May 2 - September 30 each year), must complete the UNAX briefing and certify that they received the briefing within the first 30 days of their Return to Duty date. Before being eligible to access any taxpayer information, an employee returning to duty after having a UNAX disciplinary action must complete the UNAX briefing and certify to having completed the briefing within 3 workdays of returning to duty.

The Safeguards Program provides oversight to external agencies in protecting federal taxpayer information and to internal customers in protecting taxpayer information,

employee information and other official use only information for contracting purposes. This office ensures that Federal, State and Local Agencies authorized to receive federal taxpayer information under various sections of Internal Revenue Code (IRC) Section 6103 are protecting the data in accordance with policy and legal requirements. On-site reviews are conducted at these Federal Agencies, State Welfare, Child Support, Revenue and local taxing authorities within a three-year cycle and reports issued to notify the agencies of any recommendations. In addition, Safeguard staff also conduct sensitive but unclassified contract document reviews for IRS contracts and acquisition documents to ensure that the legal and safeguards policy provisions are in place to protect taxpayer information.

Identity Theft

The IRS recognizes that taxpayers expect the IRS to safeguard personal information and provide timely resolution of identity theft related cases. To this end, about 18 months ago we began an aggressive strategy to research and address this growing problem. We established an Identity Theft Program Office charged with implementing the IRS' policy statement on identity theft. This Policy requires the IRS to take the necessary steps to provide assistance to victims of identity theft within the scope of their official duties.

Our Identity Theft Program Office works with offices throughout the IRS to implement the agencies' Identity Theft Enterprise Strategy comprised of three components—Outreach, Prevention and Victim Assistance. While the IRS took a number of immediate steps to address our strategy, we also recognized the importance of identifying and quantifying all of the material risks associated with identity theft at the agency.

As a result, in October 2005, we began a comprehensive Identity Theft Risk Assessment. Our analysis identified the potential for identity theft from both an external (impact to the IRS from an outside source) and internal (impact of an internal security breach) perspective. It also included a round table discussion with subject matter experts from financial institutions and fraud specialists to identity and leverage industry best practices and lessons learned. Working together we have developed remediation strategies which focus on encryption, enhancements of the IRS computer security and enhancing the current IRS computer security incident reporting system to specifically focus on identity theft Incident reporting, in order to better identify and track the disposition of identity theft incidents. While research shows that the IRS has one of the lowest instances of identity theft, we take this situation very seriously. We have made significant progress, but additional work remains---including implementing additional mediation strategies and conducting in-depth analyses of the remaining high-priority processes.

Being Proactive

One of the keys to protecting sensitive data is to be as proactive as possible. I have already referenced the review of our identity theft prevention procedures which we initiated 18 months ago.

In addition, as necessary, I personally notify business units with updates on security threats. For example, a year ago, I issued a memorandum in which I discussed information technology security guidance for the use of portable mass storage devices, such as flash disks, pen drives, key drives and thumb drives. These devices can be used to store a gigabyte of taxpayer information and other sensitive privacy information, but yet are so small as to make them more vulnerable to loss and theft.

I informed employees that if these devices are used to hold sensitive data that the data files must be encrypted using IRS approved encryption software. Furthermore, the devices should have no additional software/firmware beyond storage management and encryption. If an office has the need to use a portable mass storage device having an integrated central processing unit and other software applications, then it is subject to established security certification and accreditation processes.

We are also making an aggressive push for use of encryption solutions on all laptops. As discussed above, all users currently have the capability to encrypt all sensitive information. All of IRS's revenue agents have software that automatically encrypts the sensitive taxpayer information they might have.

One of the key initiatives that should serve to effectively mitigate the impact of any incidents of data loss involving IRS systems is the effort to field commercial security encryption solutions that will automatically encrypt all user data on IRS computers. We hope to have that fully deployed to all IRS laptop users within six months.

In addition, we have been proactive not only in the area of security but in our commitment to privacy as well. Almost one year ago, we took the initiative to implement OMB's directive to designate a Senior Agency Official for Privacy. Following the incident with the VA data loss, we have implemented OMB's directive to have our Senior Official for Privacy conduct a review of our policies and processes. This review will address all administrative, technical, and physical means used by IRS to control sensitive information, including but not limited to, procedures and restrictions on the use or removal of personally identifiable information beyond agency premises or control.

In addition, the Department of Homeland Security (DHS) and the Treasury Department have issued revised security incident reporting guidance and are working on implementing that revised guidance.

In terms of the reporting of loss or theft of IRS equipment or data, we are in a somewhat unique position. TIGTA provides independent oversight of IRS activities by conducting audits and investigations involving IRS programs and operations If an employee loses any IT equipment, as happened in the recent instance, he/she must report it to his manager who shall insure that the incident is reported to the Computer Security Incident Response Capability (CSIRC) and to TIGTA. These incidents are also reported to the Department of the Treasury and through Treasury to the Department of Homeland Security as appropriate. The report must include whether the sensitive data is encrypted. For incidents involving the potential loss of employee information, taxpayer information,

or other sensitive information, follow-up reports are made by the manager until the incident is resolved by TIGTA or the IRS.

Conclusions

Mr. Chairman, in conclusion, I would like to emphasize the following points:

- Privacy and information security are a growing concern in virtually every organization, both public and private;
- As technology advances, our ability to protect sensitive information must advance as well to meet new threats;
- The IRS is committed to the highest standards of protection for both sensitive taxpayer data as well as personally identifiable information;
- We have in place a robust program that focuses on security in information technology and privacy;
- We have adopted the layered "defense in depth" approach to our security defenses forcing any attacker to defeat multiple layers of security to get to our data.
- We believe the expanded use of automated encryption solutions will be a major technical component of our comprehensive strategy to effectively counter the threats posed by potential data losses
- We have attempted to be proactive in addressing potential security threats;
- We are complying fully with recent directives issued by OMB to review our policies and procedures to ensure the IRS has adequate safeguards to prevent the misuse or unauthorized access to personally identifiable information;
- In the event an incident occurs where equipment of data is lost, we refer the matter to TIGTA for investigation;
- Our biggest challenges seem to be more in the effective implementation of existing security and privacy policies and processes, and training the staff to make use of security tools and capabilities that already exist on IRS computers: and
- Despite all of our progress that we have made, as TIGTA reminds us in their audits, we continue to have significant work to do.

I appreciate the opportunity to appear and I will be happy to respond to any questions.

Chairman TOM DAVIS. I want to thank all of you very much.

Twenty-six million veterans' records, a million active duty records, 300 tax records. And I am just troubled with the number and the scope of losses. We have a lot of laws protecting secure information. Personal information really seems to fall into a different category and maybe we have to give it, you know, rethink how we deal with this.

To all of you, I guess I'd ask, what assurances can you give this committee and the American public that personal and sensitive data in Federal IT systems are secure to access, control staff are being trained in security practices and the breaches will be detected quickly and those responsible for sloppy data handling will be punished?

Mr. JOHNSON. The question is what assurances can we give? We need to give them a greater level of assurance than they have now obviously. OMB needs to be held accountable for ensuring that all agencies have plans that they deem acceptable, that OMB and Congress deems acceptable and they implement this plan and they do what they say they are going to do, and there are various ways of doing that: Reporting mechanisms, details of reporting, frequency of reporting. There are a lot of mechanisms for doing that.

I think we are doing more and more of that with the present agenda. A lot of our government-wide initiatives, security clearance reform. Where we are doing a better and better job of holding agencies accountable is for implementing some new way of doing business and we need to employ that here to everybody's satisfaction. We need to make sure we have a plan, agencies have a plan to do what's the right thing and that they then follow through and implement that plan as promised.

Chairman TOM DAVIS. I mean, Secretary Nicholson, you came in with your plan of what you were trying to do proactively to prevent this in your agency. Let me ask for the employee who was involved, he's terminated at this point; is that correct?

Secretary NICHOLSON. That's correct.

Chairman TOM DAVIS. What was the lag time of when this was stolen and when he notified his superiors? Do you know?

Secretary NICHOLSON. He notified his superiors the day that he discovered that it had been stolen.

Chairman TOM DAVIS. OK. And did they—how long did it take to get to you?

Secretary NICHOLSON. Thirteen days.

Chairman TOM DAVIS. OK. Obviously you are dealing with that in your Department, aren't you.

Secretary NICHOLSON. Yes, sir.

Chairman TOM DAVIS. We don't know what is out there, but time is critical in a case like this. Have the police department, the local police department been involved in any leads on—have they put any pressure into this knowing what's at stake?

Secretary NICHOLSON. Yes. It's a well-known fact this happened in Montgomery County, MD, and the local law enforcement people turned to it immediately.

Chairman TOM DAVIS. There are a series of burglaries in that area.

Secretary NICHOLSON. There were a series of burglaries with the same pattern, and they believe that these were young burglars whose goal was to get computers and computer peripheral equipment from other houses like they did this house. They took laptops and hard drives, overlooked other sort of valuable or semi-valuable things to get this computer equipment. They further think that their MO is to take these things, clean them up, actually to erase them and fence them into a market for college campuses and high schools where they pick this stuff up pretty cheap. We have no assurance of that.

Chairman TOM DAVIS. All right.

Secretary NICHOLSON. By the way, the FBI is intensely involved now, as our Inspector General. They have had a few leads. They've apprehended a few people who have committed these burglaries but they didn't have—we have the serial numbers of this equipment and we checked it against some of the equipment but it didn't match.

Chairman TOM DAVIS. But the answer is the locals with Federal help now have intensified what would have been a routine investigation. I want to be assured that we are doing everything at all levels to try to close this out. That would be the win/win if we could close this out, find the perpetrators, find the missing disks and be able to bring this to closure.

Secretary NICHOLSON. Indeed.

Chairman TOM DAVIS. Data breach laws at the State level which require companies to inform individuals whom the organizations exposes a breach of their personal information have really improved our understanding of this problem. Congress is carrying a national breach standard, but currently there is no requirement to notify citizens in the case of a breach, the Federal agencies notify when a breach of personal information occurs on a Federal Government data base, and what, if any, guidelines exist to determine if a breach requires a notification? How do you determine what's trivial, and General Walker, do you have any thoughts on that and should we consider a Federal agency breach notification law?

Mr. WALKER. The answer is yes, I think you should consider a Federal agency breach notification law, one that would require notification of affected individuals as well as notify OMB to obtain an understanding of what might be going on on a government-wide basis. I think one has to be careful to make sure that you do have some criteria laid out to meaningfully differentiate between certain events that don't represent a real risk of identity theft. For example, there may have been something that was misplaced for a short period of time that's been recovered. Obviously, that's not something you want to have a broad based notification on. And we would be happy to work with this committee to come up with some potential criteria. But yes, it is something you need to consider.

You may well also want to consider whether or not you want to require agencies to have certain things. For example, to restrict access to certain sensitive information, to have mandatory training and monitoring with regard to individuals who do have access to certain reporting requirements, which we just talked about; and you may also want to think about whether or not there need to be tougher sanctions here than might exist under current law.

Chairman TOM DAVIS. Thank you.

Mr. GRAY. I wanted to say under Social Security if there's a data breach, we would always notify. It is part of our policy to notify the claimant and work with them.

Chairman TOM DAVIS. Mr. Sanders.

Mr. SANDERS. Thank you very much for holding this important hearing. Before I get into the thrust of the issue today I did want to respond to something Secretary Nicholson said. We talked about the improvements in VA health care and I concur with you. But, Mr. Secretary, remember just last year your administration denied VA health care access to over 250,000 priority 8 veterans, including those who had fought in World War II. You wanted to raise—double the cost of prescription drugs for our veterans. You also wanted to increase fees substantially, which would probably have thrown hundreds of thousands of other veterans of VA health care and the veterans organizations also understand that the Bush administration is significantly underfunding the VA and the needs of our veterans.

Now in terms of this issue today, it is really difficult to imagine with all of the money we spend on security at the Federal level every year how what appears to have been a garden variety burglary in suburban Maryland could result in a breach of the personal information of over 26 million American veterans, including, it appears, over 2 million American military personnel.

You know we have about 300 million people in our country. What we are looking at is a breach of privacy for approximately 10 percent of the American population, and if you look at the adult population it is probably 15 or 20 percent, at one time, an unprecedented and extremely dangerous breach of privacy for tens of millions of Americans.

According to a variety of experts quoted in yesterday's Washington Post, this breach could enable the holder of this information to, "create a zip code for where each of the service members and their families live and if it fell into the wrong hands could potentially put them at jeopardy of being targeted."

These experts, including those at the Center for Strategic and International Studies, have expressed concern that this released information could, "reach foreign governments and their intelligence services or other hostile forces, allowing them to target their service members and families."

One anonymous Defense official quoted in the Post called the extent of the battle, "monumental."

This is serious business. I think we all understand that.

Mr. Waxman and Mr. Davis have raised some very important issues. Mr. Secretary, my question for you is, it is obvious, I think there is no disagreement here, that we have to make sure that this never happens again. We have to do a much, much better job in protecting the privacy in the records of all of the American people, including those in the military and our veterans, but this is my question for you.

After all is said and done, after hopefully we do all of these things, if—and we certainly hope this does not happen—if there is a breach of privacy, if in fact identity theft does happen and if in fact you know how—what a terrible situation would be of theft.

People spend years and years working to recover. I am on the Financial Services Committee. We've heard horrendous testimony from people for years and years who have tried to clear their names as other people have stolen their identities. It would seem to me that given what has happened and the responsibility for it at the VA, what are you going to do to protect 28 or 30 million Americans whose identity theft may be at risk if in fact that happens? Are you going to come to Congress and say we will ask for money to make sure that we will provide the financial resources necessary and the legal resources necessary to protect those tens and tens of millions of people whose identity was released?

Secretary NICHOLSON. I think that's a very good, very important question. And we—so far what we have done, we've notified every person whose identity that we have and with the cooperation of the IRS because the addresses we do not have we matched them against Social Security without a violation of their privacy and we were able to—we sent a letter to every affected person, and in that letter we give them one notice that this has happened and the steps that they can take and the steps—and we've coordinated closely with the three major credit agencies that there are in the United States who make available to every citizen upon a call or an e-mail or a fax a free credit check and a credit alert. So that they can implement that immediately. If they have any questions about how to do that or need assistance——

Mr. SANDERS. And that's fine. I am aware of that. But here's the question. If—and we hope it does not happen, but if it does happen, you know, the identity theft is a horrible thing. We have heard testimony year after year from people who have tried to clear their names and convince creditors that they have not racked up these bills. It's a terrible experience. If that happens, are you going to come before Congress and say we have to take responsibility for the financial expenses incurred by veterans for the legal expenses? Are you going to come before Congress and ask for that help, or are you going to let the men and women in our military have to cope with this by themselves?

Secretary NICHOLSON. I can tell you, Congressman Sanders, our No. 1 priority really in everything that we do at the VA is the veteran, what's best for our veteran, and we now have active service members that we would include in that priority. So what unfolds will be guided by that principle.

We also, I would mention to you, have, and this was not in place before this came to the light of day, a new Presidential task force on identity theft and very ironically had a meeting set for this task force and I serve on it. The first meeting was accelerated and met the first day that we disclosed this information. And that task force will also consider this question because it's a very important question.

I had a meeting yesterday afternoon with the veterans service organizations, leadership, 15 or 20 of them. We had the same discussion.

Mr. SANDERS. I think they have initiated a lawsuit against you; isn't that correct?

Secretary NICHOLSON. One group of them has initiated, others have issued statements saying that's not the answer to this.

Mr. SANDERS. My hope, Mr. Secretary, is that in fact you will do everything that you can, that in case there is identity theft taking place that you do everything you can to protect financially and legally our veterans, that you will come before Congress if you need the money to do that.

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

Mr. GUTKNECHT. Thank you, Mr. Chairman. I guess I am becoming a little more or less confused about this from this testimony, because what I've been reading in the papers is there was a very serious security breach and that millions of names were out there floating in space. What I am hearing today, Mr. Nicholson, is that's not exactly the case, at least we don't know that yet. Let me review what we've learned today to make sure I am on the same page.

An employee against the policy of the VA took their laptop computer home. That laptop computer was stolen. We don't know what happened to the data that probably was on that laptop, but so far none of that data has appeared in cyberspace as far as we know; is that correct?

Secretary NICHOLSON. That's correct, Congressman. I just would add that they took a laptop, some computer disks and downloaded it into a hard drive and the hard drive was stolen also.

Mr. GUTKNECHT. I am going to be clear on this. Who downloaded it or who downloaded it to the hard drive?

Secretary NICHOLSON. The employee, the subject employee.

Mr. GUTKNECHT. But the people who stole it, we don't know what they did with that data?

Secretary NICHOLSON. That's correct.

Mr. GUTKNECHT. So I think we have to be careful not to get too far ahead of ourselves in terms of real damage. So far there is no evidence that any of these people have actually sustained any real damage; is that correct?

Secretary NICHOLSON. That is correct.

Mr. GUTKNECHT. And in testimony you said that you are going to implement even tougher policies. The employee who was involved has been fired. What else has happened in terms of the agency not only to sort of cure this problem but to hopefully prevent this kind of a problem in the future—not only in your department; this could happen in any department, couldn't it?

Secretary NICHOLSON. Yes, it could. His—the Acting Assistant Secretary in that department has been let go. The principal Deputy Assistant Secretary has been let go. We are rebuilding that department and the Office of Policy and Plans. They have a very bright, recently acquired Navy admiral that the President has now announced that we've recruited. We have tremendous opportunity in the private sector and he has a great background. He's teamed up to come in if confirmed to take over to rebuild that department.

We are reviewing all of our existing rules, regulations and laws, and that is another reason I welcome the opportunity to come here not because it is pleasant to you in light of what's happened, it is my responsibility, but we need to put some more teeth into the enforcement of this because the attitude is far too laissez faire. And I would add that in the discussion that just ensued where we talked about having some teeth in HIPPA and not having teeth in FISMA, in HIPPA there is also a requirement to disclose to people

if their identity has been accidentally or intentionally compromised, where there is not in FISMA. Let's put it in there. Just another step, and then we need to start enforcing some of this so we set some examples.

Mr. GUTKNECHT. Let me—I can't resist the opportunity, Mr. Gray, I want to come back to a question that keeps coming up relative to Social Security, and that is we are having some rather heated debates in Washington about illegal immigration. And I have heard employers say that one of the real problems we have is a lot of people are using false Social Security numbers. How does the Social Security Administration deal with that because I have heard there may be three different employees using the same Social Security numbers. How does that not come back to the——

Mr. GRAY. One of the tools that we fielded last year was the Social Security number verification system that allows an employee who they hire to enter the information into a Web based application and verify that person's Social Security number really doesn't belong to them to give them a tool in making sure that Social Security number and those wages are reported correctly. In addition to that, as employers report wages throughout the year we do checks to try to make sure that we associate the wages appropriately with the person's Social Security number.

Mr. GUTKNECHT. Are you saying right now we don't have multiple employees using the same Social Security number?

Mr. GRAY. No, I am not saying that.

Mr. GUTKNECHT. How would you find that out?

Mr. GRAY. When the wage earner—when the employer reports come in we can have multiple employers showing multiple wages on the same Social Security number. We try to investigate that.

Mr. SHAYS [presiding]. I'm going to interrupt. Mr. Waxman needs his time before the vote time.

Mr. WAXMAN. Thank you, Mr. Chairman. As I understand it, we have had on the books since 1974 laws to protect privacy and another law in 2002. The General Accountability Office has been giving grades to agencies about how well they're doing in meeting requirements.

Isn't that correct?

Mr. WALKER. I think this committee is the one that gives the grades. We do, however, look at computer security as part of our audit of the financial statements, and that is a material weakness area for many agencies.

Mr. WAXMAN. In fact, this committee gave the Veterans Administration an F in terms of security for this kind of data.

Secretary Nicholson, you blame this on obviously employees being fired, on the culture, on people just not doing what they're supposed to be doing, but that doesn't sound to me like we are really getting to the heart of it. It is sort of passing the buck. Now it sounds like you are also going to seize this opportunity to clamp down, and I appreciate that. But I just want you to know how bureaucratic it all sounds. We have Mr. Johnson from the Office of Management and Budget. You are the Secretary. You are Secretary for only a short period of time and you blame the fact that an employee had been there for a long time. I don't know what relevance that has except we need to find out who has access within the VA

to the type of information that was stolen. Do you know how many people have access to this type of information?

Secretary NICHOLSON. Congressman Waxman, I don't think I could give you right now the exact number, but I will tell you that quite a few people do. We have a system of authorized telecommuting and teleworking that is a product of encouragement of the Federal Government.

Mr. WAXMAN. How many VA employees have the capacity to download this information unencrypted onto personal computers?

Secretary NICHOLSON. Well, the—of the subject information it would—I couldn't give you the exact number right now but that number would not be real high because this was a—out of what is called a BURALS file, which is an acronym for this system. He was working on a project at his home and using the entire data base. Not many would have that.

Mr. WAXMAN. You explained that individual. Do you know how many employees have such unencrypted information on personal hard drives outside of the VA offices now?

Secretary NICHOLSON. Yes. I think that 35, roughly 35,000 employees of the VA have some level of accessing data and working it on laptops or computers at home, much of it through the VPM, the Virtual Personal Network.

Mr. WAXMAN. That's a large number of people that have this information out. You have said that what we need to do is—I hope you'll take charge of those 35,000 people or so that had——

Secretary NICHOLSON. As I said in my testimony, we are doing a survey right now to see who all has access, why they have access, and what access they have, inventorying the entire system.

Mr. WAXMAN. The story seems to have changed. First we were told only veterans and some spouses were affected and then about 50,000, but no more active duty personnel were affected. And then on Tuesday we learned that 80 percent of the active duty military may have been impacted. Was any medical information on any of these veterans, on active duty members compromised?

Secretary NICHOLSON. No, sir.

Mr. WAXMAN. How about disability ratings?

Secretary NICHOLSON. Some of them had a disability classification index in part of their line. But on the medical question there were no—no medical records were compromised in this at all. There were about 300 people that we have ascertained through the forensic work that we are doing that have an annotation, a medical annotation next to their name. And I'll give you an example because I looked at all of these. One of them said asthmatic. Another herniated disc. It is fewer than 300 but nearly 300 have that degree of annotation next to their name.

Mr. WAXMAN. I see my time has expired. Thank you, Mr. Secretary. Mr. Chairman.

Mr. Shays. Thank you very much.

I'd first like to ask GAO is this something that should have shown up in our radar screen? We can throw bricks at the administration and we can throw bricks at the Department. But is this something where GAO could have alerted us better? Or you did alert us or combination of both? What's an honest assessment of

why all of a sudden we seem to be outraged and shocked by what's happened?

Mr. WALKER. I think both the GAO and Inspector General have both in this case been charged with the responsibility for auditing personal statements of respected agencies as well as U.S. Government overall. There are serious security challenges. So many agencies——

Mr. SHAYS. Same security channel. Say we are finding terrorists, it's more helpful when we are fighting Islamic terrorists we know are not from Iceland.

Mr. WALKER. I think the key, Mr. Chairman, we have a lot more controls over classified information and taxpayer information and, as Secretary Nicholson mentioned, there are now sort of the controls under HIPPA for health information. There is a gap here, and the gap is with regard to certain sensitive information that could end up improperly being disclosed, and I think one of the things we need to look at is not—clearly agencies should be taking steps on their own but Congress may want to consider requiring certain steps.

Mr. SHAYS. That's helpful information, but sometimes Congress will get blamed. Sometimes Congress will get blamed because we didn't do something. We look at the testimony and the department head says we have all of the money we needed to get the job done. You need to refer to someone.

Mr. WALKER. If I can. Thank you. I've been advised we have not issued a report directly on this. However, in the conduct of our audits we have noticed weaknesses in this area before so it was one of a number of material controls.

Mr. SHAYS. But weaknesses specifically with people taking information out?

Mr. WALKER. Weaknesses with the potential for information to be compromised, not that it actually was compromised.

Mr. SHAYS. What strikes me, you know, I heard the Secretary say he was outranked. He should be outranked because it is beyond stupid to take out sensitive documents. But I have a sense that is a common practice. So obviously we've all been a little asleep. The department heads have been asleep. The White House has been asleep. Congress has been asleep and now we are trying to deal with it, and all I wanted to know is there's been no specific outlining that we have this kind of problem. And you are coming forward and obviously saying we need to deal with this issue? You are also saying we have had security. We need to maintain security. Mr. Johnson, tell me, when you heard that this happened at the Department of Veterans Affairs? Anger would probably be one way to describe it, but were you surprised or did you start to say, my gosh, you know, is this just the tip of the iceberg?

Mr. JOHNSON. No. I was surprised. I am told that there are dozens of security breaches involving a laptop, for instance, nothing, though—a year. None of these involve 26, 27 million names. So this is the hundred-year storm of security breaches. So the magnitude of it is the alarming thing. There are breaches. There will be breaches. And in spite, no matter however we spend and how tightly we resecure this, the more we secure it, the more responsible, the fewer the number of breaches, whenever we have one we need

to respond accordingly, figure out what caused the problem and deal with it. But it was the number of names that was truly alarming to everyone.

Mr. SHAYS. If it's anticipated that this was a common theft, they weren't really looking for this bit of information and that's one of the opinions out there. Is it a strongly held opinion on the part of folks that are investigating this?

Secretary NICHOLSON. Yes, sir. I would say, Mr. Chairman, that it is quite commonly held among the law enforcement investigating communities.

Mr. SHAYS. Is it something where we can simply offer a significant reward to contact a certain person with no—that they return this with no prosecution? I mean, because what's at stake is so significant. Do we have the capability to say, you know, you stole the computer but, by the way, you have something that will cost us billions of dollars to deal with and provide some incentive for them to return it with no prosecution if they do? Do we have the capability to do that?

Secretary NICHOLSON. We do not have the capability. That was discussed at our hearings in the GAO committee. But I will say that a $50,000 reward has been posted by the Montgomery County, MD law enforcement community.

Mr. WALKER. As I mentioned earlier, and you may or may not have been here.

Mr. SHAYS. I was trying to be in a vote.

Mr. WALKER. I understand. I was briefed by my own CIO with regard to our own procedures and there are two things that I think people can think about in this area right now irrespective of whether or not Congress takes any action.

Specifically to encrypt all sensitive information of the type that we are talking about. That doesn't mean encrypt all information, but encrypt this type of sensitive information. And all—or prevent the ability to download and/or copy certain types of sensitive information. Those are things that can and should be done now. Because the fact is we are moving to use technology more. More and more government employees have laptops because they are mobile, because the government is promoting Flexiplace and things of that nature. So we need to take these steps to minimize the risk.

Mr. SHAYS. My Government Reform subcommittee oversees Defense and State Department hearings about classified material and we had DOD testing that 50 percent should be reclassified, 50 percent more than we should classify, we had the outside group saying we classified 90 percent more than we should. Then we had a hearing on all of these sensitive but not classified, which anyone could classify, and then we have a breach like this which clearly should never have gotten out of someone's office. So it blows you away and some of the secret stuff that I look at would make you laugh because there is nothing secret about it and something like this is huge and it just—when you went to look at it in your own operation, did you get a candid response from anyone who said, hey, boss, we sometimes take out stuff, too, or do you have confidence within your own department that this couldn't happen?

Mr. WALKER. I have confidence. We have extensive procedures in checks and balances. For example, when we have this type of sen-

sitive information, we typically end up having a separate hard drive that we lock up. We have computers at GAO. The people can only use computers at GAO for this type of situation. You could theoretically have somebody who willfully and intentionally, however, wants to abuse the system, and that's why we've never had that, I might note. But that's why I am saying what else can we do to even try to deal with that situation. Even if you have all of these other checks and balances, that's why I come back to encrypt this type of information and/or possibly as a supplement prevent the copying and/or downloading of this type of information.

Mr. SHAYS. Let me conclude with this and then go to Mr. Mica.

Is the biggest concern that people will be careless or that they will actually be devious and go beyond careless? What is the big concern? Maybe you could comment as well.

Secretary NICHOLSON. I think the bigger concern, Mr. Chairman, is carelessness. That's the instant case. This person wasn't being deviant. They were working on a project that he had been doing that for 3 years, taking the data home and working.

Mr. SHAYS. How long do you think it's going to take you to resolve this problem, not get the information back but make sure it doesn't happen again?

Secretary NICHOLSON. I think that it won't happen overnight but it is very doable and we are under way. It is something that absolutely has to be done, but I don't know that you were here, but we are going to need some tools for enforcement and you were touching on it a minute ago when we require——

Mr. SHAYS. I don't want to repeat the record. Yes, Mr. Johnson, and I apologize.

Mr. JOHNSON. I'd like to point out that—follow up on what Mr. David Walker was talking about. It is currently the standard that all data, sensitive data on laptops be encrypted. That is the standard. It's just not enforced. We don't hold agencies, ourselves accountable for that being the case.

Mr. SHAYS. Thank you.

Mr. Mica.

Mr. MICA. Thank you, Mr. Chairman, and I am not here really to beat up on these witnesses. In fact, I know three of them fairly well. You have three probably of the most dedicated, capable, public servants. Watched Clay Johnson and his experience over the years and Secretary Nicholson, incredible representative of the United States, and his tenure, and now incredible advocate for our veterans. Then I have known Mr. Walker since—I don't want to say since he was in diapers but for a long time. Although you look pretty old these days, Dave.

But the problem is not these capable administrators or the other witnesses you have. The problem is advances in technology, and I would venture to say since you know on this disk you have millions and millions of pieces of information and pretty soon we'll have it probably in something the size of the thumbnail, and I would venture to say that not a day goes by that someone from your agencies or congressional staffers don't take laptops home or someplace else and we are at risk.

What we had here was a theft, a criminal act. But we do have to keep the laws and the rules up with technology, and that's what

we are always having trouble with in Congress. Laptops didn't even exist. Cell phones, I was in the cell phone business and I was a pioneer in 1987, something like that. That's not that long ago. So keeping up with it.

So I have a couple of questions. I left it after a bit, but did we do our job? I see that even the President did in August 2004 a directive that actually directed OMB to take the lead here. I did read that—we have two responsibilities. One is protecting data and what to protect and then, well, what to protect and unprotecting it. And how we protect is so important.

OK. Clay, you were responsible. You're still the lead agency in this, in setting the——

Mr. JOHNSON. In some HSPD1 identification cards.

Mr. MICA [continuing]. Security of information for the agencies. Did you—have you sent out a—so you have sort of taken a lead in this? And then I read that while 20 percent of the government systems are certified and accredited, this is agency security planning. That means 20 percent are not. Do you monitor this? Is that your responsibility?

Mr. JOHNSON. Yes.

Mr. MICA. Who isn't the 20 percent? It says 80 percent of the government systems.

Mr. JOHNSON. I can get you that information.

Mr. MICA. I think that's important to find out where the gaps are.

Do you have enough legislative authority to do what you need to do to make certain there is compliance? Because I know these agencies—we have dozens of agencies and they are all going their own way. Do you have enough legal authority from the Congress to set standards?

And then the other thing, too—the important thing here, too, is reporting back an incident. And I read you directed your staff to have Homeland Security chief information officer counsel to identify the appropriate detail and schedule for distributing a periodic government-wide incident report. That is getting information back on incident.

Mr. JOHNSON. Yes, sir.

Mr. MICA. You pick them, and do you have enough authority and do they have enough authority to get compliance? And then the concern of the chairman was the timeline of information and reporting. Would you answer that elongated question?

Mr. JOHNSON. As to the second question, the reason why we refer to DHS, they are the cybersecurity office. They are the lead on cybersecurity. So that's why this reporting is to them. And it's my understanding it is not clear as it needs to be how we record different kinds of breaches, and we need to be sure that it's real clear——

Mr. MICA. Do you have a systemwide standard right now? OK, a breach has occurred. What's the reporting? Is that——

Mr. JOHNSON. We have that now, but the reporting is inconsistent and I'm not sure that they're all—it's equally clear to all agencies. So we need to make sure that it is.

Mr. MICA. Do you have the authority to require that? Not require; you are just requesting. It is a "may" rather than a "shall."

Mr. JOHNSON. I don't know. I think of them as being the same. But maybe somebody else would think of them differently, but——

Mr. MICA. Again it is nice to beat up—we pass the laws and then sometimes we allow you to pass the rules. But we have to make certain that somebody has the authority and responsibility for this, both the——

Mr. JOHNSON. I think one of the things we can do is, in general, I think we have the laws and the regulations we need. We don't need to assume that, though. We should go and make sure that maybe there's—we have 95 percent of what we need but we need extra teeth in it, as the Secretary talked about, over here and over here. So we need to review that. I bet we'll find a couple of additional things we need to do. But the big opportunity and the big challenge here is to enforce and be held accountable, all of us, for abiding by the laws and regulations and processes and procedures and standards that are already on the books.

Mr. MICA. Thank you.

Chairman TOM DAVIS. Thank you.

Mr. Souder.

Mr. SOUDER. Thank you.

What's happened here is basically every conservative's nightmare about consolidation of information in the Federal Government; what would happen. And I was pleased to see in your testimony, and then, Secretary Nicholson, you responded to it because you said that in addition to informing all concerned—I was a little concerned. Mr. Johnson just said that he didn't think there were necessarily new laws, and you've been saying we need new laws because, for example, in your statement you say this may violate Federal law and could result in administrative, civil, or criminal penalties. This is something Congress should act on immediately because when we talk about disincentives to take things home and to not follow the rules, you can sit through seminars but if there's no consequence—so I was glad to see you make that point.

I have one technical followup question to Mr. Gutknecht. You said that there is some reason to believe this is a computer fencing firm basically. Was the disc inside the computer or did they also collect discs that are lying around the site?

Secretary NICHOLSON. I'm having a little trouble hearing you. Was your question——

Mr. SOUDER. Regarding the theft, the statement said there's speculation that this may be a group of people who basically fence computers, steal the computers. But you made the statement that the drive—was that in the computer, or did they take it in particular, or did they take the other information and there may be a secondary market going on?

Secretary NICHOLSON. There was a laptop and a hard drive. They weren't at that time connected. They took both of those and did not take the discs.

Mr. SOUDER. So only the discs that were inside the equipment are what they have?

Secretary NICHOLSON. We don't know—we don't know what was loaded in his laptop.

Mr. SOUDER. We don't know that the information has been stolen——

Secretary NICHOLSON. He told us that he had downloaded these discs into the hard drive. We obviously don't have the hard drive either. That's what was stolen. But we do have the discs. And he brought those to us and that's what's been undergoing this forensic analysis is the holdings that are, you know, developed.

Mr. SOUDER. Thank you. Because what that means is that somebody has to actively download to do that, and there has to be another step in the process here.

Mr. Johnson, Congressman Sanders raised the question to Secretary Nicholson, but those of us who have been here a long time know that this is really—a lot have known—the question. If indeed we start to identify that in fact this information is being used, it is outrageous that many low-income veterans and veterans would have to pay for the credit reports. Would OMB back up the Veterans Administration in coming to Congress and saying look, we need some money because the veterans shouldn't have to fund this because it's a government error, not their error?

Mr. JOHNSON. We agree totally with Secretary Nicholson that our highest priority is to find the best way to serve the veterans and the active military personnel who are at risk of being harmed here, and that means figuring out the best way to do that and then doing it.

Mr. SOUDER. You agree it's not their financial responsibility to try to figure this out; that the government made the error, they didn't?

Mr. JOHNSON. I would agree with that. But, again, that's not just financial response—our responsibility or not. It's all the ways we can serve them.

Mr. SOUDER. It's broader than that.

Mr. JOHNSON. Yes, sir.

Mr. SOUDER. But if you don't have—if you're already trying to figure out how to cover your health care, you're already trying to figure out how to cover your housing, you don't have much income, asking to do multiple credit reports to track—like it's their responsibility that they lost it when it was the government's—is a big deal right now.

Mr. JOHNSON. Right.

Mr. SOUDER. And I wanted to ask Mr. Walker—and this may also come back to you, Mr. Johnson—that most identity theft in the United States right now isn't related to trying to steal the person's full identity, or even for financial purposes. It's related to the fact that we have Social Security numbers being stolen for illegal—by illegal immigrants who need a job, many of them in my district. In 1 month they took down three green card manufacturers who were producing with stolen Social Security numbers.

Not only related to this latest with the Veterans Administration, but in the other agencies where there's theft, do you know, or are there recommended policies, or how do we interrelate this theft with ICE, with CBT, with the Coyotes and other groups that are networking in large groups of people, fencing operations for stolen Social Security numbers? Do we have a systemic way of addressing where—if this shows up? Because this isn't just going to show up with somebody in a bank account somewhere. Maybe it would indirectly, later on in a Social Security number; if one of the veteran's

Social Security numbers are stolen, something is going to come in under FICA relatively, you know, down the road here. But it seems like one of the first points of contact should be that an alert should go out to ICE, and so we're watching whatever kind of networks we have where these Social Security numbers might pop up.

Mr. WALKER. I'll have to reflect on that, Congressman. I will say this: that one of the major problems that we have is when Social Security numbers are intentionally or inadvertently disclosed, and that provides a basis under which individuals who engage in certain other activities that can result in identity theft. And I think one of the things we're willing to do is to make sure that when you have SSNs, that type of information either, A, isn't used for an identifier; or, B, if it is, that it's encrypted in some way so that people can't attain access to that. Presumably the VA is taking steps to try to ascertain whether or not some of this information might be compromised, you know, through sampling techniques, through the type of communications that you're talking about with selected Federal authorities. I think that's important because—that they be proactive in that regard. And if it turns out that it looks like there are some that have been, and hopefully they will never be, but if it turns out, then it comes back to your question: What are you going to do for everybody with regard to credit reports and credit monitoring? But we may not get to that point.

Mr. SOUDER. But my question was, really, wouldn't the first logical place that you would be trying to track whether this has been stolen, looking—since it's the No. 1 reason Social Security numbers would be stolen—would be to work with ICE, CBP, and looking at illegal immigration, which then the secondary tail would be through FICA reports.

One of my friends—Congressman Gutknecht referred to it—had four other people on her Social Security account. And when she went to apply for a credit card, it was very difficult for her with the Social Security Administration to try to prove who she was. And if we have all these veterans going through this, one of the first places we should look at are who's likely to be using these numbers; not just bank accounts, but who's likely to be stealing them?

And I wonder, is that recognized in the government that this is the first place we ought to be looking, financial services right behind it, Social Security right behind it, but this is likely to be the first place it's going to show up in a fencing operation for Social Security numbers?

Mr. WALKER. I think you make a very good point. I mean, one of the hot debates right now is the immigration debate. To the extent that people can get a valid Social Security number, it's a way that they might be able to obtain, you know, employment and other types of opportunities. So it's a good point that I think needs to be followed up on.

Mr. SOUDER. Thank you.

Chairman TOM DAVIS. Mr. LaTourette.

Mr. LATOURETTE. Thank you very much, Mr. Chairman, for having this hearing. And to all of the witnesses, thank you for coming.

Just, first, a commercial: A number of committees are working in the Congress on data security and H.R. 3997, which is the finan-

cial services product, would in fact cover this situation and would, in fact, provide all of these veterans with 6 months of free file monitoring. So I would ask you, Mr. Johnson, if you would share that with Mr. Portman. It's the only bill that does that.

But Secretary Nicholson, I appreciate your being here, but I need to share a story with you because one of the fights we've had on that bill is I've always argued that a data security breach is different than identity theft. One doesn't always lead to the other. And when you lose a laptop, you don't necessarily have to notify everybody about what's going on.

But I have a constituent. His name is Steven Michael. He's 33 years old. He lives in Ashtabula, OH. He served for 3 years in the Army during the Gulf war, and he receives an $873 disability check each month from the Veterans Administration because he has a heart condition. On June 1st, exactly 1 week ago, he withdrew money from his account at a local ATM and noticed that his balance didn't reflect the deposit of his monthly VA check, which is made through direct deposit. He immediately called the VA's 800 number and checked on the status of the payment. The automated system said that the records couldn't be accessed at this time; so he waited and actually spoke to a real live person. He provided his personal information to verify his identity and explained that his VA disability check wasn't in his account. He was stunned to learn that it, in fact, had been put in a new account, his new account. He inquired, what new account? The woman from the VA said that it was a new account he had on file. He told her he had not set up a new account and gave her the last four digits of his existing account. Of course, it didn't come close to matching his new account. She assured him that the problem would be corrected. He asked if he should visit the VA office in Cleveland. She asked if he was close, and he said he could get in his car. And he then drove 45 minutes to Cleveland. He went to the original VA office and provided them with a copy of his account. He was told that the numbers were from his old account. He stressed that it was his current and only account and that his accurate information was entered. He was told that it could take 7 days to process.

He then asked the folks at the VA if this could be related to theft of the laptop containing the information that's the subject of this hearing. He was given a toll-free number, 800–333–4636. Mr. Michael is rightly concerned about this, and he wonders how his direct deposit form could be changed or why it happened on the heels of the reports of the stolen laptop. He believes whoever did this must have had his name, address, and Social Security number. He doesn't believe this is a simple computer glitch because his monthly disability check has been deposited in the same account for years. He is even more disturbed that his bank informed him that it was possible someone phoned in the new direct deposit information to a bogus bank account, his new account, in the State of Michigan.

If you could, Secretary Nicholson, can you give me a sense of whether this is possibly related to the stolen laptop or if my constituent is another unfortunate victim of identity theft?

Secretary NICHOLSON. Or both.

Mr. LATOURETTE. Or both.

Secretary NICHOLSON. First I would tell you, Congressman, that is the first incidence I've heard of that affecting a veteran since this has come to light. I would like to get, you know, that information and we will follow that up on an individual basis. So that is the only one.

Now, it is a fact that every year in this country, 1 to 3 percent of the people suffer from identity theft. Last year, 9 million Americans did, causing them an average of 28 hours of time to straighten it out at an average cost of $5,600, almost all of which was borne by the affected creditors, not the consumers.

We have been talking to a company that specializes in trying to find the derivative source of identity theft, the company happens to be called ID Analytics, because we have that same concern; because 1 to 3 percent of our veteran population are going to be victims of this anyway due to the statistical distribution, and we want to know what's sourcing this. So we will followup with that one and we have not yet entered into an arrangement with this company to monitor this population, but we are seriously looking at it.

Mr. LATOURETTE. I very much appreciate your answer. And to be very, very fair, I will tell you that currently the constituent is in our district office filling out some forms necessary for the regional office to help. And my caseworkers say that they've never seen the VA move so fast—I will tell you that—in response to this report.

And as someone who wrote the identity theft legislation here when we reauthorized the Fair Credit Reporting Act, I'm well aware of the difficulties and the horrible stories that come out of stealing someone's identity.

But I wanted to bring this to your attention for a couple of reasons. One, so you know that you may have one now out of these 28 million people. Two, to please ask that you, through your offices here, make sure that the folks in Cleveland stay on top of this, because obviously this veteran is concerned that the two are related. And if they're not related, then I think it's good news for the VA. If it is related, I think you've got a problem.

I thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much. I just have a couple more questions and then if anyone else has one.

Mr. Nicholson, let me just ask the Secretary, Federal telework programs allow employees and contractors to work remotely. They're good programs. They're seen as a key ingredient of continuity of operations, emergency planning, especially for extended periods of disruption, whether it's a terrorist attack, avian flu. Was this individual participating in an authorized telework program?

Secretary NICHOLSON. No, sir. He was not.

Chairman TOM DAVIS. Are there steps that should be taken as a matter of course to ensure that benefits of teleworks are not eroded by the security risk? It gives us a chance to rethink that and continue to make it—I believe we want telework to grow, but this is a reminder sometimes that there are limitations.

Secretary NICHOLSON. Yes, I think it does. I think it raises to a silhouette that we need to examine this program to see that, you know, the abuses are not taking place, we are not making it too easy for these abuses. And that is where the people thing kicks in

as well as the requirements that data be encrypted and that we monitor it more closely with enforcement for violators.

Chairman TOM DAVIS. Mr. Johnson, does OMB have the authority and the resources it needs to set and enforce government-wide information security programs, or do you need additional authority here, do you think?

Mr. JOHNSON. In general, I think we have sufficient authority, but we ought to review it. We ought to look through it.

Chairman TOM DAVIS. I think we are willing to give you, in light of this, so you seize on every opportunity—if you would look at that and come back and make sure we give you the tools you need to do it.

Mr. JOHNSON. Right.

Chairman TOM DAVIS. I know your dedication to this, but I want to make sure you've got all the tools.

And also what's the position regarding the merits of data breach legislation requiring agencies to notify affected individuals of compromises in their privacy or their personal information? If legislation is enacted, what methods should be used to determine whether and how to notify individuals with security breaches? And will all of you work with us on legislation? Obviously, it's a big deal with Social Security and IRS.

General Walker.

Mr. WALKER. We'll be happy to work with you, Mr. Chairman. Let me also mention in addition to telework, which you just talked about, which could cause increasing risk, even if a person is not on telework, they may travel and take their laptop with them. In addition to that, they may take work home at night or on the weekend, which would not be part of the telework. So we need to look at this issue as a separate and distinct challenge that has to be addressed irrespective of whether they're on telework.

Chairman TOM DAVIS. That's a good point. Mr. Johnson, will you work with us on this, too?

Mr. JOHNSON. I look forward to it.

Chairman TOM DAVIS. This is a good wakeup call.

I guess my last question would be to all of you. In your opinions, individually and collectively, do our departments provide the CIO and its organizational components with sufficient resources to establish and maintain an effective agencywide security program? We hold the CIA's feet to the fire every year with our scorecards on FISMA. We hold them responsible for agency security. Do they actually have the authority to get the job done or do you think this is agency to agency?

General Walker, let me ask you first. You kind of have a government-wide perspective.

Mr. WALKER. I think there are variances by agency. I mean, one of the keys is that under the legislation, the CIO is supposed to be reporting directly to the agency head. Is that happening in form or is that happening in substance? Obviously, there are different levels of resource allocations, not only financial resources but human resources. Do they have enough people with the right kind of skills and knowledge to be able to get the job done?

The example I gave earlier when this issue came up, I pulled the CIO in my office and talked to him directly about what are we

doing and everything else we need to do. I don't know if that happens——

Chairman TOM DAVIS. Let me just get each agency to just respond briefly. I mean, how is the relationship with the CIO? Do they have the authority they need in your agency?

Mr. GRAY. From the Social Security Administration I think they do have the authority—that our CIO does have the authority he needs to do the job effectively. I think we also have the resources we need within the agency to do that.

Mr. GALIK. Yes, Mr. Chairman, I agree. I think the CIO does have that authority and our organization has a direct link to the Commissioner of the IRS to pursue anything that needs to be pursued.

Chairman TOM DAVIS. Mr. Secretary.

Secretary NICHOLSON. I would say, Mr. Chairman, the answer to VA is no; that the CIO has not enough authority to go with his responsibility. But that is in transformation as of last October. And we're centralizing the IT function, creating a new career field where it has been decentralized out into these hundreds of hospitals and the other facilities. We're pulling that back in. So that is really progressing and we'll cure that.

Chairman TOM DAVIS. You've only been there a short time but I appreciate the headway you're making there.

And, Clay, let me just ask you, I mean government-wide you see the variance too. You have Karen Evans, I think, in your shop that helps oversee this. I know what we need to do and how you foster that relationship between the CIO and the agency heads; but wouldn't you agree with me that is very critical in all of these areas?

Mr. JOHNSON. It's critical. I don't think we have a resource problem, which is another question you asked. We spend $65 billion a year on IT; $4.5 billion of that is on security. So we're spending a lot of money on this. The question is are we backing it up with the kind of determination that the Secretary has demonstrated here to really make that stick, is the key.

Chairman TOM DAVIS. Let me thank all of you for your time here, answering a lot of questions. There's a lot of anxiety over this, and we'll continue to monitor it. But you've been forthcoming today with your answers and we appreciate it.

The hearing's adjourned.

[Whereupon, at 12:33 p.m., the committee was adjourned.]

[The prepared statements of Hon. Charles W. Dent, Hon. Jean Schmidt, Hon. Elijah E. Cummings, and Hon. Wm. Lacy Clay follow:]

Congressman Charles W. Dent
Gov. Reform Committee
June 8, 2006
"Once More Into the Data Breach: The Security of Personal Information at Federal Agencies"

Thank you, Chairman Davis for holding this important hearing on the security of personal information at federal agencies. In light of the recent security breach regarding a stolen personal computer of an employee of the Veterans Administration, it is critical that we review agency data security policies and procedures, and examine the adequacy of information security and data breach notification.

In the broader sense, this issue reaches far beyond federal agencies. I have heard from my constituents, and they want strong protections from identity theft, and want immediate notification when the security of sensitive personal information has been breached. That said, it is important that we review the question and possible ramifications of "over-notification". Does unnecessary notification, which is costly and time-consuming, have a desensitizing affect on Americans? Should there be an established threshold of the security breach causing actual harm? Or is triggering notification upon "actual harm", too little, too late? These are all questions that must be considered in developing Federal data security legislation.

As far as the recent, high-profile breach at the VA, at this time it is critical that the VA coordinate the necessary comprehensive response, and institute safeguards to prevent the future reoccurrence of a similar incident.

I look forward to the testimony of our knowledgeable witnesses and appreciate the opportunity to review lessons learned, and hear their suggestions as to preventing future information breaches. Again, thank you Mr. Chairman.

The Honorable Jean Schmidt
House Committee on Government Reform
Hearing on Data Breach: The Security of Personal Information at Federal Agencies

Thursday, June 8, 2006

Opening Statement

Mr. Chairman, thank you for holding this hearing on the very important topic of the security of personal information at federal agencies.

We have all heard the recent reports about the personal information of millions of veterans, active duty military, National Guard, and Reserve personnel, and perhaps some of their spouses, which was stolen from a Department of Veterans Affairs analyst's home last month. I have heard from many veterans in my Congressional district who are concerned about the theft of this personal data. Identity theft is a growing problem in our country, and these service men and women are worried that their personal information could be used fraudulently.

I am concerned about two things here. First, there was a lapse between the time the data was stolen, the time many personnel in the Department of Veterans Affairs were notified about the breach, including the Secretary, and the time the information was disclosed to the public. Second, I am concerned that the VA has not been a good steward of our veterans' personal information over time. Apparently, the VA's Inspector General has warned since 2001 about security vulnerabilities, including access controls, passwords and operating systems.

We owe a lot to our veterans and active duty personnel. They have put everything on the line to protect our nation's security and ensure our freedom. I look forward to hearing the panel's testimony and working with them to improve the protection of our military personnel's personal information.

U.S. House of Representatives
109th Congress

Opening Statement

Representative Elijah E. Cummings, D-Maryland

Full Committee Hearing: "Once More into the Data Breach: The Security of Personal Information at Federal Agencies"
Committee on Government Reform

June 8, 2006

Mr. Chairman,

Thank you for holding this important hearing to investigate the recent security breach at the Department of Veterans Affairs (VA).

We now know that as many as 2.2 million U.S. military personnel—nearly 80 percent of the active-duty force—could have been affected by last month's theft of a VA employee's laptop computer. This is in addition to the 26.5 million veterans we were initially told would be affected.

The ramifications of this security lapse are disturbing to say the least.

Men and women in the armed services put their lives on the line every day to ensure our country's security. Unfortunately, we have failed to return the favor by failing to protect and secure their personal information.

As you know, the Internet has increasingly become a tool used to conduct personal business such as paying bills, banking, and managing credit. With that change, Internet prowlers have become more adept at stealing American's identities and using them online.

Now, with the names, birth dates and Social Security numbers of millions of active and retired military personnel lost, it is unclear whether these people will become the victims of identity theft, too.

Furthermore, as an article in yesterday's *Washington Post* pointed out, the theft raises national security concerns. If this information falls into the wrong hands, it could be used by our enemies to target service members and their families.

James Lewis, director of technology and public policy at the Center for Strategic and International Studies, called the lost data a "treasure trove of information" for terrorists.

I am appalled by this situation that we are faced with today.

I am appalled that with all the security measures that we have set up to protect people's identities, this massive security breach still occurred. I am appalled with the unnecessary burden we have imposed on our veterans and armed forces. And I am appalled when I think about the fact that a security breach like this could happen again.

But this security breach isn't so shocking when we look to the signals that were sent up over the past several years.

The Office of Management and Budget (OMB) issues an annual report on compliance with the Federal Information Security Management Act of 2002 (FISMA), the law that sets up security standards for government programs.

In last year's report, OMB found problems in the oversight of contractor systems, testing of security controls, and reporting of security incidents. Based on OMB's report, this committee assigns grades for the government's security management.

Last year, the government's overall grade was a D+. The Department of Veterans' Affairs received an F.

Mr. Chairman, in this time of heightened national security, we cannot afford to get D's and F's for security management. As Mr. Lewis put it, "We still have a paper rules government when we are a digital nation."

Today we are faced with cleaning up the mess left by this tragedy, and doing whatever we can to make sure it never happens again.

Thankfully, we seem prepared to achieve these goals. VA Secretary James Nicholson has testified that he has established a special task force to examine the department's programs and to "bring about change" in the way it does business.

Additionally, not all stories about the government's security management are bad. The Social Security Administration, which has consistently scored high on OMB tests, provides a model for other agencies to follow.

It is my hope that by examining what went wrong, and looking at how things can be made better, we will be able to prevent a disaster of this magnitude from happening again.

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

STATEMENT OF THE HONORABLE WM. LACY CLAY
VA DATA BREACH
JUNE 8, 2006

Thank you, Mr. Chairman, for holding today's hearing and continuing your good work in the area of agency information security. I also thank the witnesses and look forward to their testimony.

The recent data breach at the VA represents a case study for the reasons why people resist the use of information technology and electronic records containing their personally identifiable information. It also exposes the lack of agency enforcement or governance over current laws that were intended to mitigate the risks of handling such information. If the government cannot guarantee the security and privacy of our citizen's information, then how are we going to require it of the private sector?

We will need to revisit our laws governing access restrictions to personal information and breach notification requirements. There is, however, an easy first step we can take on the security side of the issue. A few weeks back, William Jackson of *Government Computer News* suggested in a column that our agencies ought to require that all sensitive data contained on portable electronic devices be protected through encryption or other forms of data protection.

He rightly points out that NIST has established standards for these tools and they are readily available. While this is not a silver bullet solution, it will significantly decrease the likelihood that data breaches similar to this episode will pose as great a risk or harm to our citizens.

In closing, I hope to work with my friend, Chairman Davis, and all other committee members in developing an appropriate solution for these deficiencies. Thank you, Mr. Chairman, this concludes my remarks.

○