THE CYBER INITIATIVE

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

FEBRUARY 28, 2008

Serial No. 110–98

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

44–063 PDF WASHINGTON : 2008

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
TODD GEE, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

CONTENTS

THE CYBER INITIATIVE

Thursday, February 28, 2008

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to notice, at 10:13 a.m., in Room 311, Cannon House Office Building, Hon. Bennie G. Thompson [Chairman of the committee] presiding.

Present: Representatives Thompson, Harman, Christensen, Etheridge, Langevin, Green, McCaul, Dent, and Brown.

Chairman THOMPSON [presiding]. The committee will come to order.

The committee is meeting today to receive testimony on the Cyber Initiative. The infiltration and exploitation of Federal Government networks and critical infrastructure networks is one of the most critical national security issues confronting our country today.

Public reports suggest that Federal networks have been under attack for years. These attacks have resulted in the loss of indeterminate amounts of information. The purpose of today's hearing is to discuss the administration's proposed Cyber Initiative, a proposal that attempts to reduce the vulnerability of our Federal computer networks and critical infrastructure and the consequences of attacks against these networks.

We aim to discuss several things today, including the consolidation of trusted internet centers, known as TICs, which would reduce the number of Federal connections to the internet and allow for easier monitoring of incoming and outgoing traffic, the implementation of the Department of Homeland Security's cyber monitoring capabilities throughout Federal agencies, known as Einstein, the privacy implications of electronic data collection, efforts underway to conduct damage assessment of Federal systems, and efforts to secure our federally and privately owned critical infrastructure from cyber attack.

Thus far, I have been extremely disappointed in this administration's efforts in cybersecurity. The administration drafted a high-level national strategy for a secure cyberspace in 2002 that presented problems and possible solutions to high-level cybersecurity issues but never mandated any changes required to improve security.

In 2003, the administration eliminated its top advisor on cybersecurity, Richard Clarke, who was a key advisor to the president. Then, after Congress pushed for the creation of an assistant secretary for cybersecurity, DHS waited over a year to fill the position and buried it four levels down in the bureaucracy.

Despite the creation of a cross-agency intelligence director, the administration failed to educate Federal agency officials on the cyber threat. For instance, in a 2007 hearing before this committee, the chief information officer at DHS, Scott Charbo, who is with us today, told us that he had never received any intelligence reports about nation state hacking and that he was unfamiliar with this activity. To me, this suggests a failure on the part of the director of national intelligence who is charged with connecting dots that would prevent cross-agency intelligence failures from occurring.

This administration regularly requested inadequate budgets for DHS cybersecurity activities, both for the National Cyber Security Division, the US–CERT and the CIO security budget and the R&D activities undertaken at the Science and Technology Directorate.

This administration has vested responsibility for securing these networks in folks who don't understand the threat or the technical methods to deal with the threat. Secretary Chertoff's decision to promote Mr. Charbo to the position of deputy under secretary for National Protection and Programs places him in charge of DHS' efforts in the Cyber Initiative. This decision was made in spite of the committee's investigation into how he and his staff failed both to protect the Department's computers from intrusion and properly manage the contractor in charge of security.

In light of these and other issues, it is hard to believe that this administration now believes it has the answers to secure our Federal networks and critical infrastructure.

I want to be clear: I believe that cybersecurity is a serious problem, maybe the most complicated national security issue in terms of threat and jurisdiction. This problem will be with us for decades to come.

I am pleased that this administration recognizes the challenges we face in securing this area.

As Chairman of this committee, I continue to have numerous practical and theoretical questions about the initiative and the possibilities of its success: Who is in charge, what are the matrix for success, who is accountable, how are privacy concerns being addressed, how will future technologies be incorporated, how will future threats be addressed, what legal frameworks must be amended, how will the administration work with the private sector, and what will be done with critical infrastructure?

I am committed to charting a course toward freedom from fear, and I look forward to working through these difficult questions in the weeks, months and years to come.

The Chair now recognizes the Ranking Member of the subcommittee and who is standing in for the Ranking Member of the full committee, the gentleman, Mr. McCaul, for an opening statement.

Mr. MCCAUL. Thank you, Mr. Chairman.

Today's hearing is on the administration Cyber Security Initiative, which is a sweeping effort to better secure the computer networks owned and operated by the Federal Government.

In my judgment, since 9/11, we have been very focused on the threats in the physical world, and yet not enough attention, in my view, has been paid on threats in the virtual world.

I am glad to see that the administration has come forward with an initiative, a plan. Congressman Langevin and I have launched a nonpartisan commission to study the threat of cybersecurity to this Nation and to provide recommendations to the next President of the United States, and I look forward to seeing their recommendations as well.

As this committee learned last year, the Government's computer networks are under constant attack from hackers and criminals, many of whom are sponsored by foreign nations. Just last year, the country of Estonia was temporarily taken off the internet by organized hackers. While the chances that a similar attack could achieve similar results in this country are small, the threat remains very real.

The Department of Homeland Security will play a prominent role in developing and implementing the administration's initiative. In fact, the President's fiscal year 2009 budget request includes close to $200 million more for DHS than was requested last year for cybersecurity, and I am pleased to see that.

In addition, media reports indicates the administration plans to ask for up to $30 billion over the next 5 years. If this figure is accurate, Congress needs to know how that money will be spent. This project is still in the formative stages; therefore, I understand a number of details cannot be shared at this time or possibly in an open forum. But it is important, however, that the administration keep Congress informed so as to avoid any misunderstanding about what this initiative is designed to do.

With such a large project that cuts across the Government, efficient congressional oversight may be difficult to achieve because so many different committees claim jurisdiction over DHS. It is times like this that highlight the fact that despite promises to fulfill all the remaining 9/11 commission's recommendations, the Congress still has not consolidated oversight of DHS, and, unfortunately, it now has oversight by 86 committees and subcommittees.

I understand that the administration doesn't believe that further authorities are necessary for this initiative, but this area potentially could be added to our annual DHS authorization bill, which I urge the Chairman and this committee to take up prior to congressional action on DHS' appropriations bill later this spring. I raised this issue during our full committee this past Tuesday and was pleased to hear an optimistic response from Chairwoman Sanchez.

We on the Republican side look forward to working with our majority counterparts and colleagues on another bipartisan DHS authorization bill.

I yield back.

Chairman THOMPSON. Thank you very much.

Other Members of the committee reminded that under committee rules opening statements may be submitted for the record.

[The statement of Hon. Langevin follows:]

PREPARED STATEMENT OF HON. JAMES R. LANGEVIN

FEBRUARY 28, 2008

THE CYBER INITIATIVE

For years, Federal networks have been under attack. I believe that the infiltration and exploitation of these networks is one of the most critical issues confronting our Nation. The acquisition of our Government's information by outsiders undermines our strength as a Nation. If sensitive information is stolen and absorbed by our adversaries, we are strategically harmed.

Last year, as Chairman of the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, I held a series of hearings on the cyber threats to our Federal networks and critical infrastructure. It is clear that our failure to secure Government networks has more to do with mismanagement, and less to do with inadequate technology. This administration simply has not made cybersecurity a priority. They have not comprehensively identified or mitigated vulnerabilities on our networks; they have not held anybody accountable for breaches; and they have not invested adequate resources to solve the problems. Unfortunately, we are paying the price today.

I remain deeply concerned about the growing threat to our national critical infrastructure. The effective functioning of many infrastructures is highly dependent on control systems. which are computer-based systems used to monitor and control sensitive processes and physical functions. Cyber attacks against these pieces of infrastructure have the potential to cause serious—if not catastrophic—damage to the economy and our way of life. The administration's Cyber Initiative does not adequately prioritize this issue.

With the right vision and leadership, we can improve security on our Federal networks and critical infrastructure. There are some promising elements of the Cyber Initiative, but there are also some gaping holes. I assure the American people that we will continue to perform robust oversight on this issue.

RECAP OF THE SUBCOMMITTEE'S PREVIOUS HEARINGS

Last year, as Chairman of the subcommittee on Emerging Threats, Cybersecurity, Science and Technology, I held a series of hearings on the cyber threats to our Federal networks and critical infrastructure. We began in April 2007, with a hearing on cyber attacks against the Departments of State and Commerce. At that time, it was clear to me that the Federal Government did not understand the severity of the threat. Officials did not know the scope or topology of networks; who infiltrated our networks in the past; who was inside of our networks at the present; and how much information had been stolen. At that hearing, I promised to begin an investigation to assess the cybersecurity posture at the Department of Homeland Security. Chairman Thompson and I began requesting documents from the Department's Chief Information Officer the following week.

Our second hearing in April focused on the need to reduce critical infrastructure vulnerabilities through investment in research and development. In the last 7 years, more than 20 reports from such entities as the INFOSEC Research Council, the National Science Foundation, the National Institute of Justice, the National Security Telecommunications Advisory Committee, the National Research Council and the President's Commission on Critical Infrastructure Protection have all urged the Government to do more to drive, discover and deliver new solutions to address cyber vulnerabilities. Yet the administration routinely proposed reductions or flat funding for research and development efforts at the Department of Homeland Security. Our witnesses described the necessity to dramatically reduce the vulnerability of the national information infrastructure to attack, and make major, strategic investments that can significantly reduce infrastructure vulnerabilities over a 5- to 10-year period.

During a June 2007 subcommittee hearing, we discussed the preliminary results of our investigation into the security of the Department's networks. Due to poor security practices on its networks, the Department of Homeland Security suffered numerous significant security incidents. Routine security reviews—like rogue tunnel audits, ingress/egress filtering, widespread internal and external penetration tests, and contractor audits—were not performed. Multi-factor authentication was not fully implemented And in spite of nearly 900 cybersecurity incidents between fiscal year 2005 and fiscal year 2006, the Department continued to under-invest in IT security.

The testimony of the Department's Chief Information Officer, Scott Charbo, was disturbing to the committee. Although the Chief Information Officer is ultimately

responsible for the security of the Department's numerous information networks, Mr. Charbo seemed unaware and unconcerned about any serious malicious activity on the networks he was charged with securing. For example, when asked if he or his security team had requested or received intelligence briefings about Chinese hackers penetrating Federal networks, or if Department computers ever exfiltrated information to Chinese servers, Mr. Charbo responded "you don't know what you don't know." This answer was typical of the laissez-faire attitude that he exhibited throughout the investigation, and suggested that neither he nor the rest of the Department was taking the issue of cybersecurity seriously. Chairman Thompson and I sought additional information to determine whether these incidents could be tied to the same attacks that occurred on the networks at State and Commerce.

In September 2007, Chairman Thompson and I concluded that the Department was itself a victim not only of cyber attacks initiated by foreign entities, but of incompetent and possibly illegal activity by the contractor charged with maintaining security on its networks. The Department's intrusion detection systems—designed to monitor networks and issue alerts when outsiders attempted to gain access—were not properly installed and monitored. This resulted in dozens of computers becoming compromised by hackers, who sent an unknown quantity of information to a Chinese-language Web site. We asked the Department's Inspector General to begin an inquiry into these matters and refer the case for criminal investigation.

In October 2007, my subcommittee again revisited the issue of cybersecurity and critical infrastructure, specifically with regard to the electric grid. The effective functioning of the bulk power system is highly dependent on control systems, which are computer-based systems used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed-systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. As such, the cyber risk to these systems is increasing. Intentional and unintentional control system failures on the bulk power system can have a significant and potentially devastating impact on the economy, public health, and national security of the United States.

The subcommittee learned about an experimental cyber attack led by DHS researchers at Idaho National Laboratory. This experiment—code-named Aurora—could inflict significant damage upon the electric sector, and several Members joined me in calling upon the Federal Electric Regulatory Commission (FERC) to investigate whether the owners and operators were implementing mitigations to prevent this attack from occurring. In light of these issues, I joined Chairman Thompson, Chairwoman Jackson Lee, and Ranking Member McCaul in submitting comments to the FERC rulemaking, arguing that their proposed standards do not sufficiently ensure the production or delivery of power in the event of intentional or unintentional cyber incidents involving critical infrastructures. We suggested adopting standards for control systems proposed by the National Institute of Science and Technology.

Our final hearing focused on the implementation of the cyber aspects of the Sector Specific Plans. These 17 plans—one for each critical infrastructure sector in the United States—are supposed to describe how each sector will identify, prioritize, and protect their physical and cyber assets. However, an investigation performed for the committee by the GAO suggests that many of the 17 plans are incomplete when it comes to cybersecurity. The GAO analyzed the 17 plans under three categories: fully addressed, partially addressed, or not addressed, and found that none of the plans fully addressed all 30 cybersecurity criteria. Even more distressing was the absence of an implementation plan. Because Sector Specific Plans remain a voluntary exercise for all sectors, the Federal Government is unable to assess the effectiveness of the private sector's cybersecurity controls.

Each of these hearings suggests that the Federal Government is vulnerable to a cyber attack against Federal networks or critical infrastructure. We must continue to identify vulnerabilities in our systems. We must continue to reduce those vulnerabilities. We must continue to engage the private sector. We must make cybersecurity a priority.

Chairman THOMPSON. I now welcome our witnesses to this hearing.

Our first witness, Karen Evans, is the administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget. In this role, she oversees implementation of IT throughout the Federal Government, including advising the director on the performance of IT investments, overseeing the

development of enterprise architecture within the agencies, directing activities of the Chief Information Officer Council and overseeing the usage of the e-government funds to support interagency partnership and innovation.

Our second witness is Robert Jamison, the under secretary for the National Protection and Program Directorate at the Department of Homeland Security. He was confirmed in December 2007. Under Secretary Jamison leads the Department's integrated effort to analyze, manage and reduce risk. Mr. Jamison oversees the Department's efforts in the Cyber Initiative.

He will be joined in questioning period by Deputy Under Secretary for National Protection and Programs Directorate Scott Charbo. Mr. Charbo was named to this position earlier this month after previously serving as the Department's chief information officer.

Without objection, the witnesses' full statements will be read into the record. I ask each witness to summarize their statements, beginning with Ms. Evans for 5 minutes.

Ms. Evans.

STATEMENT OF KAREN EVANS, ADMINISTRATOR, ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET

Ms. EVANS. Good morning, Mr. Chairman and Members of the committee. Thank you for inviting me to discuss the administration's comprehensive National Cyber Security Initiative. Our work on the Cyber Initiative is focused on building upon our existing effort to continue to close the gap in areas of continued weakness, implementing existing security policies and managing our risk associated in particular with non-secure external connections, including internet points of presence.

Please note, our work is happening concurrently on all of the programs described in my written statement.

Agencies connect to the internet to deliver timely information and services to the public, but each new connection multiplies threats and vulnerabilities. Agencies can consolidate or reduce unnecessary connections while still accomplishing program goals. OMB has set a target date of completion for the reduction and optimization of agencies' external connections, including those to the internet, by June 2008.

Agencies reduce the number of internet connections, as they also will be determining transitions and, if so, their transition strategy to the network's contract managed by the General Services Administration. This transition provides an opportunity for agencies to consolidate and optimize their external access points and to obtain secure telecommunications technologies and services.

In connection with the network's transition, Einstein will be deployed at the appropriate external connection. Currently, 14 departments and agencies have deployed Einstein. Einstein will be discussed more in depth by my colleague, Under Secretary Jamison, during his statement.

Agencies are also taking advantage of products and services offered by the Information Systems Security Line of Business. This initiative, led by the Department of Homeland Security and OMB,

was introduced in the spring of 2005 and identified common solutions for four areas to be shared by the government: Security training; Federal Information Security Management Act, FISMA, reporting; situational awareness and incident response; and the selection, evaluation and implementation of security solutions.

As of November 2007, 12 agencies had implemented security awareness training services provided by three approved shared service centers, and 13 agencies have begun using FISMA reporting services provided by two approved shared service centers. As a result, agencies are beginning to reduce duplicative investment and common security tools, ensuring a baseline level of training and reporting performance and are better able to refocus their efforts to other complex and critical security issues at their agency.

With the understanding that vulnerabilities result from weaknesses in technology, as well as improper implementation and oversight of technological products, we have collaborated with the National Institute of Standards and Technology, NIST, the Department of Defense, the National Security Agency, and Microsoft to develop a set of information security controls to be implemented on all Federal desktops, which are running Microsoft Windows XP or Vista.

This set of controls, known as the Federal Desktop Core Configuration, is currently being implemented across the Federal enterprise. By implementing a common configuration, we are gaining better control of our Federal systems and are allowing for closer monitoring and correction of potential vulnerabilities, while limiting the download of internet applications to only authorized professionals.

In addition to the desktop configuration, we are also working with the vendor community to make our application safer. As part of this program, NIST has developed testing tools for use by both the Federal agencies and the vendors. NIST awarded Security Content Automation Protocol, or SCAP, validation to three products as of February 4, 2008.

Three independent laboratories have been accredited by NIST National Voluntary Laboratory Accreditation Program for the SCAP product validation.

To help agency procurement officers ensure that new acquisitions include the common security configurations, we have also provided agencies with recommended procurement language. The Federal Acquisition Council has approved the language and is completing the process of adding this language to the Federal acquisition regulations.

While notable progress in resolving IT security weaknesses has been made, and I have included more examples in my written statements, problems remain in agencies' implementation, and new threats and vulnerabilities continue to materialize. Work remains to continue to improve the security of information and systems supporting the Federal Government's missions and manage the risk associated with these systems.

To address these challenges, OMB looks forward to continuing to work with the agencies, GAO and Congress to promote the appropriate risk-based and cost-effective IT security programs, policies and procedures.

I will be happy to answer any questions at the appropriate time. [The statement of Ms. Evans follows:]

PREPARED STATEMENT OF KAREN EVANS

FEBRUARY 28, 2008

Good morning, Mr. Chairman and Members of the committee. Thank you for inviting me to discuss the administration's Comprehensive National Cybersecurity Initiative. My remarks today will focus on the progress we have made in improving the security of the Government's information and information technology (IT) systems as well as our strategy for managing the risk associated with our Government services in this ever-changing IT environment. In our increasingly interconnected and interdependent environment, security risks left unaddressed by one agency can exponentially compound security risks faced by all of us. These weaknesses prevent agencies from achieving program goals and erode the public's trust in us.

Information security and privacy are extremely important issues for the administration. On March 1, 2008, the Office of Management and Budget (OMB) will provide our fifth annual report to the Congress on implementation of the Federal Information Security Management Act (FISMA). This report will go into detail on our improvements and remaining weaknesses for both security and privacy.

OMB policies and subsequent National Institute of Standards and Technology (NIST) guidance focus on a risk-based, cost-effective approach and reflect the balance between strong security and mission needs. Agencies are responsible for implementing the policies and guidance for their unique mission requirements within their capital planning and investment control processes. Agency officials who own and operate the agency business programs are ultimately responsible and accountable for ensuring security is integrated into those program operations. Our oversight is achieved in two primary ways—via the budget and capital planning process, and through independent program reviews.

Our work on the cyber initiative is focused on closing gaps in areas of continued weakness—implementing existing security policy, and managing non-secure external connection, including Internet points of presence. Please note our work is happening concurrently on all of the programs described.

EFFECTIVELY IMPLEMENTING EXISTING SECURITY POLICIES

Securing cyberspace is an ongoing process, so as new technologies appear and new vulnerabilities are identified, NIST provides guidance to Federal agencies on securing networks, systems, and applications. Recommendations include user awareness briefings as well as training for technical staff on security standards, procedures, and sound security practices. As required by 44 U.S.C. § 3543, Federal agencies must adopt and comply with standards promulgated by NIST, and identify information security protections consistent with these standards.

For example, agencies must complete certification and accreditation (C&A)—a fundamental security procedure required by law and policy. As of first quarter fiscal year 2008, 985 systems (9.5% percent of all systems) operate without a complete C&A. Based on our annual reports to Congress, the percentage of systems C&A'd rise each year we need to be at 100%. When performed correctly, C&As identify the risks when operating an information system, tests controls necessary to mitigate them, and provides program managers a level of assurance the systems supporting their programs operate at an acceptable level of risk.

In addition to following existing policy, agencies are continuing to take advantage of GSA's SmartBUY program when acquiring security products and services. SmartBUY is a Federal Government procurement vehicle designed to promote effective enterprise level software management. By leveraging the Government's immense buying power, SmartBUY has saved taxpayers millions of dollars through Government-wide aggregate buying of Commercial Off the Shelf (COTS) software products. Agencies are utilizing new SmartBUY agreements to acquire quality security products at lower costs.

In one recent example, GSA and DoD established a SmartBUY agreement for products certified through the NIST FIPS 140–2 Cryptomodule Validation Program. These certified products will be used to encrypt data at rest. This benefit is not confined solely to Federal agencies, since the Blanket Purchase Agreement (BPA) was written so that States and local governments can also take advantage of this opportunity.

In addition to the encryption BPA, GSA worked to complete two BPA's for credit monitoring services deemed necessary by an agency in the event of a breach of per-

sonally identifiable information (PII), as well as risk assessment services for when a breach occurs. More information about the BPA related to credit monitoring services can be found in our OMB Memorandum M–07–04, "Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)," at *http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf*. More information about the BPA to assist agencies to assess risk associated with data loss can be found in our OMB Memorandum M–08–10, "Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA)," at *http://www.whitehouse.gov/omb/memoranda/fy2008/m08-10.pdf*.

Currently, the Information System Security Line of Business (ISSLOB) is working across Federal agencies and with GSA to assess the feasibility of additional security related SmartBUY and BPA opportunities for situational awareness and discovery tool sets.

MANAGING MULTIPLE NON-SECURE EXTERNAL CONNECTIONS

Agencies connect to the Internet to deliver timely information and services to the public, but each new connection multiplies threats and vulnerabilities. Agencies can consolidate or reduce unnecessary connections while still accomplishing program goals. Per OMB guidance, agencies must reduce and/or consolidate their external connections including those to the internet by June 2008 with a target of no more than 50 access points in total for the civilian agencies.

As agencies reduce the number of internet connections, they are also determining whether to transition, and if so, their transition strategy, to Networx. As you know, FTS2001/Crossover Bridge contracts, which provide services for telecommunications and networking services, for current customers will expire in May and June 2010. The Networx program is the primary replacement vehicle for these expiring contracts. We believe that this transition will provide an opportunity for agencies to consolidate and optimize their external access points including internet connections and obtain secure telecommunications technologies and services. Networx Universal and Enterprise Service contracts were awarded in March and May 2007, respectively.

OMB anticipates agencies choosing to use the Networx contract can leverage the transition process and service offerings to meet the goal of reducing the number of external connections including Internet points of presence. OMB has asked the Federal Chief Information Officers (CIO) Council to prepare a cost-benefit analysis regarding the use of the Networx contract.

The Interagency Management Council's Transition Working Group (TWG) has asked agencies seeking to qualify for transition cost reimbursement to complete Fair Opportunity decisions by September 2008. GSA recommends agencies target the completion of Fair Opportunity decisions by March 2008 to ensure sufficient time to complete transition of services prior to the expiration of FTS2001/Crossover Bridge contracts.

Currently, one major agency has completed a Fair Opportunity Analysis and selected a service provider (Treasury). As of February 2008, GSA has received 21 Statements of Work (SOWs), and anticipates at least 58 more SOWs from major agencies by September 2008.

The TWG deadline for agencies to submit all transition orders is April 2010. GSA recommends agencies target the submission of all transition orders to the extent possible for January 2009 to allow sufficient time for service providers to complete the processing of all orders and establish service on the new contracts before the expiration of FTS2001/Crossover Bridge contracts.

In concert with Networx transition, Einstein will be deployed at the appropriate external connections, including Internet points of presence; 14 departments and/or agencies have currently deployed Einstein. Einstein is an intrusion detection system managed by DHS to collect, analyze, and share aggregated network computer security information across the Federal Government. As a result of these deployments, agencies maintain an awareness of their network while DHS maintains awareness of Government-wide information security threats and vulnerabilities. With this information, agencies will be able to quickly take corrective action and reduce their risk to a manageable level.

Agencies are also taking advantage of products and services offered by the Information System Security Line of Business (ISSLOB). This initiative, led by DHS and OMB was introduced in the Spring of 2005. An inter-agency Task Force identified common solutions to be shared across Government. The Task Force identified common solutions in four areas: security training; FISMA reporting; situational awareness/incident response; and selection, evaluation and implementation of security solutions.

All agencies were asked to submit proposals to either become a Shared Service Center (SSC) for other agencies, or migrate to another agency from which they would acquire expert security awareness training services and FISMA reporting services. DHS helped coordinate the selection of SSCs, and agency implementation of these services.

As of November 2007, 12 agencies had implemented security awareness training services provided by three approved SSC, and 13 agencies had begun using FISMA reporting services provided by two approved SSC. As a result, agencies are beginning to reduce duplicative investment in common security tools, ensuring a baseline level of training and reporting performance, and are able to refocus their efforts to other complex and critical security issues at their agency. OMB expects agencies will fully report the number of employees trained via the ISSLOB in their fiscal year 2008 annual FISMA report.

Finally, vulnerabilities result from weaknesses in technology as well as improper implementation and oversight of technological products. Over the past year, in collaboration with NIST, the Department of Defense, the National Security Agency, and Microsoft, we have developed a set of information security controls to be implemented on all Federal desktops which are running Microsoft Windows XP or VISTA. This set of controls, known as the Federal Desktop Core Configuration (FDCC) is currently being implemented across the Federal enterprise. By implementing a common configuration, we are gaining better control of our Federal systems, and allowing for closer monitoring and correction of potential vulnerabilities. Security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. In particular, security configurations help protect connections to the Internet and limit the download of Internet applications to only authorized professionals.

In addition to the desktop configuration, we are also working with the vendor community to make their applications safer. As part of this program, NIST has developed testing tools for use by both Federal agencies and vendors. NIST awarded Security Content Automation Protocol (SCAP) Validation to three products as of February 4, 2008. These products and their associated validation information can be found at *http://nvd.nist.gov/scapproducts.cfm*. Three independent laboratories have been accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) for SCAP Product Validation testing. The list of accredited labs is available at the same URL. We are very optimistic this program will greatly enhance the security of our Federal desktops, and, of our Federal enterprise as a whole. To help agency procurement officers ensure that new acquisitions include common security configurations, we have provided agencies with recommended procurement language. This language can be found in our Memorandum M–07–18, "Ensuring New Acquisitions Include Common Security Configurations," at *http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf*. Currently, the Federal Acquisition Council is in the process of adding similar language to the Federal Acquisition Regulation.

These initiatives described in my testimony today in combination with other administration initiatives (including: IPv6, HSPD–12, minimum communications capabilities for continuity of Government and continuity of operation plans, and IT Infrastructure Line of Business) address our potential security gaps, help agencies optimize their information infrastructure, and facilitate appropriate network consolidation and configuration. In turn, agencies will be able to better manage their information infrastructure, allowing them to reduce risks to an acceptable level.

In closing, OMB is committed to a Federal Government with resilient information systems. The dangers posed by the internet must not be allowed to significantly affect agency business processes or disrupt services to the citizen. I would like to acknowledge the significant work of agencies and IGs in conducting the annual reviews and evaluations. This effort gives OMB and the Congress much greater visibility into agency security status and progress.

While notable progress in resolving IT security weaknesses has been made, problems remain in agency implementation and new threats and vulnerabilities continue to materialize. Work remains to continue to improve the security of the information and systems supporting the Federal Government's missions and manage the risk associated with these systems. To address these challenges, OMB will continue to work with agencies, GAO, and Congress to promote appropriate risk-based and cost-effective IT security programs, policies, and procedures to adequately secure our operations and assets.

Chairman THOMPSON. Thank you very much.

The Chair now recognizes Mr. Jamison for 5 minutes.

STATEMENT OF ROBERT D. JAMISON, UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY, ACCOMPANIED BY SCOTT CHARBO, DEPUTY UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. JAMISON. Thank you, Mr. Chairman.

Chairman THOMPSON. Congressman McCaul and Members of the committee, I appreciate the opportunity to update you on the Department of Homeland Security's efforts to improve America's cybersecurity posture.

I also appreciate the committee's interest in the Cyber Initiative. The Department and our interagency partners are committed to an ongoing engagement with Congress in an appropriate setting on the classified aspects of our activities.

In my role as under secretary for the National Protection and Programs Directorate, one of my most important programmatic activities has been cybersecurity, and I have served as the lead DHS official for the Cyber Initiative since last summer.

I am pleased this morning to be joined on this panel by my esteemed colleagues from OMB, Karen Evans, and the former DHS chief information officer and just recently appointed deputy under secretary, Scott Charbo.

Secretary Chertoff identified cybersecurity as one of the Department's top priorities for 2008, and the President's 2008 and 2009 budgets reflect this priority. We are aware of, and have defended against, malicious cyber activity directed at the U.S. Government. We take these threats seriously and remain really concerned that this activity is growing more sophisticated, more targeted and more prevalent.

The nature of the threat is diverse, ranging from unsophisticated hackers to very technically competent adversaries using state-of-the-art intrusion techniques. Many of these malicious attacks are designed to steal information and disrupt, deny access to, degrade or destroy critical Federal information systems.

Over the past 4 months, the Department has provided this committee with several classified briefings on a number of different cyber-related topics, including threats. The Department and our interagency partners remain committed to an ongoing dialog with Congress in an appropriate setting on these classified topics.

DHS has the lead responsibility for assuring the security resiliency and reliability of the Nation's information technology and communications infrastructure. Since 2003, the Department has been investing in the development of a nimble, effective cyber emergency response capability and a culture of preparedness. These activities have positioned DHS to play a key role in this important initiative we will discuss today.

We have established the National Cyber Security Division to focus on securing cyberspace. In NCSD, we have built a 24×7 watch, warning and response operation centers to defend against and respond to cyber attack, the US–CERT. US–CERT has developed and deployed an Einstein program, which provides Government officials with situational awareness about malicious activity

across the Federal civilian network so we can protect against and respond to cyber threats more effectively.

Under the National Infrastructure Protection Plan framework, we have also worked closely with our private sector partners to develop 17 sector-specific plans, which all include a cybersecurity component.

We are here today because we must do more. The Federal Government has a vast information interstate system with thousands of points of access. At last count, the Federal network had at least 4,000 access points. Defending the Federal system in its current configuration is a significant challenge. Implementing effective defensive strategies requires a manageable number of access points. Therefore, we are working with OMB to reduce the number of access points.

As we reduce the number of access points, we plan to employ an enhanced intrusion detection capability, enhanced Einstein. While valuable, currently our Einstein capability is limited. We do not have comprehensive coverage, and it is a delayed flow analysis tool. We need to enhance the capability through comprehensive coverage across our Federal system external access points and upgrade Einstein to detect malicious activity in real time.

Our goal is a comprehensive, consistent intrusion detection capability that is informed by our full understanding of the threat.

Mr. Chairman, the threat is real. To defend our networks, a comprehensive situational awareness capability must augment the foundation already in place at the Department. We will achieve this improved situational awareness by consolidating our Federal connections, enhancing our intrusion detection capabilities, improving our threat assessment and information-sharing capabilities and building a stronger watch and warning system.

These changes, coupled with an investment in our people, processes and systems, will enable the Federal Government to apply the full capabilities to the defense of our networks.

Thank you for the opportunity to update you today on DHS' efforts to improve America's cybersecurity posture, and I welcome the questions.

Thank you.

[The statement of Mr. Jamison follows:]

PREPARED STATEMENT OF ROBERT D. JAMISON

FEBRUARY 28, 2008

INTRODUCTION

Chairman Thompson, Congressman King, and Members of the committee, I appreciate the opportunity to speak about the Department of Homeland Security's ongoing efforts to improve cybersecurity. I also appreciate the committee's continued interest in the Department's cybersecurity activities and in particular the Department's role in Comprehensive National Cybersecurity Initiative. As we have done since last year, the Department and our interagency partners will continue to engage with the committee and Congress in an appropriate setting on the classified portions of our activities.

As our economy, critical infrastructure, and national security become more reliant on technology, it is essential that we take proactive measures to enhance the security and resiliency of the information technology (IT) systems and networks on which we rely. We face increasing global threats to our cyber infrastructure, and the exploitation of vulnerabilities is facilitated by the widespread availability of tools, techniques, and information. The Department has made progress in enhancing

the cybersecurity of the Nation; however, we recognize the need to take deliberate action to reinforce and build on those efforts as the threat grows. To underscore the Department's efforts in this area, Secretary Chertoff has identified cybersecurity as one of the top priorities for the Department for 2008. The enacted fiscal year 2008 and the President's proposed fiscal year 2009 budget reflect the necessary investment for this priority.

The Department has outlined four areas of focus within cybersecurity to guide our efforts over the coming year. First, we are enhancing Federal cyber situational awareness, intrusion detection, information sharing, and response capabilities. Second, we are expanding the Department's cadre of cybersecurity personnel, its capabilities, and its services to our public and private sector partners. Third, we are strengthening our efforts to integrate cybersecurity into Federal, State, private sector, and international preparedness, response, and resilience efforts. Finally, we are developing and promoting the adoption of proven cybersecurity practices with Government, private sector, the general public, and the international community.

Today, I will provide an overview of the Department's efforts to improve cybersecurity across Federal departments and agencies will focus on our first priority. Specifically, I will address two programs focused on cyber risk reduction across the Federal enterprise: the Trusted Internet Connections initiative (TIC) and the EINSTEIN program.

CYBERSECURITY: A DEPARTMENTAL PRIORITY

As Under Secretary for the National Protection and Programs Directorate (NPPD), I oversee the Directorate's efforts to advance the Department's mission of risk reduction, which encompasses identifying threats, determining vulnerabilities, and targeting resources where risk is greatest, including to our critical information systems. A key area within this mission includes the Office of Cybersecurity and Communications' (CS&C) efforts to improve cybersecurity by reducing risk to the Nation's cyber infrastructure and maintaining the resilience of our communications systems. The 2007 *National Strategy for Homeland Security* articulated the importance of this mission by recognizing that many of our essential and emergency services, including our critical infrastructure, "rely on the uninterrupted use of the Internet and the communications systems, data, monitoring, and control systems that comprise our cyber infrastructure. A cyber attack could be debilitating to our highly interdependent [Critical Infrastructure and Key Resources] and ultimately to our economy and national security."

Global threats to our cyber infrastructure and to the services, systems, and assets that depend on them continue to increase. The nature of the threat is large and diverse and ranges from unsophisticated hackers to very sophisticated adversaries. We are seeing more state-of-the-art intrusion techniques designed to disrupt, deny access to, degrade, or destroy critical information systems and steal our intellectual capital and proprietary information.

The Department is positioned to address these threats through our watch, warning, and response capabilities; our information sharing and coordination efforts with the public and private sectors; and our programs and initiatives through the National Cyber Security Division (NCSD) and United States Computer Emergency Readiness Team (US–CERT). These programs and initiatives are designed to carry out our mission of preparing for and responding to incidents that could degrade or overwhelm the operation of our Federal IT and communications infrastructure.

SECURING FEDERAL DEPARTMENTS AND AGENCIES

Since its inception, the Department of Homeland Security has been working to strengthen Federal and critical infrastructure systems and enhance our cyber operational response capabilities. The Department established a number of programs and initiatives to coordinate efforts with Federal departments and agencies to improve cybersecurity. These programs focus on enhancing situational awareness, increasing collaboration across Federal operational security teams, preventing cyber incidents, and providing inter-agency coordination during a cyber event.

The Department conducts outreach to Federal departments and agencies to raise cybersecurity awareness with operational security teams and senior official through channels such as the Government Forum of Incident Response and Security Teams (GFIRST). GFIRST is a community of more than 50 incident response teams from various Federal agencies working together to improve Federal Government security. The Department sponsors the annual GFIRST Conference, which fosters greater information sharing among IT security professionals from various departments and agencies. The 2007 conference garnered unprecedented attendance, including more than 550 IT professionals, representing numerous Federal departments and agen-

cies, including more than 100 attorneys from the Department of Justice. We expect similar success at the upcoming GFIRST Conference in June 2008.

To enhance collaboration on control systems security across the Federal Government, NCSD established and facilitates the Federal Control Systems Security Working Group, consisting of over 30 Government organizations. Since late 2006, this group has been developing a Federal Coordinating Strategy to Secure Control Systems, which seeks to place related Federal control systems activities into a unified framework, assess opportunities for sharing and leveraging information and resources, and identify possible gaps in Federal efforts. In addition, NCSD is working with other Federal organizations, such as the Tennessee Valley Authority and the U.S. Army Corps of Engineers, to provide control systems specific tools in their areas of responsibility.

NCSD co-chairs the National Cyber Response Coordination Group (NCRCG) with the Department of Justice (DOJ) and the Department of Defense (DoD) to coordinate response to a cyber incident across the Federal Government. The NCRCG serves as the principal interagency mechanism for providing subject matter expertise, recommendations, and strategic policy support to the Secretary of Homeland Security during and in anticipation of a cyber incident. The NCRCG comprises senior representatives from Federal agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from cyber incidents. The senior-level membership of the NCRCG helps ensure that during a significant national incident, appropriate Federal capabilities will be deployed in a coordinated and effective fashion.

To ensure processes and procedures involved with response to cyber incidents are up-to-date and comprehensive, the Department sponsors exercises to allow participants in the public and private sector to examine their cyber response capabilities. In February 2006, the Department held the first National Cyber Exercise—Cyber Storm—to examine various aspects of our operational mission, including collaboration with Federal departments and agencies. The Department and other participants continues to address lessons learned and after-action items from the exercise. Progress made to improve response processes and procedures will be measured in Cyber Storm II, which is scheduled for March 2008. Cyber Storm II will simulate a coordinated, large-scale cyber attack on four of the Nation's critical infrastructure sectors. The exercise will include participants from 18 Federal departments and agencies, 9 States, over 40 private sector companies, and 4 international partners. For the Federal Government Cyber Storm II will exercise strategic incident response decisionmaking and interagency coordination in accordance with national-level policies and procedures. The exercise will strengthen the ability of participating organizations to prepare for, protect against, and respond to the effects of cyber attacks.

US–CERT is the Department's watch and warning mechanism for the Federal Government's internet infrastructure. It provides around-the-clock monitoring of Federal network infrastructure and coordinates the dissemination of information to key constituencies including all levels of Government and industry. In addition, US–CERT serves as the main component for helping Government, industry, and the public work together to respond to cyber threats and vulnerabilities. A main area of focus for US–CERT is our work with Federal departments and agencies. US–CERT provides Government partners with actionable information needed to protect information systems and infrastructures. In addition, US–CERT leverages its technical expertise to further efforts to secure Federal networks and systems through targeted programs, such as the Trusted Internet Connections (TIC) initiative and EINSTEIN.

Trusted Internet Connections Initiative

The Trusted Internet Connections (TIC) initiative is a multifaceted plan to improve the Federal Government's security posture by significantly reducing the number of Federal external connections. External connections include, but are not limited to, any connection outside a department or agency, such as government-to-government connections and Internet access points. Currently, there are several thousand Federal external connections. The existence of such a large number inhibits the Federal Government's ability to implement standardized security measures effectively. The TIC initiative aims to reduce and consolidate the number of external connections to create a more clearly defined "cyber border." Fewer external connections will enable more efficient management and implementation of security measures and reduce avenues for malicious attacks. Once fully implemented, the TIC initiative will facilitate security standardization for access points across the Federal Government.

The Office of Management and Budget (OMB) maintains oversight of the TIC initiative, and implementation relies on the technical expertise of US–CERT, all par-

ticipating Federal departments and agencies, and the Information Systems Security Line of Business (ISS LOB). The ISS LOB is part of the President's Management Agenda to expand Electronic Government. The goal of the ISS LOB is to address those areas of information security which are common to all agencies and are not specific to the mission of any individual agency, ultimately resulting in improved information systems security. OMB has selected DHS as the managing agency for the ISS LOB, and DHS, through the NCSD, is leveraging its role in the ISS LOB to enhance the TIC initiative.

OMB announced [1] the TIC initiative to the heads of Federal Government departments and agencies in November 2007, subsequently outlining the specific steps departments and agencies should take as part of the initiative, including compiling a comprehensive inventory of each department and agencies' existing network infrastructure. Each department and agency is required to develop a Plan of Actions and Milestones (POA&M) to reduce and consolidate the number of external connections with a target completion date of June 2008. NCSD is in the process of reviewing initial POA&M submitted to NCSD, via the ISS LOB, for review to ensure completeness and alignment with the goals and objectives of the TIC initiative. In addition, US–CERT and the ISS LOB created an interagency technical working group to establish, for OMB's approval, a list of requirements and standards for the implementation of each TIC. Once approved, these requirements will be passed to the department and as for implementation.

The reduction of external connections will have a number of benefits for the Federal Government, particularly when coupled with other security measures. First, fewer external connections will provide the ability to establish a central oversight and compliance function. This central function will benefit Federal systems by facilitating the implementation of standardized information security policies. In addition, the TIC will enable the implementation of 24-hour watch and warning capabilities across the Federal Government and enable faster and more effective response to cyber incidents. The TIC will also enable the rollout of an intrusion detection system across Federal networks to provide better situational awareness, earlier identification of malicious activity, and overall, a more comprehensive network defense.

The EINSTEIN Program

The EINSTEIN program is another critical element of our efforts to increase cybersecurity across Federal departments and agencies. EINSTEIN is a collaborative information-sharing program that was developed in response to increasingly common network attacks on and disruptions to Federal systems. The program was initially established to help departments and agencies more effectively protect their systems and networks and to generate and report necessary IT-related information to US–CERT. EINSTEIN enhances situational awareness of the Federal Government's portion of cyberspace, allowing US–CERT and cybersecurity personnel to identify anomalies and respond to potential problems quickly. EINSTEIN is presently deployed at 15 Federal agencies, including the Department of Homeland Security, and US–CERT is in the process of deploying EINSTEIN across all Federal departments and agencies. With the TIC initiative providing a reduced number of external connections, EINSTEIN will be able to more effectively monitor activity across Federal Government networks.

The EINSTEIN program supplements departments' and agencies' intrusion detection systems by monitoring their networks from outside their firewalls, 24 hours a day, 7 days a week. EINSTEIN utilizes an automated process for rapidly collecting, correlating, analyzing, and sharing government computer security information with US–CERT and department and agency system administrators. EINSTEIN utilizes a specific tool set to analyze network flow, which is comprised of a brief summary of a network connection, including source, destination, time, bytes, and packets transferred.

US–CERT deploys EINSTEIN to Federal departments and agencies, along with all necessary hardware, software, support services, and staff training. Once implemented within a Federal department or agency, EINSTEIN identifies and establishes a baseline for normal network operational activity. From this baseline, security personnel are able to identify unusual network traffic patterns and trends, such as configuration problems, unauthorized network traffic, network backdoors, routing anomalies, and unusual network scanning activities. With this information, security personnel can quickly identify, prevent, and respond to potential problems.

EINSTEIN analyzes the information collected and posts it to a secure internet portal, which only approved personnel can access. System administrators from participating departments and agencies review their data and determine if any mitiga-

[1] The TIC was announced in OMB Memorandum 08–05.

tion activities are necessary, often in collaboration with US–CERT. Simultaneously, US–CERT personnel analyze the data from participating department and agency networks to determine if any recurring patterns and trends exist, potentially indicating the presence of malicious cyber activity targeting the Government as a whole. If US–CERT finds such patterns of unusual activity across multiple agencies, US–CERT notifies appropriate stakeholders and coordinates mitigation and response actions as necessary.

EINSTEIN already has proven successful in enhancing security within the Federal Government. For example, through the Department of Transportation's (DOT's) participation in the EINSTEIN program, we were able to quickly detect malicious activity and prevent it from infecting other government computers. In this case, a computer worm had infected an unsecured government computer in a U.S. Government agency. When the worm, in its attempts to increase its network of infected computers, tried to attack DOT's network, EINSTEIN detected the unusual traffic. After further investigation, US–CERT discovered the worm and worked with the affected departments and agencies to prevent its spread.

EINSTEIN reduces the time it takes to gather and share critical data on computer security risks from an average of 4 to 5 days to an average of 4 to 5 hours. Quick notification results in the Federal Government being able to respond to incidents and mitigate potential problems more efficiently and effectively. Government-wide deployment of EINSTEIN will further enhance the ability of US–CERT to gain a more comprehensive view of Federal systems, increasing US–CERT's analytic capabilities and augmenting the extent and quality of US–CERT's information sharing activities. Together with the TIC, broad deployment of EINSTEIN will increase our ability to address potential threats in an expedited and efficient manner.

CONCLUSION

Securing the Nation's IT systems and networks in an environment of increasing global threats by agile and sophisticated adversaries is a difficult challenge that requires a coordinated and focused effort. Secretary Chertoff's prioritization of cybersecurity for the year ahead underscores the importance of this challenge. Accordingly, the Department is working with its Federal partners to develop and implement a holistic strategy for securing our Federal networks and systems.

We have established a strong foundation of programs and activities to address the dynamic threat, and we continue to expand and improve upon those programs through new and enhanced efforts. The TIC's reduction of Internet access points and EINSTEIN's situational awareness capabilities are examples of initiatives designed to prevent the disruption of Federal critical infrastructure from unauthorized users that penetrate Federal systems and steal or compromise vital or sensitive information.

Government-wide deployment of TIC and EINSTEIN enables strategic, cross-agency assessments of irregular or abnormal Internet activity that could indicate a vulnerability or problem in the system. These programs enhance Federal Government cybersecurity by providing more robust security monitoring capabilities to facilitate the identification and response to cyber threats and attacks. They contribute to the improvement of network security, increasing the resilience of critical electronically delivered government services, and enhancing the survivability of the internet.

The Federal Government is committed to increasing its capabilities to address cyber risks associated with our critical networks and systems. Every Federal department and agency plays a role in and adds to the protection of our Nation and its citizens from cyber threats.

Thank you for your time today, and I am happy to answer any questions from the committee.

Chairman THOMPSON. Thank you very much.

I thank the witnesses for their testimony.

I now remind each member that he or she will have 5 minutes to question the panel.

I now recognize myself for the first set of questions.

Mr. Charbo, we had a hearing in June of last year where Mr. Langevin chaired the subcommittee, and it was quite revealing that a number of attacks had occurred on our system, and perhaps we were not as notified, or you and your Department, of many of those attacks until a contractor informed you of that. The infa-

mous, "You don't know what you don't know," comment was in response.

Now, to the extent possible, since that hearing, can you give this committee the follow-up as to what you have instituted in your previous position and this present position to prevent such attacks?

Mr. CHARBO. Thank you, Mr. Chairman.

At that hearing, we were asked about some of the security notifications that we have had on our networks through our intrusion detection systems. In 2005, we looked at the current contract that we had on those local networks. We identified gaps, and we put dollars in place to fill a lot of those gaps, including putting contract support in place for that. We also identified a need to recompete that contract, which we have done.

It is true that at the time of that hearing, I had not been read into any of the specific threat vectors that are in place and that we are now aware of. The first briefing that we did have was with OMB—that was to the general CIO Council, and since that, we have had follow-up briefings. This initiative has caused a number of briefings, and my staff and I have also gone out and pretty aggressively looked toward any sources we can to identify briefings that get beyond a sensitive but unclassified or even a secret level.

At the time, we said, "We are only focused on the data. That is all we can look at in terms of data of intrusion sets, et cetera, to identify anything back to whether it is a nation state attack or what is the nature of the vulnerability." We are still in that phase. There's a handful of issues that we are continuing to look at. Those in a classified state. We take every security incident very seriously at the operation.

At the Department of Homeland Security, we have instituted several issues since I have started at that Department. The one we have spoke about many times is OneNet. We have said very publicly, "That is the most important IT project that we can put in place at the Department." That is a consolidation of a wide area of points of access. It mirrors very closely to what the TIC effort is about.

We want to put state-of-the-art intrusion detection at those access points that includes Einstein and other services. We have put that in place. We have put a security operations center in place that is 24×7.

We are beginning to peer to those from our different components at the Department. We have raised the classifications of the CIOs, of our security, administrators, of our network administrators, of our deputy CIOs so that no longer are they just getting an unclassified brief. Quite honestly, what you get in that state is just a piece of information that is very difficult to interpret back to any attribution at all or to identify what the gaps are.

What makes it even more difficult at the Department of Homeland Security is we are an immigration agency, which we have clients from outside of this country who are trying to receive information on our public points of access, as well as law enforcement points, as well as border and port agencies. So we have done a number of things before the hearing, since the hearing in order to shore up our security operations at the Department, including doing a number of recompetitions and rebuilds of certain applica-

tions, moving it to our points of access, which were part of the OneNet project.

Chairman THOMPSON. Thank you. We will come back to some other questions.

I yield to the Ranking Member for questions.

Mr. MCCAUL. Thank you, Mr. Chairman.

I just want to follow up on the Chairman's line of questioning, because at the last hearing, when you testified, it did raise some serious concerns. You are the chief information officer for the Department of Homeland Security. There is a major threat of intrusion into our Federal networks, and yet you are not read into, as you said, read into the threat factors at the time. I understand you didn't know what you didn't know, but who was responsible for ensuring that you had that information, that didn't get you that information that you should have had?

We talk a lot after 9/11 about silos and not connecting the dots, not sharing information, and yet we have what I consider to be a major breach at the Federal level of not sharing information that should have been shared with you. I mean, you are the CIO of Homeland Security, and you didn't have this threat factor information.

Can you tell me what happened? Then I think you explained what you have done to correct that; that is the good news. You had a clearance, I assume, at the time. But you said you have upgraded now all the CIOs, they have the clearance to share that information.

What happened back then?

Mr. CHARBO. It is difficult to tell what happened, sir. The briefings that we get are on a compartmentalized basis. They are tear lines between information moving down from classifications level. Most of the information that we got prior was at an unclassified level. At that point, it is very difficult to interpret that.

If I can bring this back to the hearing point, in terms of the enterprise network, I think this is an issue that is going to have to be addressed across a lot of the components—raising classification levels, moving information onto secure networks and not trying to do this on our unclassed networks—and that is going to be a training, a clearance issue, a network issue. We have addressed that.

Once we do have the information at Homeland, I think we have moved very aggressively in terms of raising the visibility with our key points. We have taken that to mean our CIOs within the Department, our security officers within the Department, our network administrators. We can bring together in classified settings, action those and then task those on in an unclassified point of presence.

All I can say is, prior to that there were gaps in that.

Mr. MCCAUL. You suffered from that gap, obviously, and I think as we move forward with this initiative and as Congress provides its oversight in how best to implement this initiative, that has got to be one of the key factors to make sure the CIOs for each of the major Federal agencies involved with this initiative are certainly read into the classification level to share that kind of threat information. I mean, we have gotten the reports that the Federal Government has had massive intrusions into its Federal networks, and

it seems to me the CIOs of these agencies should be aware of that fact to better protect itself.

I know this is part of the initiative, but I would encourage you to make this a priority in this initiative, and we will be looking at that issue.

Mr. Jamison, did you have a comment?

Mr. JAMISON. Yes, sir. Congressman, you are exactly on point: This is one of the fundamental challenges that we are facing, and a lot of the threat information was extremely classified. What we are talking about trying to do is get comprehensive situational awareness.

So as we improve our Einstein deployment, improve intrusion detection, we are also coordinating with our intelligence components and all of the Federal Government agencies that have threat information so we can get more real-time information to the CIOs and to the network operation centers and security operation centers so that they can take defensive action. That is the top priority.

Mr. MCCAUL. My second question is, under this initiative—I am a believer in clear lines of authority. When you have these mergers and partnerships and sharing agreements and what not, you need to know who is in charge and who is in charge of the budget.

Under this initiative, can you tell me—maybe Mr. Jamison—who is in charge here?

Mr. JAMISON. Sure. First, let me caveat this statement by, I would be happy to give you a detailed briefing on the full budget, including the classified parts in a close session.

For what we are talking about today, for the TIC consolidation, we share the lead with OMB on helping them consolidate internet access points, but we have the lead to deploy the intrusion detection, to own, operate and manage the intrusion detection and come up with that comprehensive situational awareness picture.

There are many more parts to this initiative that I can't discuss openly in this forum and would be happy to give you a classified briefing on that.

Mr. MCCAUL. I understand that. I think at one of the hearings that the Chairman of the subcommittee, Langevin, and I had, we had testimony that the DHS was not really coordinating, certainly as well as we would hope, with the Department of Defense, and I know that may be getting into a classified area. I hope that is an area that will be focused on as well. They certainly have great expertise in this area that I think the DHS could be of great value to you in terms of the coordination. So I certainly hope that takes place.

Then, last, we heard about the declassified operation, Aurora, where the Idaho National Labs found a vulnerability where a power grid could be shut down, exploited, with the click of a mouse. That causes, obviously, shockwaves, I think, through not only in the Federal Government but also the administration and the Congress, in terms of the vulnerability.

That is great work, though, in terms of detecting that vulnerability and fixing it.

Can I hear from you maybe some of the lessons learned from this project and what you are doing to protect the United States?

Mr. JAMISON. Sure. I think it was a success story. I think, as always, when you look back there is always room for improvement. But what happened with the Aurora vulnerability is research that was funded by the Department of Homeland Security through our lab networks identified the vulnerability. Once we identified the vulnerability, we worked through the national security infrastructure protection process and our interagency partners to validate that there was a vulnerability and actually develop mitigation plans.

We developed those mitigation plans and tested those mitigation plans and actually came up with a dissemination plan within that NIPP framework, leveraging both our interagency partners and the Federal Government and our private sector partners and drove those implementation plans.

We continue to monitor the implementation plans. We are pleased with the results. What we must continue to do is make sure that we are able to validate that those measures are still being taken in the field and we continue to pursue enhanced cybersecurity.

But I do think it was a success story, especially given the fact of the sensitivity of the information and the challenges with trying to get implementation measures down the field while you don't highlight a vulnerability, and I think the system worked.

Mr. MCCAUL. I agree with that and look forward to hearing more about it.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

I now recognize the gentleman from Rhode Island and Chairman of the subcommittee for 5 minutes, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. I appreciate you yielding, and I appreciate the witnesses for their testimony. I have deep appreciation for the Chairman's line of questions, as well as the Ranking Member, about who knew what when and this issue of silos.

Obviously, the Department of Homeland Security being the lead agency for security needs to know what threats we are facing and making sure that the dots are connected, and I haven't been satisfied previously that that had been happening. I hope that this is changing, and we heard some of that in your testimony today.

I am not going to go on about that, but I will say, obviously, for years now, our Federal networks have been under attack, and I believe that the infiltration and exploitation of these networks is one of the most critical issues confronting our Nation. The acquisition of our Government's information by outsiders undermines our strength as a Nation, and if sensitive information clearly is stolen and absorbed, our systems are hacked by our adversaries, clearly, we are strategically harmed.

I don't believe that this administration, at least up until now, has made cybersecurity the priority that it should be. I believe that is starting to change, and with the right vision and leadership, I believe we can improve security of our Federal networks and our critical infrastructure.

There are some promising elements of the Cyber Security Initiative, but there are still some gaping holes, and I just want to as-

sure the American people that under Chairman Thompson's leadership and the work that we are doing on our subcommittee that we are going to continue to perform robust oversight of this issue.

In terms of questions, in terms of what I see as gaps, what I want to know is, how many and what kinds of connections does the trusted internet connection cover? For instance, does the TIC cover government-to-contractor network connections? Because we know that it is not only about the security on networks but authorized intrusions. We need to be secure about that.

We had problems right at the Department of Homeland Security where we had contractors plugging unauthorized laptops into our own network, which you have viruses on there that infiltrate our networks. So you could be securing your networks but if you have unauthorized access, that is a problem.

Also does it cover Federal-to-State and local connections? What about public service e-gov Web sites, such as student loans at the Department of Education or Social Security or the IRS e-file site? How about law enforcement internet connections used for investigative purposes?

So I would like you to answer that, as well as what will the Cyber Initiative do to secure federally owned or privately owned critical infrastructure, such as nuclear power plants and the electric grid from cyber attacks? As part of the TIC consolidation, will you consolidate connections between federally owned critical infrastructure and the internet? In other words, will dams operated by the Bureau of Reclamation or power plants operated by the TVA consolidate their connections, and will you install Einstein on these connections?

Ms. EVANS. I would be happy to answer the first part of the question, which is, what types of connections, and the way that we are approaching it is, it is all external connections.

As you clearly outlined, any external connection to an entity causes or poses a risk. So all agencies were required to report back to DHS by the guidance of OMB to tell how many external connections, and that is all of them, whether it is going to a Federal contractor, whether it is your internet point of presence, whether it is a direct connect between you and another. If it is external to your operation, it counts and it is being looked at as part of this effort.

Because we need to manage the risk associated with those, because this is a shared responsibility of managing the risk by department, by department. They all have to look at what type of information they have, what type of services they are providing and then manage the risk accordingly to that.

So they have all reported in. We gave them a reporting template. We have the number baseline of connections that they have right now so that we can then move to optimize those going forward.

Mr. LANGEVIN. And the second part of the question?

Mr. JAMISON. I will just follow up on the critical infrastructure.

As Karen mentioned, we are focused on all external connections and getting those external points solidified. The initial focus of the effort is to get the dot-gov networks under stronger intrusion detection management and situational awareness.

We are continuing our dialog through the NIPP process on critical infrastructure and how we better manage cybersecurity in

those areas. We will continue to engage them and develop a stronger plan, and some of those initiatives we will be happy to talk in more detail about in a classified session.

Mr. LANGEVIN. That is promising. We are going to continue to follow up on that.

Mr. Chairman, with your indulgence, I do have one last question. Have we ever done a full damage assessment of Federal agency networks or DHS networks? If not, why not, and will this be covered under the Cyber Initiative?

Mr. JAMISON. Not to my knowledge that a full damage assessment has been done, but I will say that we investigate known intrusions and make sure that each agency follows up and has that responsibility, and Karen may want to go into more detail about that.

US–CERT has played a support role in investigating intrusion activity and making sure that we follow up with damage assessments from known intrusions.

There is a broader effort to do a more detailed risk assessment, as we move forward with this initiative on the total risk picture for the Federal Government, as we address those risks.

Karen, you may want to follow up on that.

Ms. EVANS. I would like to clarify a couple of pieces here. One, under the FISMA, Federal Information Security Management Act, agencies do need to do an assessment right off the bat on all their systems, and the guidance has been given out to the agencies, and we report on this on an annual basis. So all systems are categorized by high-, medium- and low-risk, and we report on that. Then they all have to do testing, have security controls in place and then also then evaluate what that is. So we report on that on an annual basis. That report is due March 1 every year.

Mr. LANGEVIN. If I could just stop you there, because that is a risk assessment. That is different than a damage assessment.

Ms. EVANS. I am going to get there.

Mr. LANGEVIN. Okay.

Ms. EVANS. So the second part of that is, as a result of the loss of data that happened at the VA situation with the personal identifiable information, we put additional procedures in place so that as agencies have things happen—we also now have a BPA available for all agencies so that they can then do an assessment after the fact so that they can then go in and see how much damage has actually occurred, what they are supposed to do.

The policy is in place, they have teams that are in place at the highest levels of each department so that as they lose data, they are supposed to assess it, what is the risk associated with that, and then take proper precautions and proper notification associated with it.

Mr. LANGEVIN. Okay, but that is prospectively. You are saying that we have not and we are not going to do a damage assessment——

Ms. EVANS. No, sir. They need to do a damage assessment each time things—that is how the policy is set up now. So they do an assessment as each incident occurs and as they report the incidents in. So they report incidents into US–CERT. They have to make an assessment at that point depending on the type of incident, by the

categories we have, and then they have to continue on doing the assessment. You are calling it a damage assessment; we call it a risk, data breach type of assessment so that they can then take the appropriate actions.

That is whether you turn it over to law enforcement, whether you have to notify individuals for the services that you have done if their information may have been compromised or notify your partners so that they are aware of what has happened within your entity to be able to share for more awareness across the board.

So we have enhanced our procedures to make sure that that is being done on a consistent basis.

Mr. LANGEVIN. I yield back, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

We now yield 5 minutes to the gentleman from Pennsylvania, Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman.

My question is to Mr. Jamison.

Mr. Jamison, I guess my first question is, who is in charge of the Cyber Initiative and who is going to hold the budget authority for it?

Mr. JAMISON. Congressman, for the portions that we are talking about today, with the TIC consolidation, we share the lead with OMB, but the $115 million budget supplemental that addresses this issue of deploying Einstein and dramatically ramping up our comprehensive situational awareness, DHS has the budget authority for that and are owning, operating and managing that equipment.

I would be happy to go into more details in follow-up briefings on the rest of the classified budget and who has the leads for the other pieces.

Mr. DENT. I guess in a follow-up to that question, if the initiative is spread across the entire Government, who is going to have the ultimate control over how everybody is working together? Obviously, Mr. McCaul pointed out some gaps and people not knowing things that they needed to know, apparently, so who is going to have that ultimate control to make sure that people are actually working together on this?

Mr. JAMISON. Let me answer the question in a couple of ways. The director of national intelligence has a coordination role for all aspects of the initiative to help coordinate the project management of those initiatives. Each individual agency that has authorities and responsibilities under the initiative have that responsibility.

We would be happy to come back in a classified session and give you a lot more details on that aspect.

The Department of Homeland Security plays a key role in the protection of the dot-gov and Federal networks from an Einstein perspective and has a lead role in that. We also have a coordination role across the cybersecurity domain, and we would be happy, as that develops, the plan for that develops, to come back up in a classified session and lay out in detail how that coordination role is going to be played out to coordinate all of the activities across the Federal Government.

Mr. DENT. Thank you for that answer.

It is also my understanding that US–CERT is going to be able to view the content of communications over government networks. I guess the question is, why is this important, and what information will they be collecting, and what will they do with it?

Mr. JAMISON. First of all, if I may, I brought a couple of props with me, if I can ask one of——

Mr. DENT. Please.

Mr. JAMISON [continuing]. My employees to come up. I would like to, kind of, explain to you what the differences are.

So if you get the other two first, I want to show this.

Mr. DENT. We can't see that, by the way. Well, maybe some of you can but not me.

Mr. JAMISON. Can you take it up to the Congressman?

Our current Einstein capability is a flow analysis tool, so if you look at the current Einstein flow records, this is the basic information that Einstein captures: IP addresses, the size of data packets and where is information is flowing from network to network. We capture that and then once day, or routinely, we download it. The other chart shows you the types of analysis that we do on that information.*

So we are trying to detect patterns, we are trying to detect malicious IP addresses and to do analysis on activity that would look suspicious or have malicious intent. It is delayed and our effectiveness—and we have got good analysts—but our effectiveness is limited to how good our analysts are.

Where we want to go is we want to be able to detect the malicious code that we know about. When an adversary or an intrusion has a signature of malicious code, we want the sensors to be able to scan for that malicious code and alert us when we know that we have malicious activity.

Let me point out that this is no different than intrusion detection capabilities that are on Federal systems today. They all have commercial capability to do intrusion detection. What is different is that we are going to have comprehensive coverage of our external points to make sure that we have got intrusion detection at all those points.

We are also going to make sure it is consistent so the same intrusion detection is consistent, and it is going to be informed by the knowledge of the Federal Government of what we know about the threat, so we will have the latest signature information on the threat comprehensively across the Federal Government.

So it addresses some of the concerns that I have heard from the committee today about not knowing all the threat avenues and one agency knowing more threat information than another. This is the intent, to get to comprehensive situational awareness.

Mr. DENT. Thank you.

Real quickly, the specific role of US–CERT, the administration is requesting, I guess, about $100 million more than was enacted last year, and so I guess the question is, how are you going to spend this US–CERT money?

Mr. JAMISON. It really breaks down into a couple of different components. The majority of it is in deploying the equipment, so

*Copies of the charts have been retained in committee files.

the intrusion detection equipment to the sites. We also have a large chunk of money, about $43 million, for the 2008 budget in facilities as we ramp up our capabilities to add more people.

We have to build the backend analytical capabilities. So just as I have shown you, some of the analysis has to be done on flow records. We need to build our capability to do analysis on that, to handle a much larger percentage of the traffic. Currently, our Einstein capability handles a very, very, very small percentage of the Federal Government traffic. We want to expand that to 100 percent through this initiative, so we have to back up our analytical capability.

It also will allow us to build our malicious malware analysis labs and those things and expand them to handle the additional volume.

Those are the major components.

Mr. DENT. Thank you. I yield back.

Chairman THOMPSON. Thank you very much.

We now recognize the gentlelady from California, Ms. Harman, for 5 minutes.

Ms. HARMAN. Thank you, Mr. Chairman, and thank you for holding this hearing.

As I think the witnesses know, Members of this committee have received a number of classified briefings on the threat. Obviously, we are not discussing the threat here, but since my focus over all my years in Congress, all 100 years that I have served in Congress, has been on security threats, I take that kind of information very seriously, and I think the threats are substantial, starting with hackers but going on to much bigger threats.

I have been sitting here with my mouth open. I think that this hearing reminds me of FEMA trailers, the Government doing something and 2 years later deciding that it is toxic and taking it away. I think while all of you are well meaning and working hard at your jobs, the fact that you don't have the threat information and that you are working on projects that will take years to complete is absolutely shocking. Let me repeat that: I think it is shocking.

If we are serious about these threats—and I am serious about these threats—we are not being serious about our response to the threats. It is not timely, I don't get any sense of urgency, I don't think much of it will work.

As an example, as we all know, most of the cyber network is in the private sector. I think, absolutely, everybody knows that. You have been talking about private sector collaboration and cooperation. My understanding is the private sector considers Einstein too passive, and it doesn't deliver information in real time.

So how is it that we are going, in real time, have a response to a very significant threat? I just don't see it happening. I don't see DHS being able to do it within DHS, let alone coordinate a response across our Government. So I am sitting here really concerned about that.

Second, I hear from constituents all the time in my district. They are really aware of programs that involve having access to personal information of American citizens. Obviously, for this program to work, as you have been discussing, there has to be some collaboration with some of our security agencies, like NSA and DOD.

I have no doubt that you are working on, and that we have been briefed on, some legal protocols about all that and that there is an effort to protect privacy. However, I assure you that constituents of mine listening to this hearing—and I am sure they are all tune in, even though it is pretty early in California—are thinking about this as, "Government sets up new spy network." That is how they are going to receive this information.

So let me ask you to respond—all of you—to what I have just said, two parts. No. 1, is this in real time and fast enough to mount a serious response to a serious threat? No. 2, what would you advise me to tell my constituents who are going to call me this afternoon and ask me how I am going to stop this latest government spy network into their personal privacy?

Mr. JAMISON. Thank you, Congressman, I will address those. The previous charts I put up were trying to get exactly to that point. Obviously, I could do a better job of explaining it. But I would say that right now our Einstein capability is passive. We are looking at flow records, we are not looking for malicious activity, we are doing it after the fact, and we want to move that to real-time intrusion detection capabilities. So we want to make sure we lock down our nodes of access to the Federal Government and give ourselves real-time malicious activity intrusion detection.

So that is exactly the intent of this. We are aggressive about it. We are going to be employing—as we ramp down the number of locations, we are going to be deploying that equipment this year. As you can tell by our budget request, we have ramped up our capabilities to respond to that.

Second, on the privacy issue, I can tell you one thing: First of all, privacy and civil rights has been a top priority for this. We have had our privacy folks and our civil rights folks involved in this from the very start. Current Einstein has a privacy impact assessment that is public. We are currently in the process of doing a privacy impact assessment for the new capability as we move it forward, as well as full legal review, and we take that matter very seriously.

But I would like to add that the capability that we are talking about for detecting that malicious activity in real time is no different than a commercial intrusion detection capabilities at many agencies and every corporation in America has on their systems. The issue is, it is going to be comprehensive, it is going to be consistent, it is going to be informed by our threat information.

Ms. HARMAN. It is going to be massive, and it is going to be across the Government and possibly across the private sector. So it is a little bigger than any of the other networks or tools that individual companies have, right?

Mr. JAMISON. We are not talking about the private sector right now, we are talking about the Federal Government node and the traffic coming into the Federal Government.

Ms. HARMAN. Got it.

Other people have any answers to my two questions?

Ms. EVANS. Yes, ma'am, I would like to answer those questions as well.

In everything that we are talking about and even on the threat information and the vulnerabilities that we are all aware of, this

all starts with a defense in depth. There is no silver bullet, we all know that, and so there are several things that the agencies are doing that, first and foremost, most of these come from exploiting known vulnerabilities and through configuration management.

There is a very extensive effort, and I mentioned this in my testimony and we did this jointly with the NSA, which is set up the way that FISMA was intended where they would do standards in an open setting, and then we would go through the process that the Commerce Department has. So we have set up 700 settings that then reduce the vulnerability and then make sure that what we are doing is building that in right up front.

So some of these things that are common sense we are going ahead and trying to take care of that on a mass basis. That is also then going to be built into the computers that get delivered to the agencies. So in spite of themselves, they will be successful, because they will be coming configured securely. That is the first thing that we are doing, because those things we should take those right off the table, and that should not be an issue.

The other thing that the agencies are doing are also encrypting all their data—data at rest, data that is mobile—so that should that happen, that then it becomes harder. So you are raising the threshold up.

Then we are also using two-factor authentication, which then makes sure that people who are authorized, you know that those are the people who are supposed to be on your networks.

So we have these in place. The agencies are rolling out, they have these measures, they are implementing these, and they are upgrading their security as they go forward.

As part of privacy and security, that is an administration concern, has always been. It is a high priority, and we have been doing all of these activities in a very transparent way, so that everyone can comment on what we are doing. The privacy impact assessments are out there. We put it through the Federal Register notice process so that it is done in a very transparent way to make sure that the citizens know how we intend to protect that information.

Ms. HARMAN. Did you want to comment?

If he could just finish his response, I would appreciate that. Thank you.

Mr. CHARBO. I would just add that the Einstein program is only a part of the total cyber effort. We are really focused on also changing the way networks are operated. That is down at the operator level. In terms of just their situational awareness, their training and how they react and respond on a daily basis to operations, as well as to how we procure, how we also configure the different things, which Ms. Evans just went into.

Chairman THOMPSON. Thank you.

The gentleman from Georgia, Mr. Broun.

Mr. BROUN. Thank you, Mr. Chairman.

I would like to just go a little further with a question that Mr. Dent asked you all.

Secretary Jamison, it is my understanding that you all can view the content of all the dot-gov connections, and I am concerned about privacy too, as Congresswoman Harman is. We have had your folks from civil rights as well as the privacy protection of DHS

come testify before this committee, and the question I have or frustration I have is, I don't really see beyond just DHS how folks in my district, privacy is really going to be protected. It looks almost like the fox guarding the henhouse, proverbially.

As a United States Marine, I am very concerned about the security of this Nation, and as an original intent constitutionalist, I believe that national security and what you guys are doing is the prime purpose of the U.S. Government. But I am not convinced, as I think Ms. Harman is not convinced, that privacy is going to be protected in the process of developing these cyber protections within the government connections.

I encourage you to try to find something beyond Einstein that is going to be focusing on the bad guys and not focusing just on the general public but finding some way to protect the privacy of American citizens, the good guys. As I see DHS developing these policies, when I go through security at airports or all these other things, it just looks to me as if we are focusing more of our resources, which are very limited, more of our personnel, greater and greater bureaucracy on focusing upon all us good guys and not on the bad guys.

Can you assure me or tell me how you all maybe can go to Einstein 2.0, or whatever the system is, that is going to protect the privacy rights of American citizens, the good guys, and make sure that we don't have these security threats within the cyberspace of the dot-gov connections?

Mr. JAMISON. Thank you, Congressman.

First of all, let me say that this is a comprehensive initiative, and there are a lot of agencies involved, and it has a comprehensive plan. We want to make sure that we have the opportunity to brief that to you in full in a classified session.

From the standpoint of privacy, it is a top concern. We are currently not looking at content, as you put it. That is where we need to go.

Mr. BROUN. Not looking at any content.

Mr. JAMISON. Not currently. We are proposing that we are going to do that.

Mr. BROUN. That is my concern, too.

Mr. JAMISON. We are going through a privacy impact assessment to do that and make sure that we follow all the civil rights and civil liberties that are associated with that.

Congressman, the threat is real. Our adversaries are very adept at hiding their attacks in normal traffic and the normal everyday traffic that comes across the network very well could be disguised, and it could be malicious. So the only true way to protect your networks is to have intrusion detections. It is what everybody has on all their networks now. It is not just consistent in the Federal Government, and it is not informed by our latest threat information of what we know. That is what we are talking about.

There are a lot of other activities that we need to do to focus on improving cybersecurity beyond just this and the effort that we are talking about today, and we are working on that, and we would be happy to brief you on that in a detailed session.

Mr. BROUN. Okay. Thank you very much.

Mr. Chairman, thank you. I yield back.

Chairman THOMPSON. Thank you very much.

We now yield 5 minutes to the gentleman from North Carolina, Mr. Etheridge.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Let me thank you for being here. I must confess, I join Ms. Harman in listening to the testimony this morning.

So, Mr. Jamison, given the hundreds of cyber incidents that have taken place over the last few years, how would you rate the Department's response to cybersecurity, A through F?

Mr. JAMISON. It's been a while since I have been in school. I think currently we are——

Mr. ETHERIDGE. Well, you find the number you want to, I will be happy.

Mr. JAMISON. I think we are a solid C, and if you will allow me to expound on that from the standpoint of, as I mentioned before, our current capability from a US–CERT standpoint, and I am strictly talking about——

Mr. ETHERIDGE. Let me just say something: If you say a solid C, you know, I was a State superintendent of schools for a few years, that is sort of average, at best.

Mr. JAMISON. That is why we are here, Congressman.

Mr. ETHERIDGE. That isn't even close to being good enough in what we are talking about for the American people. But I will let you continue, because I have another question following that.

Mr. JAMISON. Congressman, that is why we are here. As I said in my opening statements, we need to do more. Currently, from a DHS and US–CERT perspective of having that responsibility across the Federal domain, we need to have more comprehensive——

Mr. ETHERIDGE. All right. Given that then, can you tell this committee what accountability has been put in place, because there are well-recorded numbers of breaches in the Government system? What accountability do we have in place when that happens? If it happens on my watch, what accountabilities am I accountable for?

Mr. JAMISON. Well, I will defer to Karen to talk about the FISMA accountabilities and some of their requirements that each CIO has.

Ms. EVANS. We hold the agencies accountable through a quarterly process. We manage, through the President's management agenda, on the score card. However, when incidents occur, agencies are held accountable. We do work with them to ensure—because, first and foremost is when it does occur, that there is a proper response, because it is involving the citizens' data, and, first and foremost, we have to make sure that the way that we handle that response is addressing their immediate needs and that we take the proper precautions in place to ensure that the citizen then knows that we are addressing that.

Yes, sir.

Mr. ETHERIDGE. Let me follow up on that, because I think that leads to a little broader question in that area, because every year OMB says that agencies are implementing more security controls on their computers, yet every year the number of successful penetrations in the Federal networks rise. This means that every year we lose more and more information to our adversaries.

That being true, OMB measures success by the percentage of certified and accredited computer systems, but even the stamp of ap-

proval that you are just talking about, sensitive data tends to seep out, okay?

That being true, are we using the right metrics? The second part of that question, shouldn't we be measuring our ability to stop attacks or at a minimum use our ability to detect and respond to attacks as the correct metric? Wouldn't that seem to be a better metric to use in terms of where we are than just measuring the other pieces? I mean, that just seems common sense to me.

Ms. EVANS. Okay. I would agree with you that initially when we first started this process, when FISMA's predecessor was the Government Information Security Act, and many of the Members have brought this up: Initially, agencies didn't know what they didn't know. So metrics evolved, and these are the first sets of metrics that we use so that agencies could make sure that they knew what their inventory was. Because if you don't know what you own, then you can't manage it appropriately and know the risk associated with it.

So the first set of metrics and the things that we have measured may need to improve, and we have talked to Congress about this and GAO, because we are now—and I would agree with you that the metrics that we look at are more output-oriented right now, and we are moving now to a level of more performance, such as the types of metrics that you are talking about, because——

Mr. ETHERIDGE. Seems to me that is how you measure it.

Ms. EVANS. Absolutely, and you know what the baseline is now. We know what these systems are, we know how the agencies are categorizing the systems, and there is consistency across the board.

Mr. ETHERIDGE. My time is running out. Let me touch one more point, if I may get it in, because I think this is critical.

Because it seems to me there are flaws on the on-the-job training. I mean, we have already heard that. If we aren't giving proper training and ongoing training, management practices within Federal agencies where workforces do not understand the effects of their actions on national security. I mean, what are we doing to train employees? That is the other side of it. We have got to measure both pieces, and that metric, it seems to me, has to change, if we are going to get—because if we do the same thing we have always done, we are going to get the same results we have always gotten.

Ms. EVANS. May I answer?

Mr. ETHERIDGE. Please.

Ms. EVANS. Thank you, sir.

Okay, so we pick certification and accreditation because it is a soup-to-nuts process. If an agency approaches the process for compliance, checks the box, because I have to tell OMB and then it goes to Congress, we aren't going to get the result that we intend.

But if you look at the process associated with that, all the issues that you brought up, when you certify an accredited system, you have to know what it is, you have to analyze the risk, you have to put together rules of behavior so that each user, as they sign on, know what they are supposed to do and the consequences associated with not doing that.

The last part of that also is residual risk, because the manager in charge needs to say, "That service is important. I will live with

this risk. Here is the compensating control and hold me accountable."

That is really how the process is supposed to work, and that is where we have to now move it to the next level so that we are actually achieving the result versus a paperwork exercise where we just get a bunch of paper and people are producing stuff and people don't really know what their responsibility is and what they should be held accountable for.

Mr. ETHERIDGE. We are doing a lot of work.

Ms. EVANS. We are improving it.

Mr. ETHERIDGE. But the results are meager for the investment, and we have got to do better to protect the American people. I really believe that. Thank you.

Thank you.

I yield back, Mr. Chairman.

Chairman THOMPSON. Thank you.

The gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. Thank you and the Ranking Member for holding this hearing, and because I know that time is of the essence, I will move as quickly as possible.

I have a few questions, and thank you, witnesses, for appearing today.

Is it true, Mr.—is it, Charbo, am I pronouncing it correctly?—Mr. Charbo, that you were the CIO of Homeland Security at a time when some intelligence reports about hacking were known to other agencies but not reported to you? Is this true?

Mr. CHARBO. Well, sir, I am not sure what was reported to other agencies. My assumption is, is that is probably correct.

Mr. GREEN. Okay. At a 2007 hearing, according to the intelligence that I have, the Department of Homeland Security CIO, Scott Charbo—that would be you—told the committee that he had never received any intelligence reports about nation states hacking and that he was unfamiliar with the activity.

Mr. CHARBO. The response, I believe, was that we had had one. I had had one previous to that hearing, which was sponsored through the CIO Council——

Mr. GREEN. Yes, sir.

Mr. CHARBO [continuing]. And at that time, there was nothing that pointed back to DHS.

Mr. GREEN. You were not familiar with it. There were others who knew but you did not know; is this true?

Mr. CHARBO. Not by the name, I believe, that was being discussed at the hearing. I mean, obviously, we had heard about nation state hacking and different nations, but I had never had a briefing that pointed back to the Department. They were all, basically, in general at a lower classification level.

Mr. GREEN. Well, did it happen? Maybe I should start there. Did this happen? Was there actually a hacking that took place?

Mr. CHARBO. At the Department?

Mr. GREEN. Yes, sir.

Mr. CHARBO. We have lots of security events at the Department. Whether or not those are nation states——

Mr. GREEN. Whether they are nation states—all right, let's talk about nation states. Was there a nation state hacking?

Mr. CHARBO. Yes, there are a few that we are looking at, and we would have to address that on a classified level.

Mr. GREEN. Okay. Is it your opinion that we have not had any cross-agency intelligence failures?

Mr. CHARBO. I certainly think it can be improved, and I think that is what this effort is about.

Mr. GREEN. All right. Well, let me go to my next question. Is it true that we had a contractor charged with securing networks at the Department, and this contractor did not install intrusion detection systems?

Mr. CHARBO. Those are gaps that we identified, and that we had them put in place.

Mr. GREEN. Is that a true statement?

Mr. CHARBO. That is a true statement.

Mr. GREEN. Okay. The question becomes then, what are the consequences when we have these kinds of occurrences? Have we ever had a contractor terminated for failure to perform to the level that this contractor failed to perform? Terminated. We are not talking about renewing a contract. But have we ever had one terminated?

Mr. CHARBO. Well, I can only speak to this incident. I mean, from a broader contracting perspective, that would have to go to our contracts. We did recompete this contract.

Mr. GREEN. Let me ask you about what you know? Do you know of any contractor ever having been terminated?

Mr. CHARBO. I can't speak to anything specific.

Mr. GREEN. So you don't know of one.

Mr. CHARBO. To my knowledge, I don't know of that.

Mr. GREEN. Okay. Do you know of anyone who has ever been fired for failure to properly provide intelligence across agencies that should have been provided?

Mr. CHARBO. I couldn't put a name on it, but, certainly, we have had contractors removed.

Mr. GREEN. Well, now I am talking about a person being fired as opposed to a contractor. We went through the contracting and you indicated that you didn't know about the contractors.

Mr. CHARBO. The question is?

Mr. GREEN. The question is, have we had anybody fired? Has anybody ever been fired?

Mr. CHARBO. To my knowledge, I have never fired a Federal employee. We certainly have responded to performance, but I have not fired a Federal employee.

Mr. GREEN. Do you know of anyone that has ever been fired for failure to perform in this area of sensitive security information transmission?

Mr. CHARBO. I can't speak to anything specifically.

Chairman THOMPSON. Will that gentleman yield?

Mr. GREEN. Yes, sir.

Chairman THOMPSON. In the interest of making sure we get the record straight, Mr. Charbo, that incident that was referred to by Mr. Green I think it was the committee staff that brought it to your attention of your shop that there had been some problems with a contractor that you all were not aware of. I think after that was brought to your attention, you all moved forward and looked at it.

Please.

Mr. CHARBO. The one incident that I believe is being referred to was made aware of by our staff. What was incomplete was the closure of that because of the different opinions. I mean, much of this hearing is about the level of data that you receive on a particular event. One analyst can look at a piece of data and have one interpretation. Several others can look at it and have different interpretations. A lot of that is dependent on the situational awareness that an individual has.

In this case, that is what was presented to me. That coincided with the hearing. We asked for that information. At that time, I turned that over to our security group and said, "I have conflicting information here. It is something for you to look at."

I believe that is currently still under investigation, sir.

Mr. GREEN. All right, Mr. Chairman, thank you.

Chairman THOMPSON. Thank you very much.

We now have three votes on the floor, and we have concluded all of our witnesses and our questions for the witnesses. I would like to thank them for their valuable testimony. The Members of the committee may have additional questions for the witnesses, and we will ask that you would respond expeditiously in writing to those questions.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 11:27 a.m., the committee was adjourned.]

APPENDIX

QUESTION FROM HONORABLE YVETTE D. CLARKE FOR HONORABLE KAREN EVANS, ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET

Question. Ms. Evans, it is my understanding that you have worked with Director Will Pelgrin, head of NY State's Cyber Security Office and the chair of the Multi-State Information Sharing and Analysis Center, including coordination on the Data-at-Rest Smart Buy program. Can you describe your involvement with this effort with the State and local governments and what were the results?

Answer. SmartBuy is a Government-wide initiative which leverages the Federal Government's requirements and buying power. As a member of the governance board, we help determine the priorities and technical requirements to be included in SmartBuy efforts. A major effort of the SmartBuy program was the Data-At-Request (DAR) Blanket Purchase Agreements (BPAs) to provide encryption products to Federal agencies, NATO, and State and local governments to protect sensitive, unclassified data on mobile computing devices and removable media.

Protecting DAR is increasingly critical in today's information technology (IT) environment of highly mobile data and decreasing device size. Personal identity information or sensitive Government information stored on devices such as laptops, thumb drives and personal digital assistants (PDAs) can be unaccounted for and unprotected, and can pose a problem if these devices are compromised. In addition to saving taxpayer dollars, the DAR BPA enhances DAR information security and requires vendors to meet stringent technical and information assurance requirements.

OMB Memorandum M–06–16, Protection of Sensitive Agency Information, issued in June 2006 was a key impetus for the actions resulting in these agreements. Two months after OMB issued this memo, the DoD Data-at-Rest Tiger Team (DARTT) was developed to address technical requirements. Eventually, the DARTT evolved into an interagency team comprised of 20 DoD components, 18 Federal agencies and NATO, with State and local governments joining in March 2007. These requirements were presented to the governance board and accepted.

The State and local governments are participating under GSA's Cooperative Purchasing Program, which allows them to purchase IT products and services from both GSA's Multiple Award Schedule 70 and Consolidated Schedules that have IT special item numbers.

To date 127,296 licenses have been issued across 15 States (including local governments). This has resulted in savings of $24.1 million on purchases of encryption software through use of these Federal DAR contracts and approximately $8 million using the special State and local government offers—for a total of more than $32 million in savings/cost avoidance to date.

QUESTION FROM HONORABLE YVETTE D. CLARKE FOR HONORABLE ROBERT D. JAMISON, UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Question 1. Secretary Jamison, how much of the Infrastructure Protection and Information Security (IPIS) account in the fiscal year 2009 budget request is intended to support State and local Government cybersecurity activities?

Answer. The Department of Homeland Security collaborates with a broad range of security partners, including State, local, and international governments, private-sector owners and operators, and individuals, in its efforts to improve the Nation's cybersecurity posture. Specifically, the Department's United States Computer Emergency Readiness Team (US–CERT), the national focal point for coordinating the defense against and response to national cyber attacks, engages with State and local governments by sharing information with States and providing direct support to States requiring response and recovery assistance. Budgetary support for State and

local government cybersecurity efforts is embedded within the Department's many programs and activities and does not maintain a specific line item; however, the Department does provide funding to the Multi-State Information Sharing and Analysis Center (MS–ISAC). Much of the increase in funding to cybersecurity will result in improved situational awareness of threats, intrusions, and response methods across the Federal domain. State and local governments will benefit from this enhanced focus.

Through a contract with the Department, the MS–ISAC supports a number of operational and awareness activities. The current contract with the MS–ISAC, spanning from November 2007 through November 2008, totals $1,694,825, and a similar amount is estimated for fiscal year 2009. These activities include operating the MS–ISAC State and Local Operations Center for Cybersecurity, which collaborates with US–CERT and contributes to State and local cybersecurity by maintaining situational awareness of the State cyber landscape; by hosting bi-monthly webcasts with cybersecurity experts for the general public to raise awareness about emerging cybersecurity issues; and by developing cybersecurity educational materials offering best practices, tools, and tips as part of the Department's national cybersecurity awareness efforts.

In addition to the funding provided to the MS–ISAC for these efforts, the Department has dedicated staff to support ongoing MS–ISAC efforts. This includes more than two full-time equivalents who liaise with the MS–ISAC to ensure coordination with the Department on current State and local government efforts by engaging in MS–ISAC activities, including various working groups to help with the creation, production, and dissemination of education and awareness resources for use by the States; and by participating in regular meetings as well as the MS–ISAC annual meeting. In addition, Department staff members work to oversee the fulfillment of the statement of work. Staff support to and coordination with the MS–ISAC is estimated at $270,000 annually.

An important component of the Department's work is its support of efforts to advance State and local cybersecurity activities. In addition to funding provided to support the MS–ISAC, the Department has committed significant resources, through various programs and activities, to help State and local security partners address their cybersecurity preparedness and response needs and effectively manage cybersecurity issues.

Question 2. Secretary Jamison, how much of the increased funding to DHS for cybersecurity initiatives to address improvements in the security posture of State and local governments is specifically set aside for programs to be coordinated or performed by the Multi-State ISAC?

Answer. The Cyber Initiative is an interagency effort that aims to enhance the security of Federal Government networks. Increased funding has been primarily directed to enhancements for the Department of Homeland Security's United States Computer Emergency Readiness Team (US–CERT), the Nation's watch and warning mechanism. US–CERT provides around-the-clock monitoring of cyber infrastructure and coordinates the dissemination of information to key constituencies, including all levels of government and industry. It serves as the focal point for helping Federal, State, local, and international governments, industry, and the public work together to achieve the appropriate responses to cyber threats and vulnerabilities. The additional funding allocated to enhance US–CERT capabilities is primarily focused on improving Federal network security through programs such as the Trusted Internet Connections (TIC) initiative and the Einstein program. It will also result in increased level of service and information sharing with all cybersecurity partners, which includes all of the Information Sharing and Analysis Centers (ISACs); however, no additional funding has been allocated to the Multi-State Information Sharing and Analysis Center (MS–ISAC) or any other ISAC under this initiative.

Although the Cyber Initiative is focused on Federal networks, the enhanced products and services from US–CERT will provide specific additional benefits to State and local governments. States are dependent upon Federal network operations and information for a range of services and daily critical functions. Cyber threats to the Federal networks could have potentially devastating effects on State and local government networks given their interconnectedness. Improving US–CERT's capabilities to monitor, detect, report, and mitigate malicious activity will enable the Department to identify threats to Federal networks more effectively and efficiently, thus protecting those networks upon which State and local governments rely.

The Department recognizes the importance of State and local government cybersecurity in its efforts to better secure the Nation's cyber assets. Under the Cyber Initiative, programs and activities to secure Federal networks will benefit State and local governments. Through US–CERT's enhanced watch, warning, and response capabilities, State and local governments will benefit from improved infor-

mation sharing of alerts, warnings, and mitigations plans. In addition, the Department has established and maintains strong cooperative relationships with State and local governments, and it has developed several programs directed at addressing State and local government cybersecurity issues. With existing and new programs, the Department remains committed to improving the cybersecurity posture of State and local governments.