CYBERSECURITY: DHS' ROLE, FEDERAL EFFORTS, AND NATIONAL POLICY

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JUNE 16, 2010

Serial No. 111–71

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

64–697 PDF WASHINGTON : 2011

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

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
DINA TITUS, Nevada
WILLIAM L. OWENS, New York
VACANCY
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio
TOM GRAVES, Georgia

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

CONTENTS

CYBERSECURITY: DHS' ROLE, FEDERAL EFFORTS, AND NATIONAL POLICY

Wednesday, June 16, 2010

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

The committee met, pursuant to call, at 10:00 a.m., in Room 311, Cannon House Office Building, Hon. Bennie G. Thompson [Chairman of the committee] presiding.

Present: Representatives Thompson, Harman, Lofgren, Jackson Lee, Cuellar, Clarke, Richardson, Kirkpatrick, Cleaver, Green, Himes, King, Smith, Lungren, McCaul, and Dent.

Chairman THOMPSON. The Committee on Homeland Security will come to order. The committee is meeting today to receive testimony on "Cybersecurity: DHS's Role, Federal Efforts, and National Policy." I want to thank the witnesses for appearing here today.

Today's hearing entitled "Cybersecurity: DHS's Role, Federal Efforts, and National Policy" will examine the Department of Homeland Security's efforts to secure cyberspace. Since 1997, GAO has designated information security as a high-risk area in the Federal Government. Ten years later, information security is still high risk. Some would say that it is the difficulty of this task that keeps us from achieving it, but I know that few things worth doing are easy. Security of the Federal Government's network from a wide array of cyber attackers is not easy, but few tasks are more necessary.

According to GAO, the cybersecurity incidents reported by Federal agencies have increased 400 percent in the last 4 years, from 5,503 incidents in fiscal year 2006 to about 30,000 incidents in fiscal year 2009. Whether military or intelligence-gathering operations of foreign nations, domestic or international terrorist groups, lone wolf, hate-driven individuals, common criminals or thrill-seeking hackers, those attempting to infiltrate and export this country's computer networks are both numerous and determined. But they will not win if we match their determination with our resolve and defeat their abundance with our expertise.

As the lead agency for cybersecurity in a Federal civilian agency, the Department of Homeland Security is responsible for guiding and directing the Federal efforts to defeat this multifaceted cyber enemy.

So my question today is: Does the Department have what it needs to win the war? US–CERT, the office within the Department that is charged with leading our cyber defense effort, has significant deficiencies. It does not have sufficient staff to analyze security information. It cannot develop internal capacity because con-

tractors outnumber Federal employees by 3 to 1. It has not developed leadership consistency because US–CERT has had four directors in 5 years. Given these administrative failures, it should come as no surprise that day-to-day operations may suffer.

According to the President's National Security Strategy released this month, Federal cyber networks must be secure, trustworthy, and resilient. DHS must be a major actor in this Nation's effort to secure the Federal computer networks.

In addition to the Federal Government, DHS must reach out to State, local, and Tribal governments as well as the private sector to assure the protection and resiliency of our cyber infrastructure. But none of this can occur without adequate staffing, planning, and funding. Today we must pledge to become as committed to secure our networks as our enemies are committed to breach them.

Again, I want to thank our witnesses for agreeing to attend and testify today, and I look forward to that testimony.

[The statement of Chairman Thompson follows:]

PREPARED STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JUNE 16, 2010

Today's hearing, entitled "Cybersecurity: DHS' Role, Federal Efforts, and National Policy" will examine the Department of Homeland Security's efforts to secure cyberspace. Since 1997, GAO has designated information security as a high-risk area in the Federal Government. Ten years later, information security is still high-risk.

Some would say that it is the difficulty of this task that keeps us from achieving it. But I know that few things worth doing are easy. Securing the Federal Government's networks from a wide array of cyber attackers is not easy. But few tasks are more necessary.

According to GAO, the cybersecurity incidents reported by Federal agencies have increased 400 percent in the last 4 years. From 5,503 incidents in fiscal year 2006 to about 30,000 incidents in fiscal year 2009. Whether the military or intelligence-gathering operations of foreign nations; domestic or international terrorist groups; lone wolf hate-driven individuals; common criminals, or thrill-seeking hackers, those attempting to infiltrate and exploit this country's computer networks are both numerous and determined.

But they will not win if we match their determination with our resolve and defeat their abundance with our expertise. As the lead agency for cybersecurity in Federal civilian agencies, the Department of Homeland security is responsible for guiding and directing the Federal efforts to defeat this multi-faceted cyber enemy. So my question today is: Does the Department have what it needs to win this war?

US–CERT—the office within the Department that is charged with leading our cyber defense efforts has significant deficiencies. It does not have sufficient staff to analyze security information. It cannot develop internal capacity because contractors outnumber Federal employees by about 3 to 1. It has not developed leadership consistency because US–CERT has had four directors in 5 years. Given these administrative failings, it should come as no surprise that day-to-day operations may suffer.

According to the President's National Security Strategy released last month, Federal cyber networks must be "secure, trustworthy, and resilient."

DHS must be a major actor in this Nation's efforts to secure the Federal computer networks. In addition to the Federal Government, DHS must reach out to State, local, and Tribal governments as well as the private sector to assure the protection and resiliency of our cyber infrastructure. But none of this can occur without adequate staffing, planning, and funding. Today, we must pledge to become as committed to secure our networks as our enemies are committed to breach them.

Chairman THOMPSON. The Chairman now recognizes the Ranking Member of the full committee, the gentleman from New York, Mr. King, for an opening statement.

Mr. KING. Thank you, Mr. Chairman. Thank you for holding this hearing, which the Republican Members requested several months ago, to address the serious and growing threat of cyber attacks on

our Government and private sector networks. I would like to thank all of the witnesses appearing today and especially welcome back Stewart Baker. It is great to see him and to thank him for his terrific service for the Department of Homeland Security. Great to see you, Stu.

We requested this hearing because cyber attacks have risen to epidemic levels in the United States and are increasing. Critical intellectual property is regularly stolen and fraud is rampant. As stated in the National Security Strategy, quote, cybersecurity threats represent one of the most serious, National security, public safety, and economic challenges we face as a Nation. The Deputy Assistant of the FBI's Cyber Division has said that cyber attackers pose a threat to the existence of the United States as we know it.

General Alexander, recently appointed head of the U.S. Cyber Command, noted that cyber threats are evolving from data theft and temporary disruption to sabotage, which give the United States pause for concern. The former DNI, Mike McConnell, stated, if the Nation went to war today in a cyber war, we would lose.

The United States needs a robust plan for migrating cyber threats, yet the Federal response remains fragmented. The United States needs to move forward with continuous monitoring of Federal network traffic for malicious activity so that we can increase situational awareness and fight cyber attacks in real time. The cyber threat must be anticipated and not addressed after the fact.

I would note that Chairman Lieberman and Senator Collins recently took a major step forward in coordinating and clarifying Federal policy when they introduced the Protecting Cyberspace As a National Asset Act of 2010. In a very positive step, the Lieberman-Collins bill codifies the role of the Department of Homeland Security as the lead agency to coordinate the protection of Federal systems against cyber attacks and to coordinate with the private sector on the protection of critical information infrastructure.

The bill also empowered DHS with the enforcement authority necessary to carry out its mission. That lack of adequate departmental authority was prominently raised in the Inspector General's report that was released today, and this committee should work quickly to address that serious deficiency.

I strongly support the legislation introduced by Chairman Lieberman and Senator Collins, and I look forward to working with my House colleagues to introduce companion legislation promptly.

I thank the Chairman and I yield back the balance of my time.

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

[The statement of Hon. Richardson follows:]

PREPARED STATEMENT OF HONORABLE LAURA RICHARDSON

JUNE 16, 2010

Mr. Chairman, thank you for convening this hearing today on the Department of Homeland Security's efforts to secure cyberspace. I thank our distinguished panel of witnesses for appearing before us today to share with us the work they are doing on this issue and their recommendations for what else needs to be done.

The National cybersecurity effort is a top Presidential priority. It was not until 2008 that the Bush administration sought to reevaluate the Federal mission in cyberspace, so I am pleased that this reform effort is one of President Obama's main

concerns. Our Government and the Congress is years late in coming up with a comprehensive security effort for cyberspace, as cybersecurity threats represent one of the most serious National security, public safety, and economic challenges faced by this Nation. A complete cybersecurity policy and plan is a key component of keeping our homeland safe, so I am pleased that today this committee will get a chance to delve into the issues surrounding this policy.

As the Government and the private sector rely more and more on computers and digitized information in our everyday life, we also face more and more risks on that front. For example, in the Federal sector, many kinds of information may present an appealing target including National security information, taxpayer data, Social Security records, medical records and proprietary data. Just this past week, a cybersecurity sweep at Penn State University, a State university, found the Social Security numbers of 25,000 individuals may have been exposed to a security breach because of infected computers.

It concerns me that in the fiscal year 2009 Government Accountability Office (GAO) performance and accountability reports, 21 of 24 major Federal agencies noted that inadequate information system controls over their financial systems and information were either a material weakness or a significant deficiency. There were numerous reasons cited for this inadequacy, including lack of awareness, understanding, and interest of technical and policy issues in Executive and Legislative branches. If we do not make cybersecurity a priority, our security will continue to be in jeopardy.

I realize that addressing this problem has been a difficult challenge for the Department of Homeland Security due to the number of agencies involved, funding levels, and need for direction. However, this hearing is an excellent opportunity to examine what Congress can do to further DHS's efforts in this area. I look forward to the testimony of our distinguished panel of witnesses as to where improvements need to be made.

Thank you again, Mr. Chairman, for convening this hearing. I yield back the balance of my time.

Chairman THOMPSON. I welcome our witnesses today. We will have only one panel of witnesses.

Our first witness is Mr. Greg Schaffer, the Assistant Secretary for Cybersecurity and Communications. Mr. Schaffer oversees, among other things, the operations of the National Cybersecurity Division, which includes the United States Computer Emergency Readiness Team, US–CERT. Welcome, Mr. Schaffer.

Our second witness, no stranger to this committee, Mr. Richard Skinner, the Department of Homeland Security Inspector General. As Inspector General, Mr. Skinner is responsible for overseeing audits, investigations, and inspections relating to the programs and operations of the Department. Welcome, Mr. Skinner.

Our third witness is Mr. Greg Wilshusen, Director of Information of Security Issues at the Government Accountability Office. GAO serves as the principal and trusted investigative arm of Congress. GAO has performed dozens of engagements on the topic of cybersecurity, many of them at the request of this committee. Welcome, Mr. Wilshusen.

Our final witness, no stranger to this committee either, Mr. Stewart Baker. Mr. Baker is former Assistant Secretary for Policy at the Department of Homeland Security. He is currently a partner in Steptoe & Johnson, LLP, as well as an author of a recently released text on matters of interest. Welcome.

We thank our witnesses for being here today. Without objection, the witnesses' full statement will be inserted in the record. I now recognize Assistant Secretary Schaffer to summarize his statement for 5 minutes.

STATEMENT OF GREGORY SCHAFFER, ASSISTANT SECRETARY, CYBERSECURITY AND COMMUNICATIONS, DEPARTMENT OF HOMELAND SECURITY

Mr. SCHAFFER. Chairman Thompson, Ranking Member King, and distinguished Members of the committee, it is a pleasure to appear before you today to discuss the Department of Homeland Security cybersecurity mission. I will provide an update on our efforts to better secure the systems and networks of the Federal Executive branch and of the critical infrastructure while strengthening our public-private partnerships. The President has clearly laid out DHS's roles and responsibilities for protecting Nationally critical civilian networks. DHS has the lead to secure Federal civilian systems, sometimes described as the dot-gov domain. DHS works with critical infrastructure and key resources owners and operators to bolster their cybersecurity preparedness, risk mitigation, and infinite response capabilities.

At the Department, we have focused our efforts on enhancing the cybersecurity posture of the Nation by improving our capacity to prevent, identify, respond to, and recover from cyber threats, which are becoming more targeted, more sophisticated, and more numerous.

The administration's focus on addressing these threats is clear. Consistent with the President's cyberspace policy review, the Department has a number of foundational and forward-looking efforts underway to reduce cyber risk. Elevating these cyber risk reduction efforts, the Department's Quadrennial Homeland Security Review made cybersecurity one of the Department's top five mission areas. The QHSR details two overarching goals for cybersecurity: To help create a safe, secure, and resilient cyber environment and to promote cybersecurity knowledge and innovation. DHS's work towards these goals is carried out largely within the Office of Cybersecurity and Communications, which I lead, a component of the National Protection and Programs Directorate with significant contributions being made by other DHS offices.

I would like to highlight a few of the key programs today. First, the Trusted Internet Connection Initiative is working to reduce and consolidate external access points across the Federal enterprise, manage security requirements, and ensure compliance with program policies. This will help create an efficient and manageable frontline of defense for Federal Executive branch civilian networks.

Second, the Department is deploying EINSTEIN 2 to these TIC locations to monitor incoming and outgoing traffic for malicious activity. EINSTEIN 2 is currently deployed and operational at 11 of 19 planned departments and agencies. The EINSTEIN 2 system is already providing us with, on average, visibility into more than 278,000 indicators of potential malicious activity a month.

Additionally, DHS is building upon the enhanced situational awareness that EINSTEIN 2 provides. We are working with the private sector, the National Security Agency, and a wide range of other Federal partners to test the technology for the third phase of EINSTEIN, an intrusion prevention system which will provide DHS with the capability to automatically detect malicious activity and disable attempted intrusions before harm can be done to our critical networks and systems.

Furthermore, CS&C is implementing a defense in depth approach to cybersecurity. We are doing this through complementary efforts, including initiatives such as the OMB's new FISMA reporting requirements, shifting away from paper compliance and towards implementing solutions that actually improve cybersecurity. DHS will provide operational support to agencies by monitoring and reporting progress to ensure the new OMB guidance is effectively implemented.

Another aspect of defense in depth is the protection of critical infrastructure and key resources from cyber threats. As part of this effort, the DHS Control System Security Program works to protect critical infrastructure by providing expertise, tools, and leadership to the owners of control systems. DHS has trained more than 14,000 control system operators and has assisted in vulnerability assessments throughout the country. Additionally, our Industrial Control Systems Cyber Emergency Response Team, the ICS–CERT provides on-site support for incident response.

As we move forward, public-private cooperation is growing ever more important. We are developing a National cyber incident response plan that will define cyber incident roles and responsibilities and will provide all levels of Government and the private sector with a better understanding of how to respond to a cyber event during a crisis.

It is important to note that continued success is reliant upon increasing the numbers of dedicated and skilled people at the Department. To this end, the National Cybersecurity Division tripled its Federal workforce from 35 to 118 in fiscal year 2009 and we hope to more than double that number to 260 in fiscal year 2010. Over the past year since I took office, my staff and I have worked closely with the GAO, the Inspector General, and this committee to improve organizational efficiencies and implement recommendations in line with Departmental priorities and our overarching approach to cybersecurity. To this end, I think both GAO and the Inspector General will agree that much progress has been made.

I would like to thank the committee for the strong support you have provided to the Department and thank you for this opportunity to testify, and I would be happy to answer any questions that you may have.

[The statement of Mr. Schaffer follows:]

PREPARED STATEMENT OF GREGORY SCHAFFER

JUNE 16, 2010

INTRODUCTION

Mr. Chairman, Ranking Member King, and distinguished Members of the committee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission. I will provide an update on our efforts to better solidify the Federal Executive branch civilian networks and systems, critical infrastructure, and our public-private partnerships. At the Department, our efforts are focused on enhancing the cybersecurity posture of the Nation by improving our capacity to prevent, identify, respond to, and recover from cyber threats.

As a nation, it is essential that we are aware of, and focused on, the cyber threat. Just as important, the Government must be able to move quickly and purposefully to address cyber threats as malicious actors rapidly change techniques, technology, and tradecraft. As you know, Mr. Chairman, threats are becoming more targeted, more sophisticated, and more numerous.

OVERVIEW OF DHS CYBERSECURITY RESPONSIBILITIES

DHS is responsible for helping Federal Executive branch civilian departments and agencies to secure their unclassified networks, often called the dot-gov domain. DHS also works closely with partners across Government and in industry assisting them with the protection of private sector critical infrastructure networks. The Department has a number of foundational and forward-looking efforts under way, many of which stem from the Comprehensive National Cybersecurity Initiative (CNCI).

The President has described our networks, as "strategic National assets" and called the growing number of attacks on these networks "one of the most serious economic and National security threats our Nation faces." The President has also clearly laid out the roles and responsibilities for protecting Nationally critical civilian networks:

- DHS has the lead to secure Federal civilian systems, sometimes described as the dot-gov domain.
- DHS works with critical infrastructure and key resources (CIKR) owners and operators—whether private sector, State, or municipality-owned—to bolster their cyber security preparedness, risk mitigation, and incident response capabilities, in coordination with other Federal Sector-Specific Agencies as appropriate.

The CNCI comprises a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

- Establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with State, local, and Tribal governments and private sector partners—and the ability to act quickly to reduce current vulnerabilities and prevent intrusions.
- Defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.
- Strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

DHS plays a key role in many of the activities supporting these goals and works closely with our Federal partners to secure our critical information infrastructure in a number of ways. We are reducing and consolidating the number of external connections Federal agencies have to the internet through the Trusted Internet Connections (TIC) initiative. Further, DHS continues to deploy its intrusion detection capability, known as EINSTEIN 2, to those TICs. Through the United States Computer Emergency Readiness Team (US–CERT), we are working more closely than ever with our partners in the private sector and across the Federal Government to share what we learn from our EINSTEIN deployments and to deepen our collective understanding, identify threats collaboratively, and develop effective security responses. In addition, the Department has a role in the Federal Government for cybersecurity research and development (R&D). The DHS Science and Technology (S&T) Directorate's Cyber Security R&D (CSRD) program funds activities addressing core vulnerabilities in the internet, finding and eliminating malicious software in operational networks and hosts, and detecting and defending against large-scale attacks and emerging threats on our country's critical infrastructures. The CSRD program includes the full R&D lifecycle—research, development, testing, evaluation, and transition—to produce unclassified solutions that can be implemented in both the public and private sectors. The S&T Directorate has established a Nationally recognized cybersecurity R&D portfolio addressing many of today's most pressing cybersecurity challenges. The CSRD program has funded research that today is realized in more than 18 open-source and commercial products that provide capabilities, including the following: Secure thumb drives, root kit detection, worm and distributed denial of service detection, defenses against phishing, network vulnerability assessment, software analysis, and security for process control systems.

President Obama determined that the CNCI and its associated activities should evolve to become key elements of the broader National cybersecurity strategy. These CNCI initiatives and its associated activities will play the central role in implementing many of the key recommendations of President Obama's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.*

With the publication of the *Cyberspace Policy Review* on May 29, 2009, DHS and its components have developed a long-range vision of cybersecurity for the Department's—and the Nation's—homeland security enterprise. This effort resulted in the

elevation of cybersecurity to one of the Department's five priority missions, as articulated in the Quadrennial Homeland Security Review (QHSR), an overarching framework for the Department that defines our key priorities and goals and outlines a strategy for achieving them. Within the cybersecurity mission area, the QHSR details two overarching goals: To help create a safe, secure, and resilient cyber environment, and to promote cybersecurity knowledge and innovation.

In alignment with the QHSR, Secretary Napolitano has consolidated the Department's cybersecurity efforts under the coordination of the National Protection and Programs Directorate (NPPD) and its Deputy Under Secretary who also serves as the Director of the National Cyber Security Center. As NPPD leadership, we are moving aggressively to build a world-class cybersecurity team, and we have identified three key priorities that enable and establish a "system-of-systems" approach encompassing the people, processes, and technologies needed to create a front line of defense and grow the Nation's capacity to respond to new and emerging threats. Most immediately, we are focusing on three priorities:

1. Continue enhancement of the EINSTEIN system's capabilities as a critical tool in protecting our Federal Executive branch civilian departments and agencies.
2. Develop the National Cyber Incident Response Plan (NCIRP) in full collaboration with the private sector and other key stakeholders. The NCIRP will ensure that all National cybersecurity partners understand their roles in cyber incident response and are prepared to participate in a coordinated and managed process. The NCIRP will be tested this fall during the Cyber Storm III National Cyber Exercise.
3. Increase the security of automated control systems that operate elements of our National critical infrastructure. Working with owners and operators of the Nation's critical infrastructure and cyber networks, we will continue to conduct vulnerability assessments, develop training, and educate the control systems community on cyber risks and mitigation solutions.

DHS also bears primary responsibility for raising public awareness about threats to our Nation's cyber systems and networks. Every October DHS, in coordination with other Federal agencies, governments, and private industry, makes a concerted effort to educate the public through the National Cybersecurity Awareness Month (NCSAM) campaign, and we are making progress. For example, in 2009, the Secretary of Homeland Security and the Deputy Secretary of Defense jointly opened the campaign, we engaged in our most significant outreach ever, and all 50 States, the District of Columbia, and the U.S. Territory of American Samoa, as well as seven Tribal governments, endorsed NCSAM.

Teamwork—ranging from intra-agency to international collaboration—is essential to securing cyberspace. Simply put, the cybersecurity mission cannot be accomplished by any one agency or even solely within the Federal realm; it requires teamwork and coordination across all sectors because it touches every aspect of our lives. Together, we can leverage resources, personnel, and skill sets that are needed to accomplish the cybersecurity mission. The fiscal year 2011 NPPD budget request for cybersecurity strengthens the on-going work in each of the Department's offices to fulfill our unified mission.

The Office of Cybersecurity and Communications (CS&C), a component of NPPD, is focused on reducing risk to the Nation's communications and IT infrastructures and the sectors that depend upon them, and enabling timely response and recovery of these infrastructures under all circumstances. CS&C also coordinates National security and emergency preparedness communications planning and provisioning for the Federal Government and other stakeholders. CS&C is comprised of three divisions: the National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System.

NCSD collaborates with the private sector, Government, military, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of the civilian Government and private sector critical cyber infrastructures. NCSD also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and private sector constituents. To that end, NCSD carries out the majority of DHS' responsibilities under the CNCI.

Within NCSD, US–CERT leverages technical competencies in Federal network operations and threat analysis centers to develop knowledge and knowledge management practices. US–CERT provides a single, accountable focal point to support Federal stakeholders as they make key operational and implementation decisions and secure the Federal Executive branch civilian networks. US–CERT's holistic approach enables Federal stakeholders to address cybersecurity challenges in a manner that maximizes value while minimizing risks associated with technology and se-

curity investments. Further, US–CERT analyzes threats and vulnerabilities, disseminates cyber threat warning information, and coordinates with partners and customers to achieve shared situational awareness related to the Nation's cyber infrastructure.

DHS is responsible for supporting Federal Executive branch civilian agencies in the protection and defense of their networks and systems. The Department's strategy, which supports a layered defense, requires situational awareness of the state of Federal networks, an early warning capability, near real-time and automatic identification of malicious activity, and the ability to disable intrusions before harm is done. DHS, through NCSD and US–CERT, developed a "system-of-systems" approach to support its cybersecurity mission (noted above). This overall system-of-systems is known as the National Cybersecurity Protection System (NCPS), in which DHS is deploying a customized intrusion detection system, known as EINSTEIN 2, to Federal Executive branch civilian agencies to assist them in protecting their computers, networks, and information.

None of this is possible, however, without a comprehensive understanding of Federal Executive branch civilian networks from an enterprise perspective. The CNCI TIC initiative provides the Federal Government this understanding by reducing and consolidating external access points across the Federal enterprise, assisting with the managing security requirements for Federal agency network and security operations centers, and establishing a compliance program to monitor Federal agency adherence to TIC policies.

The Department is installing EINSTEIN 2 capabilities on Federal Executive branch civilian networks in distinct but interconnected steps. The first step, under the TIC initiative, is the consolidation of external connections and application of appropriate protections thereto. This will help create an efficient and manageable front line of defense for Federal Executive branch civilian networks. The goal is to get down to less than 100 physical locations. Our Program has been working with departments and agencies to better understand how civilian agencies configure their external connections, including internet access points, and improve security for those connections. In parallel with learning about how agencies are configured, we are working with OMB and departments and agencies to consolidate their external connections and as they do that DHS is deploying EINSTEIN 2 to these TIC locations to monitor incoming and outgoing traffic for malicious activity directed toward the Federal Executive branch's civilian unclassified computer networks and systems. EINSTEIN 2 uses passive sensors to identify when unauthorized users attempt to gain access to those networks. EINSTEIN 2 is currently deployed and operational at 11 of 19 departments and agencies. The EINSTEIN 2 system is already providing us with, on average, visibility into more than 278,000 indicators of potentially malicious activity per month.

The TIC initiative and EINSTEIN 2 deployments are critical pieces of the Federal Government's defense-in-depth cybersecurity strategy. DHS is also building upon the enhanced situational awareness that EINSTEIN 2 provides. We currently are working with the private sector, the National Security Agency, and a wide range of other Federal partners to test the technology for the third phase of EINSTEIN, an intrusion-prevention system which will provide DHS with the capability to automatically detect malicious activity and disable attempted intrusions before harm is done to our critical networks and systems.

For all these deployments, it is important to note that EINSTEIN capabilities are being carefully designed in close consultation with civil rights and civil liberties and privacy experts—protecting civil rights, civil liberties, and privacy remains fundamental to all of our efforts.

These accomplishments are reliant upon increasing the number of dedicated and skilled people at CS&C. To this end, NCSD tripled its Federal workforce from 35 to 118 in fiscal year 2009, and we hope to more than double that number to 260 in fiscal year 2010. We are moving aggressively to build a world-class cybersecurity team, and we are focusing on key priorities that address people, processes, and technology.

Recently, the Office of Management and Budget (OMB) and the President's Cybersecurity Coordinator issued new Federal Information Security Management Act (FISMA) reporting requirements that will help our cybersecurity workforce to inculcate a culture of cyber safety. The new requirements are designed to shift efforts away from compliance on paper and towards implementing solutions that actually improve cybersecurity. The new reporting requirements will automate certain security-related activities and incorporate tools that correlate and analyze information, giving the Government's cyber leaders manageable and actionable information that will enable timely decision-making. DHS will provide additional operational support to agencies in securing their networks by monitoring and reporting agency progress

to ensure the new OMB/Cybersecurity Office guidance is effectively implemented. This new reporting follows a three-tiered approach:

- Data feeds directly from department and agency security management tools—agencies are already required to report most of this information. It includes summary information on areas such as inventory, systems and services, hardware, software, and external connections.
- Government-wide benchmarking on security posture will help to determine the adequacy and effectiveness of information security and privacy policies, procedures, and practices throughout the Government.
- Agency-specific interviews will be focused on specific threats each agency faces and will inform the official FISMA report to Congress.

Sensitive information is routinely stolen from both Government and private sector networks, undermining confidence in our information systems, the information collection and sharing process, and the information these systems contain. As bad as the loss of precious National intellectual capital is, we increasingly face threats that are even greater. We can never be certain that our information infrastructure will remain accessible and reliable during a time of crisis, but we can reduce the risks.

Perhaps more ominously, malicious cyber activity can instantaneously result in virtual or physical consequences that threaten National and economic security as well as public health and safety or an individual's civil rights and civil liberties and privacy. Thus, while we strive to prevent loss of intellectual capital from our networks, we are also working to ensure that the systems that support the essential functions that underpin American society—critical infrastructure and key resources (CIKR)—are protected from cyber threats.

Of particular importance are those systems that operationally control our critical infrastructure, such as the energy grid and communications networks. These systems must remain accessible and reliable during times of crisis. Understanding the nexus between the physical and the cyber worlds is an essential mission area for the Department, and one that must permeate all of our efforts.

At DHS, we are very aware that some critical infrastructure elements are so vital to our Nation that their destruction or incapacitation would have a debilitating impact on National security and economic well-being. We recognize that partnering with the private sector to assist in securing critical infrastructure is one of our most important missions. One key priority is DHS' control systems security program, which provides expertise, tools, and leadership to the owners of control systems. A cyber attack on a control system could result in dire physical consequences, even loss of life. We are providing operational support to the control systems community through our Industrial Control Systems Cyber Emergency Response Team (ICS–CERT).

ICS–CERT provides on-site support for incident response and forensic analysis at the request of the affected entity. It also shares and coordinates vulnerability information and threat analysis through information products and situational alerts. Through our advanced vulnerability discovery laboratory, we identify vulnerabilities in control systems and develop and distribute mitigation strategies in partnership with both private sector vendors and operators. The control system program also provides tools (such as the Cyber Security Evaluation Tool) and training to increase stakeholder awareness of the evolving risks to control systems. To date, DHS has helped train more than 14,000 control system operators in the classroom and on the web on how to deal with a variety of cyber attacks. We also created a collection of recommended practices and informational products to assist owners and operators in improving the security of their control systems.

DHS conducts site assessments of selected CIKR facilities (and encourages self-assessments by owners and operators of additional facilities) to identify vulnerabilities and recommend enhancements. In late 2009, we took steps to meet increasing industry requests by implementing a dedicated cybersecurity evaluations program that ensures vulnerabilities identified in our key cyber infrastructure are done so under a consistent and formal framework of evaluation. The program office is working closely with industry to bolster their cybersecurity preparedness, risk mitigation, and incident response capabilities. Through this direct outreach, we expect to improve our capacity to measure private sector performance in managing cybersecurity. We conduct these assessments in close partnership with NPPD's Office of Infrastructure Protection, recognizing the need to intertwine physical security with cybersecurity. In just the last few weeks, we have had teams in Washington, Massachusetts, Missouri, Arizona, and North Dakota to look at individual facilities, regional clusters of critical infrastructure, control systems, and business networks.

In addition to work done with the ICS–CERT, DHS has other efforts designed to help protect critical infrastructure and key resources. In 2006, we established the Cross-Sector Cyber Security Working Group to address cross-sector cyber risk and

explore interdependencies between and among various sectors. The working group serves as a forum to bring Government and the private sector together to address common cybersecurity elements across the 18 CIKR sectors. They share information and provide input to key policy documents, such as the *National Strategy for Trusted Identities in Cyberspace.* The Department conducts its critical infrastructure protection activities under the National Infrastructure Protection Plan (NIPP) framework to facilitate effective coordination between Government infrastructure protection programs and the infrastructure protection and resilience activities of the owners and operators of CIKR resources.

To secure critical infrastructure, the NIPP relies on the sector partnership with the Federal Government. This includes Sector Coordinating Councils and their associated Information Sharing and Analysis Centers, the Homeland Security Information Network, technology and service providers, specific topical working groups, and partners from across the 18 CIKR sectors. These information-sharing mechanisms will continue to enhance and facilitate information exchange throughout the CIKR community, private sector, and Government—making everyone's networks and systems more secure.

The Information Technology Sector Baseline Risk Assessment (ITSRA) is an example of public and private sector information sharing. The completion of the ITSRA last fall was a significant milestone for both the NIPP sector partnership model and for the IT Sector Specific Plan implementation. This important effort identifies strategic and National-level risks to the IT sector and will inform risk management activities across the IT sector this year. It will also focus additional attention on important cross-sector IT risk-related dependencies and inform both Government and industry mitigations, research and development priorities, and resource decisions.

In this sense, it is a true force multiplier in that many sectors are apt to benefit from the IT sector's close working relationship with the public sector. DHS will continue to work with IT sector partners to use the IT sector risk management methodology to identify appropriate responses for the risks identified for each IT sector critical function. This will prioritize mitigation activities and inform corresponding risk management strategies to provide the greatest reduction to the National-level risks identified in the ITSRA. The 2010 Communications Sector Risk Assessment, which is currently under way, will outline security measures that will better support business operations and form the basis of meaningful infrastructure protection metrics. This assessment will complement the ITSRA's functions-based approach and augment its 2008 assessment.

As we move forward, public-private cooperation is growing ever more important. We are building on already successful partnerships and looking forward to new opportunities. DHS is moving toward greater, more actionable sharing of information with the private sector based on new analytical insights derived from a comprehensive understanding of the Government-wide cyber domain. DHS has initiated several pilot programs that enable the mutual sharing of cybersecurity information at various classification levels:

- DHS and Michigan are conducting a proof-of-concept pilot in which the EINSTEIN 1 network flow monitoring technology helps secure Michigan's dot-gov networks. The purpose of this study is to help State governments enhance their cybersecurity and to increase DHS overall cyber situational awareness.
- DHS, the Department of Defense (DOD), and the Financial Services Information Sharing and Analysis Center have launched a pilot designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information—in both directions—to mitigate the impact of attempted cyber intrusions. This builds on the products and success of DOD's Defense Industrial Base initiative. This pilot is currently at the For Official Use Only level, but shortly will be enhanced to include Secret-level information.
- We are also working on a pilot that brings together State fusion centers and private sector owners and operators of critical infrastructure to provide access to Secret-level classified cybersecurity information. The Cybersecurity Partners Local Access Plan is a pilot initiative allowing security-cleared owners and operators of CIKR, as well as State Chief Information Security Officers and Chief Information Officers, to access Secret-level cybersecurity information and participate in Secret-level video teleconference calls via their local fusion centers, allowing classified information sharing outside of Washington, DC.
- DHS has instituted a Top Secret/Sensitive Compartmented Information clearance program for CIKR representatives to enable their engagement in analysis of the most sensitive cybersecurity threat information.

The Department also is working in the areas of software assurance and supply chain management so that Government and private sector partners can work together to solve what is a potentially serious security issue. We believe software developers must automate security and institutionalize it from the beginning in an effort to change the current security posture from reactive to proactive.

Shifting to a proactive posture will also help prevent threats from entering our critical systems and networks, to which end software assurance and supply chain management are so vitally important. By definition, the private sector will have the largest role in developing solutions for more secure software and in supply chain management. To be sure, the Government can help by driving security requirements, but we need to be creative and collaborative in developing partnerships between and among the private and public sector cyber communities to exchange information and ideas.

We need to develop a cybersecurity culture that realizes that everyone—Government, corporate, or private—has a vested stake in all aspects of cybersecurity. For example, we need to evaluate and reflect upon each software failure and break in the supply chain to gain greater process insights and develop long-term software assurance and supply chain management solutions. To do this, we will need to authenticate people, processes, and devices. In other words, we need to develop inherently secure business practices in supplying critical products. In terms of software, this means we need mechanisms that allow computer code to stand on its own merits and speak for itself.

As I mentioned earlier, DHS is taking steps to improve the overall cybersecurity posture of the Nation. Our approach interlocks strategically with other efforts that are on-going across the Federal Government, private sector, and across the country in States and localities. One of our most important initiatives is our effort to improve cybersecurity incident handling and response processes via the National Cyber Incident Response Plan, or NCIRP. The goal of the NCIRP is to build upon the concepts and methodologies of the National Response Framework, the National Incident Management System, and the NIPP. This is an interagency effort in coordination with State, local, Tribal and private sector partners to define the cyber incident roles and responsibilities across a wide spectrum of stakeholders. The plan will provide Federal agencies; State, local, and Tribal governments; and the private sector with a better understanding of how to respond to a cyber event during a crisis or under normal operating conditions. We will test the plan during the Cyber Storm III National Cyber Exercise this fall.

The NCIRP will be crucial for effective incident response, which will leverage the strength of our new operations center. During the first quarter of fiscal year 2010, DHS launched the National Cybersecurity and Communications Integration Center (NCCIC), a facility that improves our capability and capacity to detect, prevent, respond, and mitigate disruptions of the Nation's cyber and communications systems. The NCCIC collocates vital IT and communications operations centers, thereby converging existing incident response mechanisms and better reflecting the reality of technological convergence. Under the NIPP partnership framework, the collaborative activity of the NCCIC blends together the interdependent missions of the National Coordinating Center for Telecommunications, US–CERT, the DHS Office of Intelligence and Analysis, and the National Cyber Security Center. We are working through the legal and operational details to enable the planned inclusion of private sector representation on the NCCIC floor.

CONCLUSION

I appreciate the opportunity to speak with you today about the progress that the Department has made and the road ahead for future improvements to our Nation's cybersecurity. DHS is committed to working collaboratively with our public, private, academic, and interagency partners to ensure that the cyber elements of our Nation's critical infrastructure are secure. We strive to ensure that these systems are robust enough to withstand attacks, responsive enough to recover from attacks, and resilient enough to sustain critical operations. We will continue to build upon our efforts and create more effective partnership opportunities that will allow us to make our Nation's critical infrastructure safer and more secure.

Again, thank you for this opportunity to testify. I would be happy to answer any questions you may have.

Chairman THOMPSON. Thank you for your testimony, Mr. Schaffer.

We are now recognizing Inspector General Skinner to summarize his statement for 5 minutes.

STATEMENT OF RICHARD L. SKINNER, INSPECTOR GENERAL, DEPARTMENT OF HOMELAND SECURITY

Mr. SKINNER. Thank you. Good morning, Chairman Thompson and Ranking Member King and Members of the committee. Thank you for inviting me here today to discuss the results of our most recent report on the Department of Homeland Security's U.S. Community Emergency Readiness Team, or as we refer to it as US–CERT. If I can indulge the committee for just a few seconds, I would like to introduce three staff members that I brought with me today, and that is Frank Deffer, Barbara Bartuska, and Shannon Frenyea, who were very instrumental in the preparation of this report and very instrumental in a lot of our IT work in the Department. I am often referred to as a cyber immigrant; that is, I was not born into this cyber world. So a lot of this stuff is very, very foreign to me and I rely very heavily on the people that I brought with me today to advise me.

No one here in this room I am sure questions the importance of cybersecurity. Our economy, our critical infrastructure, our National security all relies on technology and I think we have a very important mission here, departmentally and in security, to make sure we protect that technology.

The Department in my opinion has come a long way since 9/11 in protecting cybersecurity, particularly in the last 2 years. They have been working very, very hard in building relationships and building partnerships and developing guidelines and issuing reports and building infrastructure within the Department to address cybersecurity on a National scale. But as our audit demonstrated, there is a lot more that needs to be done. There are a lot of challenges out there. We raise essentially five issues that we think have or is hindering our ability to move forward.

One is sustaining leadership. Over the last 5 years, US–CERT has had five directors. In our opinion, we think that in fact can impede and is in fact impeding our ability to move forward. Without the leadership to direct our strategic plans and guide our day-to-day operations, it is going to slow us down.

The second thing is the investment of resources. It was not until 2008 did the Secretary of Department of Homeland Security identify cybersecurity as a top priority. Now, when you interpret that into dollars, it was not until 2010 were the funds put aside or increased to allow the Department to build its cybersecurity capabilities. If you look at 2008, I think there were only 38 people working in US–CERT. There is now authorization to bring that up to 98 people. But I believe as of this past week or as of last Friday, there was only 55 of those people on board. For a variety of reasons it is very, very difficult not to just bring bodies on board, but to bring the right talent on board. There is a lot of efforts underway to bring those people on board. But it is slow. Until we have those resources, we are going to continue to run into impediments in implementing our National cybersecurity strategy.

The third thing I think that is very important—and this is where I think Congress can play a very important role—and that is the lack of authority to enforce its guidelines and its recommendations. The US–CERT makes recommendations to other Federal agencies and to its critical infrastructure and issues guidelines. What the

they cannot do is compel compliance and until they have that authority or until there are mechanisms in place to ensure that compliance is, in fact, taking place, we are going to continue to experience problems.

The fourth thing I think that needs to be recognized is that we are not in this alone. This is a partnership. We rely very, very heavily on the private sector and within our Federal partners. If you look around, one of the things that I thought was very interesting when we did our review is that it was only 21 Federal agents or 20 Federal agencies, one State agency that has EINSTEIN or installed EINSTEIN into their infrastructure. Twenty-one in all of Federal Government. There is a variety of reasons why we are not moving faster there. One, IT could be a resource issue, a financial issue, it could be a technological issue. But there is many reasons why we cannot install more. But we need to put pressure on our Federal partners, our stakeholders in the private sector, to start taking cybersecurity a little more seriously, or a lot more seriously and start using the tools that we have developed to help them to secure their networks, communication systems and their computers.

The last thing I would like to just mention I think is something that we can do a better job of, but it requires additional resources and it requires an investment of time. That is our outreach efforts, our education, and our training programs in our communications with our partners and our stakeholders. I know we have come a long way. We are doing a lot better job of that. The Department is doing a lot better job of that. But we still have a long way to go.

Many of the stakeholders we talked to during the course of our audit complained, No. 1, that they didn't understand EINSTEIN; No. 2, they weren't adequately trained on EINSTEIN once they did have it; No. 3, they did not feel that the information was being adequately shared as a result of some of the work that US–CERT is doing. We recommend in our report that in essence we need to explore better ways to ensure that our partners are fully informed and understand what we are doing, why we are doing it, and when we are doing it. I think that can go a long way. That is education, training, and outreach and communications.

In summary, let me just say there is a lot of progress here, but nonetheless, there is a lot more that needs to be done and I think that we are heading in the right direction. I think US–CERT is heading in the right direction, the Department is heading in the right direction. We are starting to invest resources, but it is going to take time. It is not going to happen next week. It is going to take a sustained effort.

Thank you. That concludes my opening remarks. As always, of course, I will be happy to answer any questions you may have.

[The statement of Mr. Skinner follows:]

PREPARED STATEMENT OF RICHARD L. SKINNER

JUNE 16, 2010

Chairman Thompson, Ranking Member King, and Members of the committee: Thank you for inviting me here today to discuss the Department of Homeland Security's U.S. Computer Emergency Readiness Team, or US–CERT.

My testimony today will address US–CERT's progress made thus far, and remaining challenges for its analysis and warning program. The information provided in this testimony is contained in our June 2010 report, "U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain" (OIG–10–94).

BACKGROUND

The Department of Homeland Security (DHS) is responsible for developing the National cyberspace security response system, which includes providing crisis management support and coordinating with other agencies to provide warning information. The National Cyber Security Division (NCSD) created US–CERT in 2003 to protect the Federal Government network infrastructure by coordinating efforts to defend against and respond to cyber attacks. Specifically, US–CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating cyber incident response activities.

Additionally, US–CERT collaborates with Federal agencies, the private sector, the research community, academia, State, local, and Tribal governments, and international partners. Through coordination with various National security incident response centers in responding to potential security events and threats on both classified and unclassified networks, US–CERT disseminates cybersecurity information to the public.

Further, NCSD developed the National Cybersecurity Protection System, operationally known as Einstein, to provide US–CERT with a situational awareness snapshot of the health of the Federal Government's cyberspace. US–CERT manages Einstein and maintains its public website and secure portal to fulfill the mission. Technologies, such as Einstein, enable US–CERT to detect unusual and previously identified network traffic patterns and trends that signal unauthorized, threatening, or risky networks activities and categorize anomalous activity that could pose a risk to US–CERT constituents. US–CERT uses other systems in addition to Einstein. Through fusion of information received from all of these sources, US–CERT is able to prioritize and escalate cyber activity appropriately, coordinate incident response activities, and share alerts, warnings, and mitigation strategies regarding threats and vulnerabilities.

Actions Taken to Address Cybersecurity

US–CERT has made progress in developing and implementing the capabilities to detect and mitigate cyber incidents across Federal agencies' networks. Similarly, US–CERT leads and coordinates efforts to improve the Nation's cybersecurity posture, promote cyber information sharing, and mitigate cyber risks.

For example, the Office of Cybersecurity and Communications developed the National Cybersecurity and Communications Integration Center (NCCIC), which is a unified operations center to address security threats and incidents that may affect the Nation's critical information systems and network infrastructure. The NCCIC consists of the following organizations: National Communications System, National Coordinating Center; NCSD, US–CERT; NCSD Industrial Control System Cyber Emergency Response Team; Office of Intelligence and Analysis; National Cybersecurity Center; Department and Agency, Security Operations Centers; Law Enforcement and Intelligence Community; and the private sector. Specifically, the NCCIC helps DHS to fulfill its mission to secure cyberspace by supporting the decision making process for the Federal Government, and enabling incident response through shared situational awareness. As a result, the NCCIC serves as the "central repository" for the cyber protection efforts of the Federal Government and its private sector partners.

Other actions designed to improve the expertise of US–CERT staff and information sharing include the following:

- Conducting in-person and on-line training to increase individual's knowledge, skills, and abilities regarding specific information topics that are relevant to US–CERT operations. Training relates to packet capture analysis and signature development; malware; and web browser security.
- Participating in public and private sector working groups to promote information sharing and collaboration. The working groups assist in the coordination and mitigation of computer and cybersecurity incidents as well as the development of best security practices.
- Distributing US–CERT products regarding specific vulnerabilities and situational awareness, as well as quarterly trend and analysis reports, to public and private sectors.

Improvements Needed to Strengthen the Cybersecurity Program

Notwithstanding its many accomplishments over the past several years, US–CERT is still hindered in its ability to provide an effective analysis and warning program for the Federal Government in a number of ways. Specifically, US–CERT does not have the appropriate enforcement authority to help mitigate security incidents. Additionally, it is not sufficiently staffed to perform its mission. Further, US–CERT has not finalized and approved its performance measures and policies and procedures related to cybersecurity efforts.

Enforcement Authority Could Help Mitigate Security Incidents

US–CERT does not have the appropriate enforcement authority to ensure that agencies comply with mitigation guidance concerning threats and vulnerabilities. It needs the authority to enforce its recommendations so that Federal agencies' systems and networks are protected from potential cyber threats. Without this authority, US–CERT is limited in its ability to mitigate effectively ever evolving security threats and vulnerabilities.

However, US–CERT was not given the authority to compel agencies to implement its recommendations to ensure that system vulnerabilities and incidents are remediated timely. US–CERT management officials stated that the proposed Federal Information Security Management Act (FISMA) 2008 legislation would have given it some leverage to implement incident response and cybersecurity recommendations. For example, the proposed legislation would have required agencies to address incidents that impair their security. Further, the agencies would have had to collaborate with others if necessary to address the incidents. Additionally, agencies would be required to respond to incidents no later than 24 hours after discovery or provide notice to US–CERT as to why no action was taken. Finally, agencies would have had to ensure that information security vulnerabilities were mitigated timely. Since the proposed legislation was not approved, US–CERT remains without enforcement authority.

US–CERT's notices contain recommendations that address the threats and vulnerabilities in Federal agencies' infrastructures. Additionally, US–CERT products help to update Federal information security policy and guidance. However, without the enforcement authority to implement recommendations, US–CERT continues to be hindered in coordinating the protection of Federal cyberspace.

Additional Staffing Could Help Meet Mission

US–CERT does not have sufficient staff to perform its 24/7 operations as well as to analyze security information timely. US–CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners. Without sufficient staffing, US–CERT cannot completely fulfill its responsibilities to analyze data and reports to reduce cyber threats and vulnerabilities as well as support the public and private sectors.

Although US–CERT's authorized positions were increased from 38 in 2008 to 98 in 2010, as of January 2010, only 45 positions are filled. In October 2009, the DHS Secretary announced that cybersecurity is an urgent priority for the Nation and the Department would hire additional cyber analysts, developers, and engineers to ensure that crucial computer networks are not vulnerable to possible cyber attacks. Currently, US–CERT augments its staffing shortages by contractor support.

Strategic Plan and Performance Measures are Needed

US–CERT has not developed a strategic plan to formalize goals, objectives, and milestones. Specifically, US–CERT has not identified or prioritized key activities for the division to monitor its progress in accomplishing its mission and goals. Without a strategic plan and performance measures, US–CERT may have difficulty in achieving its goal to provide response support and defense against potential cyber attacks for the Federal Government.

According to program officials, US–CERT is developing a strategic plan and revising the performance measures to align with the strategic plan. The strategic plan should describe how US–CERT will perform its critical role by identifying and aligning goals, objectives, and milestones through a variety of means and strategies. Also, the strategic plan should contain performance measures related to specific programs, initiatives, products, and outcomes.

As the sophistication and effectiveness of cyber attacks have been steadily advancing in recent years, a strategic plan can help US–CERT to ensure that critical milestones and goals are accomplished in a timely manner. Further, strategic plan and performance measures will aid US–CERT in evaluating its progress in building an effective organization capable of mitigating long-term cyber threats and

vulnerabilities and improve program operations by promoting the appropriate application of information resources.

Policies and Procedures Have Not Been Approved

US–CERT has not approved its policies and procedures to ensure that management and operational controls are implemented to defend against, analyze, and respond to cyber attacks. Without the approved policies and procedures, US–CERT may be hindered in its ability to respond to security incidents effectively and promote continuity of operations and consistency.

Leadership and staff turnover and a continually evolving mission have hindered US–CERT's past efforts to update its standard operating procedures. Under the prior director, US–CERT outsourced to contractors off-site the function to maintain and update procedures. The process of updating the procedures discontinued once the director departed. Further, US–CERT officials determined that the outsourced procedures did not fully address the mission or the day-to-day activities that cyber analysts encounter. According to the officials, outsourcing off-site was not the best method to update these policies and procedures since US–CERT personnel have a better understanding of its mission. After internal reassessment, US–CERT officials decided to use contractor support on-site to develop more concise and direct SOPs.

Currently, US–CERT is in the process of developing appropriately 80–90 standard operating procedures (SOP) for its four sections pertaining to various areas of activity, such as, network and targeted analyses, malware submission handling, and signature template development. The goal is to have a structure that maps to functions, roles, the organization, and the mission. US–CERT is attempting to make the procedures understandable and practical with contents based on analysts' experiences.

Better Information Sharing and Communication Can Enhance Coordination Efforts With the Public

US–CERT needs to improve its information sharing and communication efforts with Federal agencies to ensure that threats and vulnerabilities are mitigated timely. Specifically, officials from other Federal agencies expressed concerns that US–CERT was unable to share near real-time data and classified and detailed information to address security incidents.

We interviewed officials from eight Federal agencies to obtain feedback on Einstein and to determine whether US–CERT shared sufficient information and communicated effectively. Overall, these agency officials indicated that Einstein is an effective tool but expressed concerns regarding the effectiveness of US–CERT's information sharing and communication.

Officials from six agencies expressed concerns regarding US–CERT not sharing Einstein data and analysis results. According to some of the Federal agency officials we interviewed, US–CERT agreed that they would have access to the Einstein flow data but subsequently did not provide the information. This data could assist agencies in performing analyses with their locally collected data to identify potential threats and vulnerabilities. Also, agency officials stated that it would be helpful for US–CERT to list which agencies are being attacked and provide common trends to other agencies to determine whether the incident is isolated or systemic.

Further, agencies indicated that US–CERT has not provided sufficient training on the Einstein program. Some agencies indicated that they received compact disk, portable document format brochures, and handbooks about the Einstein program, while other agencies received nothing. Agencies indicated that they would like to receive additional Einstein training from US–CERT.

US–CERT officials acknowledged that there are communications issues regarding sharing classified and detailed information with other agencies. For example, US–CERT collects and posts information from several systems and sources to different portals, all of which have different classification levels. As a result, US–CERT officials believe that communications needs could be best addressed by developing a consolidated information sharing portal. The consolidated portal could provide a multiple classification platform and serve as a central repository to meet the needs of the stakeholders.

A challenge US–CERT faces is that many intelligence agencies communicate classified information on Top Secret/Sensitive Compartmented Information networks. Since not all agencies have access to classified networks, US–CERT is limited in what it can convey. Some agencies do not have secure facilities, equipment, and cleared personnel to send or receive classified information.

Additionally, US–CERT has to deal with the various network architectures of the different agencies. Since US–CERT does not have access to each agency's architecture, it is imperative to have the agency Chief Information Officer (CIO) and Chief

Information Security Officer (CISO) involved in addressing cyber activities. Establishing direct, regular communication with agency CIOs/CISOs or key security assurance personnel ensures that US–CERT's cybersecurity efforts are implemented. For example, US–CERT and the CIO/CISO can determine what should be implemented to improve the agency's situational awareness. Further, they can address network and cybersecurity challenges such as fragmented infrastructures, legacy systems, and limited budgets.

Currently, US–CERT uses working groups and portals to share information with the public and private sectors. For example, US–CERT established the Joint Agency Cyber Knowledge Exchange and Government Forum of Incident Response and Security Teams (GFIRST) to facilitate collaboration on detecting and mitigating threats to the ".gov" domain and to encourage proactive and preventative security practices. The Joint Agency Cyber Knowledge Exchange meetings are held at a classified level to discuss threat-related tactics, techniques, and protocol. Additionally, US–CERT disseminates various reports and notices through the GFIRST and US–CERT portals. Products US–CERT disseminates include: Situational Awareness Reports, Critical Infrastructure Information Notices, Federal Information Notices, Early Warning Indicator Notices, and Malware Initial Findings Reports. These products contain a summary of the incident, mitigation strategies, and best practices. The products are disseminated to stakeholders on an as-needed, daily, monthly, or quarterly basis.

It is essential that US–CERT and the public and private sectors share cybersecurity information to ensure that appropriate steps can be taken to mitigate the potential effect of a cyber incident. US–CERT cannot defend against and respond consistently and effectively to cyberactivity without other agencies' involvement. By sharing potential security threats collected through its data sources, US–CERT can provide agencies with detailed information regarding attacks to their networks.

Improved Situational Awareness and Identification of Network Anomalies Can Better Protect Federal Cyberspace

US–CERT is unable to monitor Federal cyberspace in real time. The tools US–CERT uses do not allow real-time analyses of network traffic. As a result, US–CERT will continue to be challenged in protecting the Federal cyberspace from security-related threats.

Currently, US–CERT maintains near real-time situational awareness as it performs information aggregation activities. US–CERT collects data real-time but it must perform analysis on the data in near real-time. Cyber analysts receive information from a variety of sources and other US–CERT activities to identify potential incidents and to assess their possible scope and impact on the Nation's cyber infrastructure.

Einstein is being deployed in three different versions, whereby, each builds on the capabilities of the previous version:

- Einstein 1 (E1) collects and relies on net flow analysis capability and uses net flow collectors. Net flow data is queried for analysis.
- Einstein 2 (E2) is an intrusion detection system, but is still passive, performing analysis while traffic is continuous. E2 looks for anomalous activity from net flow information based on every session between two computers on the internet. E2 is more beneficial for detecting and mitigating cyber incidents because of its ability to analyze packet data. Additionally, E2 performs full session packet analysis.
- Einstein 3 (E3) draws on commercial technology and specialized Government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving the Executive branch networks. This system also deploys an intrusion prevention feature.

With Einstein, US–CERT can gather more network traffic information and identify cyber activity patterns. However, US–CERT cannot capture all network traffic because Einstein has not been deployed to all Federal agencies. Initially, the deployment of E1 to Federal agencies was entirely voluntary. In September 2008, OMB made Einstein part of the Trusted Internet Connections initiative and required all agencies to install sensors on their networks.

As of October 2009, NCSD's Network Security Deployment Branch had deployed E1 to 19 agencies and E2 to 8 agencies. Currently, US–CERT is conducting a pilot exercise of E3 to evaluate its capabilities. According to the Comprehensive National Cybersecurity Initiative and US–CERT officials, E3 will contain real-time full packet inspection and an intrusion prevention feature. These additions should give US–CERT better response and monitoring capabilities.

According to US–CERT officials, many agencies have not installed Einstein because they have not consolidated their gateways to the internet. Further, some

agencies have fragmented networks and must upgrade their architectures before Einstein can be deployed.

Additionally, US–CERT does not have an automated correlation tool to identify trends and anomalies. With this vast amount of network traffic, US–CERT experienced a long lead time to analyze potential security threats or abnormalities. To reduce the lead time, NCSD purchased an automated correlation tool to analyze the vast amount of data from Einstein. However, US–CERT is currently experiencing problems with reconfiguring the tool to collect data and understand the overall data flow. US–CERT management stated that it may be 6 months before the problems are corrected and the benefits of the system can be seen.

An effective analysis and warning program is critical to secure the Federal information technology infrastructure. For US–CERT to perform its responsibilities successfully it must have sufficient state-of-the-art technical and analytical tools and technologies to identify, detect, analyze, and respond to cyber attacks. Additionally, cybersecurity information can provide the public and private sectors with valuable input for mitigating risks and threats, protecting against malicious attacks, and prioritizing security improvement efforts.

CONCLUSION AND RECOMMENDATIONS

US–CERT has made progress in implementing a cybersecurity program to assist Federal agencies in protecting their information technology systems against cyber threats. Specifically, it has facilitated cybersecurity information sharing with the public and private sectors through various working groups, issuing notices, bulletins, and reports, and web postings. Further, Office of Cybersecurity and Communications established a unified operations center, which includes US–CERT, to address threats and incidents affecting the Nation's critical information technology and cyber infrastructure. To increase the skills and expertise of its staff, US–CERT has developed a technical mentoring program to offer cybersecurity and specialized training.

While progress has been made, US–CERT still faces numerous challenges in effectively reducing the cybersecurity risks and protecting the Nation's critical infrastructure. US–CERT must continue to improve its ability to analyze and reduce cyber threats and vulnerabilities and to disseminate information through a cohesive effort between public and private sectors.

We recommended in our report that the Under Secretary of National Protection and Programs Directorate (NPPD) require the Director of NCSD to:

- Establish specific outcome-based performance measures and a strategic plan to ensure that US–CERT can achieve its mission, objectives, and milestones.
- Approve policies and procedures to ensure that US–CERT can effectively detect, process, and mitigate incidents as well as perform its roles and responsibilities in a consistent manner.
- Improve communications with Federal agency CIOs and CISOs to address their concerns, to identify areas of improvement about the program, and to enhance US–CERT's ability to combat cybersecurity challenges.
- Establish a consolidated, multiple classification level portal that can be accessed by the Federal partners that includes real-time incident response-related information and reports.
- Develop a process to distribute and share Einstein trends, anomalies, and common/reoccurring attacks with other Federal agencies.
- Provide training to Federal agencies on using available features of Einstein to foster better cooperation in analyzing and mitigating security incidents.
- Establish a capability to share real-time Einstein information with Federal agencies partners to assist them in the analysis and mitigation of incidents.

Mr. Chairman and Members of the committee, you can be sure that my office is committed to continuing our oversight efforts for this challenging and complex issue in the months and years ahead.

This concludes my prepared statement, and I welcome any questions from you or Members of the committee.

Chairman THOMPSON. Well, I am sure we will. Thank you for your testimony.

I now recognize Director Wilshusen to summarize his statement for 5 minutes.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION TECHNOLOGY, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Thompson, Ranking Member King, and Members of the committee, thank you very much for inviting me today to testify at today's hearing on cybersecurity.

Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of the Federal Government. In recent testimony, the Director for National Intelligence highlighted that many nation-states, terrorist networks, and organized criminal groups have the capability to target U.S. information infrastructure for intelligence collection, intellectual property theft, or disruption.

The ever-increasing dependence of Federal agencies on information systems to carry out essential everyday operations can make them vulnerable to an array of cyber-based risks. Thus, it is increasingly important that the Federal Government carry out a concerted effort to safeguard its systems and the information they contain.

Today I would describe cyber threats to Federal systems and cyber-based critical infrastructures, the control deficiencies that make Federal systems vulnerable to those threats, and opportunities that exist for improving Federal cybersecurity.

Mr. Chairman, cyber-based threats to Federal systems and critical infrastructure are evolving and growing. These threats can come from a variety of sources, including criminals and foreign nations as well as hackers and disgruntled employees. These potential attackers have various techniques at their disposal, which can vastly enhance the reach and impact of their actions. For example, cyber attackers do not need to be physically close to their assets. Their attacks can easily cross State and national borders, and cyber attackers can more readily preserve their anonymity.

Further, the interconnectivity between information systems, the internet and other infrastructure creates additional avenues for such attacks. Consistent with this, reports of security incidents from Federal agencies are on the rise, as the Chairman pointed out earlier, increasing by over 400 percent from fiscal year 2006 to 2009.

Compounding the growing number and kinds of threats, GAO and agency inspectors general have identified significant security control deficiencies on Federal systems. Indeed, most agencies have weaknesses in most types of security controls such as access controls, configuration management, and security management. These weakness affect the security of both financial and nonfinancial systems, including systems essential to achieving agency missions. They also continue to place Federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, and critical operations at risk of disruption.

Fortunately, Mr. Chairman, multiple opportunities exist to improve Federal cybersecurity. To address, identify deficiencies in agency security controls and shortfalls in their information security programs, GAO and agency IGs have made hundreds of recommendations over the past several years, many of which agencies

are implementing. In addition, the White House, the Department of Homeland Security, and other Federal agencies have undertaken several Government-wide initiatives intended to enhance Federal security. While progress is made on these initiatives, they all face challenges that requires sustained attention, and GAO has made recommendations for improving the implementation and effectiveness of these initiatives.

Further, the Department of Homeland Security also needs to fulfill its key cybersecurity responsibilities such as developing capabilities for ensuring the protection of cyber-based critical infrastructures and developing a robust cyber analysis and warning capability.

Finally, a GAO-convened panel of experts has made several recommendations for improving the Nation's cybersecurity strategy, including, for example, developing a National strategy that articulates the goals, objectives, and priorities and that focuses more on prioritizing assets and assessing and reducing vulnerabilities and on developing additional plans. Realizing these opportunities for improvement can help provide additional insurance to the Federal information systems and critical cyber-based infrastructures are effectively protected.

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

[The statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

Chairman Thompson and Members of the committee: Thank you for the opportunity to testify at today's hearing on cybersecurity regarding our recent work on challenges facing Federal efforts to protect systems and critical infrastructure from cyber-based threats.

Pervasive and sustained cyber attacks against the United States continue to pose a potentially devastating impact on Federal systems and operations. In February 2010, the Director of National Intelligence testified that many nation-states, terrorist networks, and organized criminal groups have the capability to target elements of the U.S. information infrastructure for intelligence collection, intellectual property theft, or disruption.[1] As recently as July 2009, press accounts reported that a widespread and coordinated attack over the course of several days targeted websites operated by major Government agencies, including the Departments of Homeland Security and Defense, the Federal Aviation Administration, and the Federal Trade Commission, causing disruptions to the public availability of Government information. Such attacks highlight the importance of developing a concerted response to safeguard Federal information systems.

In my testimony today, I will describe: (1) Cyber threats to Federal information systems and cyber-based critical infrastructures, (2) control deficiencies that make Federal systems vulnerable to those threats, and (3) opportunities that exist for improving Federal cybersecurity. In preparing this statement in June 2010, we relied on our previous reports on Federal information security. These reports contain detailed overviews of the scope and methodology we used. The work on which this statement is based was performed in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

[1] Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence,* statement before the Senate Select Committee on Intelligence (Feb. 2, 2010).

BACKGROUND

As computer technology has advanced, Federal agencies have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Virtually all Federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions without these information assets. Information security is thus critically important. Conversely, ineffective information security controls can result in significant risks. Examples of such risks include the following:

- Resources, such as Federal payments and collections, could be lost or stolen.
- Sensitive information, such as National security information, taxpayer data, Social Security records, medical records, and proprietary business information, could be inappropriately accessed and used for identity theft or espionage.
- Critical operations, such as those supporting critical infrastructure, National defense, and emergency services could be disrupted.
- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in the ability of Federal organizations to conduct operations and fulfill their responsibilities.

FEDERAL SYSTEMS AND INFRASTRUCTURES FACE INCREASING CYBER THREATS

Threats to Federal information systems and cyber-based critical infrastructures are evolving and growing. Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and foreign nations. Federal law enforcement and intelligence agencies have identified multiple sources of threats to our Nation's critical information systems, including foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors.

These groups and individuals have a variety of attack techniques at their disposal. Furthermore, as we have previously reported,[2] the techniques have characteristics that can vastly enhance the reach and impact of their actions, such as the following:

- Attackers do not need to be physically close to their targets to perpetrate a cyber attack.
- Technology allows actions to easily cross multiple State and national borders.
- Attacks can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time.
- Attackers can easily remain anonymous.

The connectivity between information systems, the internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. As Government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

Reported Security Incidents Are on the Rise

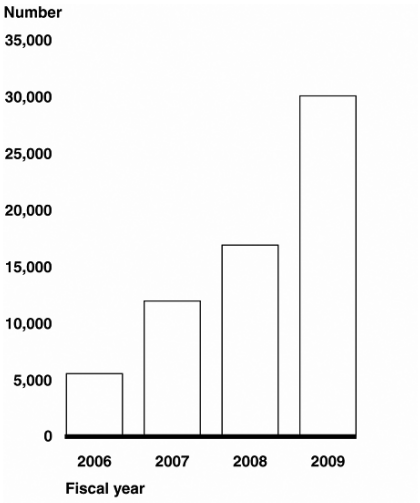
Consistent with the evolving and growing nature of the threats to Federal systems, agencies are reporting an increasing number of security incidents. These incidents put sensitive information at risk. Personally identifiable information about U.S. citizens has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

When incidents occur, agencies are to notify the Department of Homeland Security's (DHS) Federal information security incident center—the United States Computer Emergency Readiness Team (US–CERT). As shown in figure 1, the number of incidents reported by Federal agencies to US–CERT has increased dramatically over the past 4 years, from 5,503 incidents reported in fiscal year 2006 to about 30,000 incidents in fiscal year 2009 (over a 400 percent increase).

---

[2] GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats,* GAO–07–705 (Washington, DC: June 22, 2007).

Figure 1: Incidents Reported to US-CERT in Fiscal Years 2006 through 2009



Source: GAO analysis of US-CERT data.

The four most prevalent types of incidents and events reported to US–CERT during fiscal year 2009 were: (1) Malicious code (software that infects an operating system or application), (2) improper usage (a violation of acceptable computing use policies), (3) unauthorized access (where an individual gains logical or physical access to a system without permission), and (4) investigation (unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review).

VULNERABILITIES PERVADE FEDERAL INFORMATION SYSTEMS

The growing threats and increasing number of reported incidents highlight the need for effective information security policies and practices. However, serious and widespread information security control deficiencies continue to place Federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. GAO has designated information security as a high-risk area in the Federal Government since 1997.

In their fiscal year 2009 performance and accountability reports, 21 of 24 major Federal agencies noted that inadequate information system controls over their financial systems and information were either a material weakness or a significant deficiency.[3]

Similarly, our audits have identified control deficiencies in both financial and nonfinancial systems, including vulnerabilities in critical Federal systems. For example, we reported in September 2008[4] that, although the Los Alamos National Laboratory—one of the Nation's weapons laboratories—implemented measures to enhance the information security of its unclassified network, vulnerabilities continued to

[3] A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis.

[4] GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network,* GAO–08–1001 (Washington, DC: Sept. 9, 2008).

exist in several critical areas. Similarly, in October 2009[5] we reported that the National Aeronautics and Space Administration (NASA)—the civilian agency that oversees U.S. aeronautical and space activities—had not always implemented appropriate controls to sufficiently protect the confidentiality, integrity, and availability of the information and systems supporting its mission directorates.

OPPORTUNITIES EXIST FOR ENHANCING FEDERAL CYBERSECURITY

Over the past several years, we and agency inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies. Agencies have implemented or are in the process of implementing many of our recommendations.

In addition, the White House, OMB, and certain Federal agencies have undertaken several Government-wide initiatives that are intended to enhance information security at Federal agencies. However, these initiatives face challenges that require sustained attention:

- *Comprehensive National Cybersecurity Initiative (CNCI).*—In January 2008, President Bush initiated a series of 12 projects aimed primarily at improving the Department of Homeland Security's (DHS) and other Federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[6] The initiative is intended to reduce vulnerabilities, protect against intrusions, and anticipate future threats against Federal Executive branch information systems. As we recently reported,[7] the White House and Federal agencies have established interagency groups to plan and coordinate CNCI activities. However, the initiative faces challenges in achieving its objectives related to securing Federal information, including better defining agency roles and responsibilities, establishing measures of effectiveness, and establishing an appropriate level of transparency. Until these challenges are adequately addressed, there is a risk that CNCI will not fully achieve its goals.
- *Federal Desktop Core Configuration (FDCC).*—For this initiative, OMB directed agencies that have workstations with Windows XP and/or Windows Vista operating systems to adopt security configurations developed by the National Institute of Standards and Technology, the Department of Defense, and DHS. The goal of this initiative is to improve information security and reduce overall information technology operating costs. We recently reported[8] that while agencies have taken actions to implement FDCC requirements, none of the agencies has fully implemented all configuration settings on their applicable workstations. In our report we recommended that OMB, among other things, issue guidance on assessing the risks of agencies having deviations from the approved settings and monitoring compliance with FDCC.
- *Einstein.*—This is a computer network intrusion detection system that analyzes network flow information from participating Federal agencies and is intended to provide a high-level perspective from which to observe potential malicious activity in computer network traffic. We recently reported[9] that as of September 2009, fewer than half of the 23 agencies reviewed had executed the required agreements with DHS, and Einstein 2 had been deployed to 6 agencies. Agencies that participated in Einstein 1 cited improved identification of incidents and mitigation of attacks, but determining whether the initiative is meeting its

[5] GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks,* GAO–10–4 (Washington, DC: Oct. 15, 2009).

[6] The White House, National Security Presidential Directive—54/Homeland Security Presidential Directive—23 (Washington, DC: Jan. 8, 2008).

[7] GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative,* GAO–10–338 (Washington, DC: Mar. 5, 2010).

[8] GAO, *Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements,* GAO–10–202 (Washington, DC: Mar. 12, 2010).

[9] GAO, *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies,* GAO–10–237 (Washington, DC: Mar. 12, 2010).

objectives will likely remain difficult because DHS lacks performance measures that address how agencies respond to alerts.

- *Trusted Internet Connections (TIC) Initiative*.—This is an effort designed to optimize individual agency network services through a common solution for the Federal Government. The initiative is to facilitate the reduction of external connections, including internet points of presence. We recently reported[10] that none of the 23 agencies we reviewed met all of the requirements of the TIC initiative, and most agencies experienced delays in their plans for reducing and consolidating connections. However, most agencies reported that they have made progress toward reducing and consolidating their external connections and implementing security capabilities.

DHS Needs to Fully Satisfy Its Cybersecurity Responsibilities

Federal law and policy[11] establish DHS as the focal point for efforts to protect our Nation's computer-reliant critical infrastructures[12]—a responsibility known as cyber critical infrastructure protection, or cyber CIP. We have reported since 2005 that DHS has yet to fully satisfy its key responsibilities for protecting these critical infrastructures. Our reports included recommendations that are essential for DHS to address in order to fully implement its responsibilities. We summarized these recommendations into key areas listed in table 1.

TABLE 1.—KEY CYBERSECURITY AREAS IDENTIFIED BY GAO

1.	Bolstering cyber analysis and warning capabilities.
2.	Improving cybersecurity of infrastructure control systems.
3.	Strengthening DHS's ability to help recover from Internet disruptions.
4.	Reducing organizational inefficiencies.
5.	Completing actions identified during cyber exercises.
6.	Developing sector-specific plans that fully address all of the cyber-related criteria.
7.	Securing internal information systems.

Source: GAO.

DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but the Department still has not fully implemented our recommendations, and thus further action needs to be taken to address these areas. For example, in July 2008, we reported[13] that DHS's US–CERT did not fully address 15 key attributes of cyber analysis and warning capabilities related to: (1) Monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, US–CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. As a result, we recommended that the Department address shortfalls associated with the 15 attributes in order to fully establish a National cyber analysis and warning capability as envisioned in the National strategy. DHS agreed in large part with our recommendations and has reported that it is taking steps to implement them.

Similarly, in September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS had demonstrated progress in addressing eight lessons it had learned from these efforts.[14] However, its actions to address the lessons had not been fully implemented. Specifically, while it had completed 42 of the 66 activities identified, the Department had identified 16 activities as on-going

[10] GAO–10–237.

[11] These include The Homeland Security Act of 2002, Homeland Security Presidential Directive—7, and the National Strategy to Secure Cyberspace.

[12] Critical infrastructures are systems and assets, whether physical or virtual, so vital to the Nation that their incapacity or destruction would have a debilitating impact on National security, National economic security, National public health or safety, or any combination of those matters. Federal policy established 18 critical infrastructure sectors: Agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; Government facilities; information technology; National monuments and icons; nuclear reactors, materials, and waste; postal and shipping; public health and health care; transportation systems; and water.

[13] GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability,* GAO–08–588 (Washington, DC: Jul. 31, 2008).

[14] GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise,* GAO–08–825 (Washington, DC: Sept. 9, 2008).

and 7 as planned for the future.[15] Consequently, we recommended that DHS schedule and complete all of the corrective activities identified in order to strengthen coordination between public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation. Since that time, DHS has continued to make progress in completing some identified activities but has yet to do so for others.

Improving the National Cybersecurity Strategy

Because the threats to Federal information systems and critical infrastructure have persisted and grown, efforts have recently been undertaken by the Executive branch to review the Nation's cybersecurity strategy. In February 2009, President Obama directed the National Security Council and Homeland Security Council to conduct a comprehensive review to assess the United States' cybersecurity-related policies and structures. The resulting report, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* recommended, among other things, appointing an official in the White House to coordinate the Nation's cybersecurity policies and activities, creating a new National cybersecurity strategy, and developing a framework for cyber research and development.[16] In response to one of these actions, the President appointed a cybersecurity coordinator in December 2009. We recently initiated a review to assess the progress made by the Executive branch in implementing the report's recommendations.

We also testified in March 2009 on needed improvements to the Nation's cybersecurity strategy.[17] In preparation for that testimony, we obtained the views of experts (by means of panel discussions) on critical aspects of the strategy, including areas for improvement. The experts, who included former Federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our National cybersecurity posture. The key strategy improvements identified by cybersecurity experts are listed in table 2.

TABLE 2.—KEY STRATEGY IMPROVEMENTS IDENTIFIED BY CYBERSECURITY EXPERTS

1.	Develop a National strategy that clearly articulates strategic objectives, goals, and priorities.
2.	Establish White House responsibility and accountability for leading and overseeing National cybersecurity policy.
3.	Establish a governance structure for strategy implementation.
4.	Publicize and raise awareness about the seriousness of the cybersecurity problem.
5.	Create an accountable, operational cybersecurity organization.
6.	Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7.	Bolster public-private partnerships through an improved value proposition and use of incentives.
8.	Focus greater attention on addressing the global aspects of cyberspace.
9.	Improve law enforcement efforts to address malicious activities in cyberspace.
10.	Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate Government and private sector efforts.
11.	Increase the cadre of cybersecurity professionals.
12.	Make the Federal Government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

These recommended improvements to the National strategy are in large part consistent with our previous reports and extensive research and experience in this area.[18] Until they are addressed, our Nation's most critical Federal and private sector cyber infrastructure remain at unnecessary risk of attack from our adversaries.

In summary, the threats to Federal information systems are evolving and growing, and Federal systems are not sufficiently protected to consistently thwart the threats. Unintended incidents and attacks from individuals and groups with mali-

[15] At that time, DHS reported that one other activity had been completed, but the Department was unable to provide evidence demonstrating its completion.

[16] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: May 29, 2009).

[17] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture,* GAO–09–432T (Washington, DC: Mar. 10, 2009).

[18] We are currently conducting additional reviews related to these improvements.

cious intent have the potential to cause significant damage to the ability of agencies to effectively perform their missions, deliver services to constituents, and account for their resources. To help in meeting these threats, opportunities exist to improve information security throughout the Federal Government. The prompt and effective implementation of the hundreds of recommendations by us and by agency inspectors general to mitigate information security control deficiencies and fully implement agency-wide security programs would strengthen the protection of Federal information systems, as would efforts by DHS to develop better capabilities to meets its responsibilities, and the implementation of recommended improvements to the National cybersecurity strategy. Until agencies fully and effectively implement these recommendations, Federal information and systems will remain vulnerable.

Mr. Chairman, this completes my prepared statement. I would be happy to answer any questions you or other Members of the committee have at this time.

Chairman THOMPSON. Thank you very much for your testimony.

I now recognize Mr. Baker, to summarize his statement for 5 minutes.

STATEMENT OF STEWART A. BAKER, PARTNER, STEPTOE & JOHNSON, LLP

Mr. BAKER. Thank you, Chairman Thompson. It is a pleasure to be here, Ranking Member King, Members of the committee. As you mentioned, Mr. Chairman, I have recently finished a book that deals with this problem and I thought that might be useful just to point out that while two past Presidents have raised this issue and concerns about security, we have never been able to talk about the risks in unclassified terms. But there was a study done, a completely unclassified study done of the Dalai Lama's network and what happened to the Dalai Lama's network recently that is completely unclassified and gives us a sense of just how urgent this problem was.

The Dalai Lama's network is actually very secure, it is well run and currently administered, and they understand that they are the subject of a lot of attacks. One person in that organization opened an e-mail from someone that they trusted. They opened an attachment that had survived anti-virus scrutiny. That one click, opening that one attachment, gave attackers access first to this person's machine, they downloaded information about that machine, uploaded compromising equipment that allowed them to compromise that machine and the network. When they were done, they were able to turn on the camera and watch that fellow at work, log every keystroke, turn on his mic and listen to him, download from the network all of the Dalai Lama's negotiating positions in the international negotiations.

These are things that are happening to us as well. Everyone in this room if they are of interest to a foreign power could have that happen to them. Crooks are doing the same thing. They have begun using these same tools to compromise electronic fund transfer authorities that people have to steal hundreds of millions of dollars from American businesses. This is really a crisis.

On the question of what—whether DHS, as the Chairman says, has what it needs, I think the answer is not yet. I think it is clear that this administration has taken the problem seriously, but probably has not moved quickly enough to address all of the issues. This committee can help, as can the President, by making it quite clear that the authorities, that it is granting DHS the kind of au-

thority that it needs to address these problems. More authority would be particularly welcome.

Two last points that I would raise. First, the Senate bill deals with a number of security issues and is a very good first step towards solving some of the security problems that we have.

The last point that I would make is simply the BP oil spill shows us how much damage a single company can do that the company cannot then redress. If we had known how bad things were, how many corners were being cut in the industry before that oil spill, we would have demanded action on the part of industry as well as the Government. Well, we do know that we face exactly that kind of crisis in the context of cybersecurity. We are going to have a meltdown of our critical and National infrastructure, and now is the time to begin raising the standards.

Thank you.

[The statement of Mr. Baker follows:]

PREPARED STATEMENT OF STEWART A. BAKER

JUNE 16, 2010

Chairman Thompson, Ranking Member King, Members of the committee, it is a pleasure to appear before you again on a topic of such importance. I am Stewart Baker, formerly the Assistant Secretary for Policy at the Department of Homeland Security, and I am speaking for myself.

I was responsible for cybersecurity policy while at DHS, and since leaving the Department, I have been practicing law and writing a book on, among other things, the risks posed by computer insecurity. I'm celebrating the release of the book today by attending this hearing, and I'm happy to share some of what I learned with you today. (Chapters of the book itself are also being made available for free on-line at *www.skatingonstilts.com.*)

The first and most important thing to know about the cybersecurity crisis is that you no longer need a clearance to understand how bad things are. For a decade or more, Presidents told us that we faced such a crisis, but they were never able to provide much detail. The crisis was classified. As a result, Americans didn't pay much attention, and they certainly weren't galvanized to action.

Thanks to a group of security researchers in Canada and elsewhere, though, we now have a good, unclassified analysis of what a cyberattack looks like. It is not pretty. And it is certainly not reassuring. If anything should stir the country to action on cybersecurity, it is the story of what was done to the Dalai Lama's computer network.

The Dalai Lama and his office have been using the internet since the 1990s. His network administrators understand security risks, and they've been careful about computer security for years. They've implemented the standard defenses against network attacks.

But even so, they kept getting signals that their communications had been compromised. So they called in a team of computer security experts.

What the experts found was deeply troubling, and not just for the Dalai Lama.

Some of the Dalai Lama's staff participate in internet forums. They chat with other, like-minded individuals about the Dalai Lama's goals and activities. Sometimes one of their online acquaintances sends them Word or .PDF documents relevant to those activities.

No surprises there. Most of us have done most of those things.

But the experts concluded that hackers had monitored these forums and then forged an email from a forum participant to a member of the Dalai Lama's staff. Attached to the email was a document of mutual interest. When the staff member opened the document, he also activated a piece of malware packed with it. While the staff member was reading the document, the malware installed itself in the background.

The malware was cleverly designed; two-thirds of commercial antivirus software programs would have missed it. (Hackers often subscribe to antivirus software so they can test their malware against it at leisure.) Even if one attachment were stopped, it was a simple matter to retransmit the message using a different bit of malware; the attackers could keep trying until something got through.

Once installed, the malware would "phone home," uploading information about the victim's computer and files to a control server operated by the hackers.

Next, the captured computer would download more malware to install on the staff member's machine. This was often a complete administrative program that would allow the attackers to completely control the staffer's computer, and in some cases the entire network.

The administrative malware took full advantage of today's technology. It featured a graphic interface with dropdown menus offering even an unsophisticated attacker a wide variety of options.

Want to record every keystroke as the user types so you can steal all his passwords? Check one of the options on the menu.

Want to turn on the user's microphone, turning it into a bug so you can listen to the office conversations? Check another box.

Want video straight from the user's desktop camera? That's just another option on the menu.

In the end, the Dalai Lama's office was living a version of Orwell's 1984. Telescreens in each room spied on the occupants. But in this version of 1984, Big Brother didn't even have to pay for this spy equipment. It had been purchased and installed by the victims.

Once the hackers had compromised a single computer on the network, it wasn't hard to compromise more. Every time an infected computer sent a document by email, malware could be attached to the file. The recipient couldn't possibly be suspicious; the email and attachment were exactly what he expected to receive from his colleague, and it had been reviewed by an antivirus program. He opened the document. The malware installed itself in the background. The cycle began again. It was an entire network of surveillance, dubbed Ghostnet by the security team.

Ghostnet has lessons for all of us, including Members of this committee. Do you rely on standard commercial antivirus software to scan attachments? Do you open documents sent by people you've encountered on-line? How about documents from sources, contributors, or constituents? How about colleagues, coworkers, and staff? Of course, you do. So do I. And that means that most of us are no more able to defend ourselves from this attack than the Dalai Lama was.

That means we have no guarantee that foreign governments have not penetrated our home or even our office computer networks in the same way as the Dalai Lama, no guarantee that they are not monitoring our every keystroke on-line.

Indeed, when I talk to computer security experts about how to defend against intrusions, they usually tell me to assume that the intrusions have happened before and will happen again. Because there's no way to stop them. At best, you might be able to catch the intruders when they try to steal your data. But you can't count on that, either.

Now that we understand the scope of the problem, what are we doing about it?

So far, not much. That's not a recent development, either. President Clinton cautioned a decade ago, in January 1999, that, "We must be ready—ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire, and health services—or military assets." A year later he proposed a series of measures to address the security problem.

Two years later, President George W. Bush created a special adviser on cybersecurity who spent a year developing a computer security strategy.

Neither effort made much headway. The public didn't see the problem. The network attacks that alarmed official Washington were classified. Officials couldn't talk about them.

Meanwhile, privacy and business interests worked overtime to persuade the public that National security concerns were overwrought. The real risk was Government monitoring and Government regulation, they insisted.

And that, by and large, was the view that prevailed—twice, and under two Presidents. Nothing was done about computer security that anyone in the privacy or business lobbies might object to.

In 2009, President Obama became the third President who promised to make computer security a top priority. Shortly after taking office, the Obama administration produced a security strategy. Once again, though, the strategy lacked punch. It failed to call for any action that could possibly irritate business or privacy groups.

Since then, the President has belatedly appointed an experienced security professional to the National Security Council. DHS has begun hiring a large number of security professionals, and it is rolling out the least controversial incarnations of the Government's intrusion detection system, called Einstein. But the administration has shown no sense of urgency in addressing the massive problems we face, especially in the private sector, where most of our critical infrastructure can be found.

That's why I'm pleased to be able to say that the Senate Homeland Security Committee has risen to the challenge. It recently offered a bipartisan and comprehensive bill that would address the problem in a responsible fashion. Senators Joe Lieberman (I–Connecticut), Susan Collins (R–Maine), and Tom Carper (D–Delaware) have introduced a bill that offers a real opportunity to improve the Nation's cybersecurity.

I'm going to set aside the "boxology" imposed by the act—a new White House Office for Cybersecurity Policy headed by a Senate-confirmed director, and a new free-standing security office (the NCCC) at DHS, which would include the existing U.S. Computer-Emergency Response Team (US–CERT) and would be responsible for detecting, preventing, analyzing, and warning of attacks. This office too would be headed by a political appointee who would be Senate-confirmed and would report directly to the Secretary of Homeland Security. If that were all the bill did, it would not add greatly to our security.

The real substance of the bill lies in the requirements it would impose on those critical infrastructures selected by the Secretary for coverage. ("'Critical infrastructure" is defined by statute as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters private sector.")

First, the NCCC would, in coordination with the private sector, identify cyber vulnerabilities in covered infrastructures, and submit the findings to Congress. After consulting with the private sector, the NCCC would then issue regulations creating "risk-based" security performance requirements for covered infrastructures. Owners and operators of the infrastructures would then select the specific security measures they will implement to satisfy the security performance requirement, and submit a compliance plan to the NCCC. Owners and operators would have the flexibility to implement any security measures that the Director determines would satisfy the security performance requirements. But, they would have to certify that they are in compliance, and would be subject to penalties if an audit by the NCCC determines that they are not. Those companies that meet the requirements would obtain some protection from liability, including immunity from punitive damages and limits on non-economic damages.

Second, critical infrastructure companies would be required to report to the NCCC "any incident affecting [their] information infrastructure . . . to the extent the incident might indicate an actual or potential cyber vulnerability, or exploitation of a cyber vulnerability." ("Information infrastructure" means the "underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices and communications networks and any associated hardware, software, or data.") This requirement would sweep far more broadly than the data breach notification rules that presently exist at the State level, since it would include "any incident" that indicates even a "potential cyber vulnerability." But information shared with the NCCC would be protected from public disclosure.

Third, the bill would authorize the President to declare a National cyber emergency, which would then trigger the issuance by the NCCC of specific emergency measures to protect the continuing operations of critical infrastructure. Those measures would expire after 30 days unless the President or NCCC Director extended them. The emergency measures would have to be the "least disruptive" means necessary, and could not be used to avoid the requirements of the rules for intercepting phone calls or emails for law enforcement or intelligence purposes. Owners of covered critical infrastructures would have to comply with the emergency measures unless the NCCC approved alternative measures suggested by the infrastructures. Those owners that comply would be immune from civil suit in some instances, or would be protected from punitive damages and damages for non-economic harm in others.

I have no doubt that this bill will prove controversial. Privacy groups will tell us that the Government can't be trusted with any authority over the computer networks on which we depend. Business groups will tell us that Government regulation will raise costs and stifle innovation. I have no doubt that the proposed legislation will need to be modified as it makes its way through Congress. But I strongly urge this committee to give it careful consideration.

Today, we have a new, and troubling, example of what can happen if Government fails to take responsibility early for avoiding a serious risk.

As I speak, oil has been escaping from BP's Deepwater Horizon spill for nearly 2 months. As the spill shows, private companies are quite capable of setting the stage for catastrophes well beyond their ability to remedy. We properly expect the Government to regulate companies to address risks that can't be internalized by the

companies taking the risks. And when disaster strikes despite those efforts, we expect the President to have the authority to respond. The Government is paying the price today for the actions it didn't take in the months and years before the blowout.

The same thing will be true, in spades, if another country launches a computer network attack on U.S. infrastructure. Do we want the Government to look as helpless in response to such an attack as it looks today in response to the BP spill?

Bad as the spill is, the country still has electric power, working phones, and a banking system. If we are attacked, we can't count on any of those things. But without something like the Senate bill, the President will be even more helpless to respond to the attack than he has been to respond to the oil spill.

Put simply, the country can't afford a disaster on that scale. And neither can its leaders.

Chairman THOMPSON. Thank you very much. I am not certain when the book signing will be, Mr. Baker, but I am sure we will hear from you. Thank you very much. Let me thank our witnesses for their testimony, and we will now start with our questioning. I will begin.

Mr. Schaffer, can you tell the committee your guesstimate of how many times our systems are hacked on a daily basis, if you know?

Mr. SCHAFFER. Sir, I couldn't give you an estimate of how many times our systems are hacked on a daily basis. I can tell you that our systems, like most of the internet, is under a constant barrage of attacks from a variety of known actors, ranging from basic criminals, sophisticated criminals to nation-state actors. So there is a wide range of attackers out there taking advantage of the vulnerabilities that are in the infrastructure. The Federal Government, like all others who leverage that infrastructure, are subject to attacks.

Chairman THOMPSON. To what extent are we able to deter those attacks?

Mr. SCHAFFER. I think that we are making progress towards deterring those attacks on a regular basis through the various programs like EINSTEIN and the Trusted Internet Connection, reduction of our connections to the open internet through deploying intrusion capabilities that allow us to have situational awareness and that give warnings of mitigation to the departments and agencies.

Chairman THOMPSON. Ten percent, 20 percent, 30 percent?

Mr. SCHAFFER. Sir, I wouldn't venture to guess the percentage because until you know the entire attack surface, it is hard to know what we are——

Chairman THOMPSON. So we don't know?

Mr. SCHAFFER. I would say we don't know the full extent of what is being blocked, no.

Chairman THOMPSON. Mr. Skinner, do you have any information on that?

Mr. SKINNER. No, Mr. Chairman, I do not. One of the things that we did identify doing our audit, there is big gaps out there. We are only monitoring through EINSTEIN those 21 agencies. Those that are not signed into, we cannot adequately monitor, so that there is no way to see what is going on with these others agencies.

Chairman THOMPSON. Thank you. Mr. Schaffer, since we monitor those 21, can you give us the statistics on those?

Mr. SCHAFFER. Sir, what we have deployed today—we are deployed to and operational at with the EINSTEIN 2 technology——

Chairman THOMPSON. Have we deployed EINSTEIN 2?

Mr. SCHAFFER. We have deployed EINSTEIN 2 to 11 of 19 agencies that it is currently planned for, yes.

Chairman THOMPSON. So we couldn't do it with EINSTEIN 1?

Mr. SCHAFFER. EINSTEIN 1 was a flow monitor. It allows us to see the traffic moving through and then we would do analysis on the traffic.

Chairman THOMPSON. Give me what EINSTEIN 2 has provided.

Mr. SCHAFFER. EINSTEIN 2 is showing us about 278,000 indications of potential malicious activity at the perimeter of our networks on a monthly basis today with the deployments that we have. That doesn't mean that all of those attacks were successful. It simply means that there is indications of malicious activity 278,000 times on the average month.

Chairman THOMPSON. Okay. In the event of a cyber attack to our system who is in charge?

Mr. SCHAFFER. Sir, in event of a cyber attack on our civilian networks, our Executive branch civilian networks, DHS has the lead to manage that response. The various departments and agencies, including the Department of Defense, the NSA, various others, would all be involved and engaged depending on what the nature of the attack looked like, where the attackers were focusing their energies and what was needed in order to execute on the response.

Chairman THOMPSON. So Mr. Wilshusen, can you provide any more information on the question of who is in charge based on your review?

Mr. WILSHUSEN. I think that is one of the challenges that needs to be addressed, is who is actually in charge. With the White House Cybersecurity Coordinator in place now, what is his role relative to those at DHS? I think that is certainly a valid challenge that still remains to be addressed.

Chairman THOMPSON. So is it we are not quite sure who is in charge or what? Mr. Wilshusen.

Mr. WILSHUSEN. I think that is the case, yes.

Chairman THOMPSON. Mr. Skinner, with respect to the overreliance on outside contractors to staff this operation, do you see that as a vulnerability for that Department?

Mr. SKINNER. I believe what we should be doing is in fact inherently governmental, we should be using our own employees. Right now that is the only alternative we have. It is better to have cleared contractors than to have no one. The contractors have been very, very useful in filling the gap until we can fill up our resources.

Chairman THOMPSON. Mr. Schaffer, at what point do you think, given the goodness of Congress to provide authority for significant staffing of your operation, that you can complete that mission?

Mr. SCHAFFER. Mr. Chairman, we have been staffing up within the National Cybersecurity Division significantly and in particular at US–CERT. At the start of fiscal year 2009 we had 16 people at US–CERT. At the start of 2010, we had 31. Today we have 55. We have another 25 in the pipeline going through security that have been offered jobs. So by the end of the year for US–CERT, we anticipate that we would have about 80 Federal staff in place.

Chairman THOMPSON. So by the end of the year you will have 80 people. How long did it take you to hire 80 people?

Mr. SCHAFFER. Again, the ramp-up has been fairly steep, sir. But we went from 16 at the start of fiscal year 2009 to hopefully 80 at the end of fiscal year 2010.

Chairman THOMPSON. So in 2 years you hope to hire 80 people?

Mr. SCHAFFER. Sir, the type of people that we need to hire, as mentioned by some of the gentlemen to my left, are not easily found. The skill sets that we are looking for are very specific and very high level of skill and capability in cybersecurity and they are sought after by every department and agency that is trying to implement their program, by the private sector players who are anxious to ensure that their systems are correctly defended. These are the type of people that we are looking for that are in very high demand and we are looking for the right ones in order to fulfill the mission.

Chairman THOMPSON. Thank you. I yield to the Ranking Member.

Mr. KING. Thank you, Mr. Chairman. This is sort of a follow-up to the Chairman's line of questioning.

Mr. Schaffer, if a sophisticated cyber attack were launched today or tomorrow against the financial systems, banks, New York Stock Exchange, who coordinates the Federal response and whose authorities are triggered?

Mr. SCHAFFER. Again, I think that it is clear that ultimately the White House is responsible for coordination and the coordinator, Howard Schmidt, has that ultimate responsibility. Within the interagency, there are lanes where different agencies would have responsibility, lead responsibility for the defense of the networks and for the dot-com space. With the financial services industry, I believe DHS has the lead. We are in the process of building out a National Cyber Incident Response Plan, and that plan will more clearly define the roles and responsibilities of the different departments and agencies, how DOD, DOJ, DHS and others will participate and play their various roles. That plan is being developed as an interagency process as well as in cooperation with the private sector entities that would have to play a large role because they own so much of the infrastructure and will have to provide so much of the support in a major incident.

Mr. KING. That doesn't make me confident, though, that if we were attacked tomorrow everyone would know how to respond. It seems like you are still trying to work your way through that.

Mr. SCHAFFER. We are certainly in the process of finalizing the National Cyber Incident Response Plan. Until that is finalized and moved through the interagency process, there will be some questions. But we are in the process of trying to get to clarity there.

Mr. KING. Does anyone else wish to comment on the immediacy of that threat as to what would happen if we were attacked tomorrow? Stewart.

Mr. BAKER. There is no doubt that we are not prepared to address a major cyber attack today. I don't want to overemphasize the importance of sorting out all of the lanes in the road because in a crisis the President will take charge, he will own this. It won't be Howard Schmidt, it will be the President who has to make sure that this problem is solved. I believe that rather than focusing too much on which box goes where or who has what authority, the im-

portant thing is to make sure that the resources are there, that there is bipartisan support for hiring people quickly to address these problems, and that we find much better ways to work with the private sector, which I think at this point has no clue who would be their contact point or what their responsibilities would be. That is something that I think the Senate bill does a good job of starting to address.

Mr. KING. Let me ask you that then, about the Lieberman-Collins bill. What are the greatest advantages offered by the legislation?

Mr. BAKER. I think first it responds to the need to deal with the fact that the risks are principally in the private sector and much of the infrastructure is in private sector hands, and yet a desire to avoid heavy-handed regulation by saying we are going to pick out the most critical infrastructure, we are going to impose performance requirements on the critical infrastructure and make sure they can meet certain standards any way they want and then requires a reporting of incidents that raise questions about whether the infrastructure will actually function and an ability in an emergency for the President to say this is what has to happen first, this is what has to happen second, and to make sure that the private sector responds. An authority that clearly when you look at things like financial meltdown or the BP oil spill, the President has to have and he doesn't really have in this area.

Mr. KING. In your testimony, Mr. Baker, you talk about the lack of a sense of urgency in addressing the massive problems with cybersecurity. How can we best address this lack of urgency? How do we get this out to the departments, to the people, to the society as a whole?

Mr. BAKER. Clearly the President needs to own this and to move forward with a number of the issues that really have been hanging fire since the beginning of the administration. I don't say that this President is alone in not having solved the problem. Two other Presidents have said this is a crisis, we need to address it, and have not fully addressed it. But he clearly needs to make it a priority for every part of Government to address this problem.

Congress can do the same by strengthening DHS's authorities. We need to make it clear to industry that this is our top priority because the next time we get into a serious international conflict, we could lose large parts of our cyber infrastructure to attackers.

Mr. KING. Thank you. I thought you were going to suggest that everybody read your book. But in any event, I yield back.

Thank you.

Chairman THOMPSON. The Chairman now recognizes the gentlelady from California, Ms. Lofgren for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman. Thanks for having this hearing. I think it is very important, and I hope that we will have other opportunities in addition to this one to review these matters. I was happy to read the IG's report and I think there is some useful suggestions in there. I was actually disappointed, I did not realize that US–CERT did not have automated correlation tools. That is something that ought to be remedied pretty promptly.

But I want to get into the capacity issue. There has been a discussion that the U.S. Government authority, DHS or OMB I guess

for that matter, ought to have more authority, and it seems to me without more capacity, we are not in a very good position to be asking for more authority.

I am not as troubled by the idea of having contractors on board provided that they are adequately directed and supervised for this reason. I see the kids walking over the line to graduate with their Ph.D.s in computer science at Stanford, and I don't know that we are going to succeed in getting those young people to apply for a Federal job, but we need them. We are going to have to pay them a lot of money, more than the GS scale provides. Even then we will be lucky to get some of them. So provided that we are using contractors to attract really people that are in that competitive league I would personally encourage that we do so and promptly. Not that those young people necessarily have the managerial skills that are necessary to organize the responses, but the technical skills cannot be replicated by someone who is 5 or 6 years out from the academic studies, in my opinion.

So you can comment if you want on that. I also wanted to comment on where we are vis-a-vis the critical infrastructure. I am mindful that it really has been many years since we have had somebody in the White House with expertise on cyber, and I was glad to see that the President appointed Howard Schmidt, who has a background, who is an old hand. But the thing is he can't do the operations. He is looking to the civilian sector I hope in DHS, which I think is better suited theoretically than OMB. What I do want is to have sufficient capacity in DHS so that we don't end with up the NSA running this program. Because if you look at the entire panoply of expertise that resides in the Federal Government, you would have to say they have probably the most to offer today in terms of just raw expertise.

So what is the strategy to get the talented people we need as soon as possible? Are we paying enough? I come from Silicon Valley. Hiring, it has woken up. All the big companies are hiring now. The economy is coming, so we are about to have an even more competitive job market. Now is the time to grab those young people.

Mr. SCHAFFER. Congresswoman, I think that there is no question that we are trying to execute expeditiously to hire as many people as we are authorized to have within the program. Indeed, we expect within NCSD, and I think you have to look at all of NCSD, not just US–CERT, to realize all of the programs and execute well, not just US–CERT with the situational awareness and the dissemination of information, but also the programs designed to go into the departments and agencies and make repairs, as well as the programs designed to get information out to the critical infrastructure players and assist them in dealing with incidents and being prepared for incidents. So in NCSD, the numbers there are significant as well. We went from 35 on staff in 2009 to 118 in—beginning of 2010 to about 193 today with 46——

Ms. LOFGREN. Could I ask you, since our time is limited? Could you follow up—you don't need to give me the names—but the individuals and kind of their profile, where did they get their Ph.D., what year did they get their Ph.D., just so I can have a sense of the personnel that has been selected?

Mr. SCHAFFER. We can certainly get that.

Ms. LOFGREN. I would appreciate that. I just want to say that I think we are so far behind where we need to be, really a decade of serious neglect honestly, that I am worried. It is not because of whether there will be cyber attacks. There are right now and there will be more.

I continue to be concerned not only about our lack of preparation internally within the Government, but the coordination between clinical infrastructure that is held for the most part outside the Federal Government, either by private sectors or in some cases non-Federal public sectors, in energy development, energy transmission, water storage, water movement, financial sectors and the like.

I don't think that they are as prepared—certainly the IT sector is all over this, but that doesn't mean that the non-IT sector has taken even minimally adequate steps. We have to do much more with those critical infrastructures sectors, and I don't think that we are really ready yet. I would like to see, Mr. Chairman, if in 6 months' time or 4 months' time we could have a better plan, maybe everyone in a workshop or closed session on where the benchmarks are, how we are getting there in terms of these major critical infrastructure sectors.

I know my time is up. I thank you for your indulgence, Mr. Chairman.

Chairman THOMPSON. Thank you very much. I look forward to making sure that information is provided. Also, Mr. Schaffer, staff met with you on June 9 and there was some information requested at that meeting that is yet to be provided. So we need to remind you to pick out where it is in the system and get it to them.

Mr. SCHAFFER. Mr. Chairman, I know that is underway.

Chairman THOMPSON. Thank you. The gentleman from Texas, Mr. McCaul, for 5 minutes.

Mr. MCCAUL. Thank you, Mr. Chairman. In my judgment, this is probably one of the most serious National security threats we have today. Because everything is tied to the networks. We know there have been massive intrusions into the Federal networks. We know that espionage is taking place. If foreign agents were to cull paper files leaving the Pentagon, it would be on the front page of the Washington Post, and yet I think that is happening in the virtual world and no one is talking about it. The cyber warfare capability is growing every day. There was a denial-of-service attack last 4th of July. Imagine a stronger denial-of-service attack that hit the United States and shut power grids and energy sectors.

We held hearings last Congress on this issue, then Chairman Langevin and I, and we asked a question of: Who is in charge? Nobody seemed to know the answer to that question. Since that time it is a little more, I think, clarified that DHS has a responsibility to defend the Nation from cyber attacks. We have tremendous offensive capability, but I am afraid our defensive capability is lacking. That is the weakness and sense of vulnerability. I think that is where we need to be strengthening our National asset, as the Chairman referred to. This is for—actually Mr. Schaffer and Mr. Skinner, the coordination with DHS and the other organizations. We have NSA, DOD that are very good at the offensive capability,

but they are not working with, in my view, adequately enough with DHS to better prepare and defend this Nation.

Can you comment on that?

Mr. SCHAFFER. Thank you, Congressman. Actually, our relationship and cooperation with NSA is fairly extensive and quite productive. They support our mission in a variety of ways with technical assistance on various programs. The EINSTEIN program in particular, where we are currently conducting an exercise on new EINSTEIN 3 intrusion prevention capabilities, is supported by assistance from NSA. We work with DOD on a variety of initiatives in order to execute well and leverage the information that they can bring to bear on the commercial side and for the civilian branch departments and agencies in the dot-gov space.

So our goal is to bring all of the resources of the Federal enterprise to the fight to defend the networks. I think the problem for all of us today is that defense loses in cyber too much of the time because the ecosystem was not designed and built from the beginning to be a good place to defend yourself. So offense has the advantage, and until we change that we will continue to have some challenges. But I think we are working very hard across the interagency and in cooperation with both the White House and our partners at DOD to try to bring all of the resources to the fight.

Mr. MCCAUL. That is good to hear. We worked with CSIS to issue a report to the President, recommendations that in terms of this coordination role that this be coordinated from the White House, had to be elevated to the White House level. A Cyber Coordinator position had to be created. That has been done. Howard Schmidt is the cyber coordinator. I am concerned that his requisite authorities are not strong enough to carry out that mission and that responsibility.

Mr. Skinner, I know in your report you talk about the White House responsibility for leading and oversee a National cybersecurity policy. Chairman Langevin and I introduced a bill to make this cyber coordinator position a Senate-confirmed position with an Office of Cyberspace in the requisite budget authority to give them the authorities necessary to carry out the coordination mission. Do you have any comments or thoughts on that?

Mr. SKINNER. We did not look at the authorities or the responsibilities of the White House per se. What we were focusing on is the authorities within US–CERT and how they can compel their partners, their stakeholders, and the Federal agencies to comply with or provide assurances that they are addressing or reacting to recommendations and guidance provided by DHS and that we just focused on that one particular issue.

Mr. MCCAUL. I just think that needs to be strengthened in my judgment.

Last set point, my time is running out. Private sector coordination. We have the Information Sharing Analysis Centers, the ISACs. Can you tell me, Mr. Schaffer, how that has improved, if it has?

Mr. SCHAFFER. The Department, of course, is leveraging the ISACs as well as all of the NIP structure, the 18 sectors and their sector coordinating councils to execute well in terms of getting information out to the private sector. I think with the MS–ISAC and

the IT–ISAC, the financial services ISAC, we have various projects on-going to expand our connectivity to those organizations. So for the financial sector, for example, you have an on-going pilot where we are using DOD information, DHS information, and the financial services industry information, bringing that together in a way that anonymizes the private sector data so that they are more willing to bring the information forward so that that can be shared among those organizations, operationally improving all of our security posture.

So we have got some projects, I think, that really do leverage those ISACs and take advantage of what they can bring to the fight.

Mr. MCCAUL. Thank you very much. I see my time has expired.

Chairman THOMPSON. Thank you. The gentleman from Missouri for 5 minutes, Mr. Cleaver.

Mr. CLEAVER. Thank you, Mr. Chairman. Yesterday our subcommittee of this committee dealt with the Office of Disability Integration and Coordination and I was concerned there that they had insufficient funding to do the job they were commissioned to do. I find myself today equally concerned about and frustrated over the fact that the GAO believes the staffing is not sufficient to fulfill this Herculean mission you have, Mr. Schaffer. If we have 98 positions authorized and we have only filled 38 of those positions, it means that we are fighting a cyberspace war with only half our troops. I would like to note what the problem is in filling all of the positions and doing so quickly.

Mr. SCHAFFER. Thank you, Congressman. I think that today we are at 55. So we have made some progress since when the report being referenced was issued. We have 25 more in the pipeline which will get us to about 80 by the end of the fiscal year. The challenge is in identifying the right people and getting them to accept positions and to come on board here with us to move things forward. Again, it is a space where there are a limited number of resources that really can fulfill the mission, go through the security clearance process, and be able to staff us the way we need to be staffed.

We augment those positions with contractors. Right now US–CERT is leveraging about 230 contract staff. The process of ramping up in this space is challenging and we are doing everything that we can to aggressively hire. We will reach our full complement within all of NCSD in terms of the authorized positions we think by the end of the year. So we are doing everything we can to be aggressive about getting the positions filled.

Mr. CLEAVER. That is refreshing to hear because if something should happen, we get beat up twice. We have the incident and then the pain of we weren't paying attention, we didn't have the sufficient staff to deal with the problem.

Let me skip down. I represent Kansas City, Missouri, and an area around it. Kansas City is the second-largest freight rail center in the Nation. As freight rail companies turn more to internet to control its signals and dispatching, it also means that they become more and more vulnerable to cyber threats.

Is there something being done with regard to the private sector in this battle that we find ourselves fighting? If so, what can we

do to enhance it? What can this committee do to enhance that relationship and coordination?

Mr. SCHAFFER. Yes, sir. That area is indeed one of our primary areas of focus at the Department. The control system, the industrial control system security is paramountly important because, as you point out, connectivity to the internet of those systems is increasing. So we have done several things. We stood up this year, last year the ICS, the Industrial Control System Computer Emergency Response Team. That team provides assistance to the private sector. We have trained 14,000 individuals in industrial control vulnerability and defense. We are putting out teams to do a vulnerability assessment and to assist the private sector in understanding what their particular system might be vulnerable to and how to implement mitigation strategies.

We have flyaway teams that are capable of going out during an incident to assist a private sector entity with a problem so that it doesn't involve a breakdown of the control systems, a power grid going out or water system failing and such.

We are working hard to put out best practices and information so that the private sector has the best thinking from the Government around how to defend these systems. We hope to get in front of the problem as more and more of these industrial controls are attached and leveraging the IP-based networks that the IT systems have long been attached to. So we see that as a primary area to focus attention on, and we are doing a lot to try to expand in that space.

Mr. CLEAVER. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. The Chairman now recognizes the gentleman from Texas, Mr. Smith, for 5 minutes.

Mr. SMITH. Thank you, Mr. Chairman. Mr. Wilshusen, first question to you, and that is I believe it was March 2009 when you made your recommendations to Department of Homeland Security. That is about 15 months ago. What percentage of your recommendations have been implemented to date?

Mr. WILSHUSEN. Are you referring to the National strategy?

Mr. SMITH. Yes.

Mr. WILSHUSEN. That is one thing we are still following up on in terms of the recommendations DHS is making some progress with——

Mr. SMITH. I know they are making some progress and I have heard today they have a ways to go. I am asking you though what percentage of that strategy have they actually implemented now, 15 months later?

Mr. WILSHUSEN. Well, of the National strategy, not all of the issues would actually pertain to DHS.

Mr. SMITH. Okay. Of the ones that pertain to DHS.

Mr. WILSHUSEN. That I would have to get back to you in terms of the very specific numbers on those.

Mr. SMITH. I am not asking for a specific number, I am just asking for a guesstimate.

Mr. WILSHUSEN. I would say at present it is probably about 30 to 40 percent.

Mr. SMITH. Thirty to 40 percent after 15 months? Okay. Thank you for that response.

Mr. Baker, how would you compare the private to the Federal Government as far as its ability to deter cyber attacks?

Mr. BAKER. Parts of the private sector are clearly well ahead of the Federal Government. Financial institutions have stronger systems in place. They have since for about 5 or 8 years been actively monitoring every packet that comes in and rejecting any packet that appears to be malware using very sophisticated signatures. We are barely at the point of getting about half of our institutions to monitor what is coming in, which only tells them that they have been screwed. It doesn't tell them that they are protected. So we have got—we are talking about installing systems that monitor the malware as it comes in. Prevention, actually rejecting them, is going to wait still for many agencies for months or years, and a lot of that is hung up in lawyers, you know, wringing their hands about whether they can really implement those programs.

Mr. SMITH. Private sector ahead. Thank you.

Let me address my next question to you, Mr. Skinner and Mr. Wilshusen and Mr. Baker, and it is this. All you have said in one way or another that the Federal Government, the administration has been slow in implementing or taking the necessary steps to protect the Federal Government against cyber attacks.

What are the consequences of this continued vulnerability to the country? Mr. Skinner.

Mr. SKINNER. If I may begin, it definitely puts us at risk. We have to understand why this was not a top priority within the Department. One, we were new, established in 2002, 2003.

Second, we had to establish priorities, and there was only so many resources that can go around. We focused, the Department focused its attention on border security and air security. As we matured in those areas, then we turned, the Department turned its attention to cybersecurity.

Unfortunately, the train has left the station. We are now chasing the problem as opposed to being ahead of the problem. We have a long way to go. But at least we recognize that we have a serious problem here, a serious threat here that needs to be controlled, and that is where we are headed right now.

Mr. SMITH. Thank you. Mr. Wilshusen.

Mr. WILSHUSEN. I think the risk is very significant to Federal systems as well as to critical infrastructure that is cyber-based. We have reported on a number of occasions on incidents that have occurred and the resulting effect of that which resulted in at some points personally identifiable information being disclosed to unauthorized individuals, to vast amounts of information related to various different security programs being exfiltrated out to their organizations and individuals. So the risk is very real and significant to the Federal Government.

Mr. SMITH. Thank you. Mr. Baker, I am going to go to my last question because I only have a short period of time left, but I do address it to all three of you all. Mr. Skinner and Mr. Wilshusen, you have just said that we are at risk. So my last question is this: What are the odds of the United States sustaining a debilitating cyber attack in the next year? I know, again, that forces to you guess, but are the odds great? Are they low? Give us some indica-

tion of how vulnerable we are and how much at risk we are. Mr. Skinner.

Mr. SKINNER. Congressman, I just wouldn't want to venture to because it would be a wild guess. But we are vulnerable. It could be significant.

Mr. SMITH. If you say we are vulnerable and at risk that is pretty significant, too. Mr. Wilshusen.

Mr. WILSHUSEN. Again, I couldn't hazard a guess as to the percentage. But it is more than what we should be and more than what Federal agencies should be able to protect their systems.

Mr. SMITH. Okay. Mr. Baker.

Mr. BAKER. If we end up in a serious conflict with five or 10 very sophisticated countries, we will be attacked and we will not know how to respond. So the real question is: Are we going to end up in a conflict like that? One of the things I worry about is that we will not defend our interests, the interest of our allies for fear of a cyber attack. That could happen at any time.

Mr. SMITH. Thank you very much. All very informative. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you. The Chairman now recognizes the gentlelady from California, Ms. Harman, for 5 minutes.

Ms. HARMAN. Thank you, Mr. Chairman. I want to express my solidarity with Mr. Skinner as a cyber immigrant. That may apply to many of us over a certain age, but I would observe that the number of students who have been wandering, or not wandering but walking in an orderly way in and out of this hearing probably have come to these issues more naturally than we have. But we are catching up. Let me observe that on behalf of the older class. We are catching up, and the business is urgent.

The visual image that we all have on our television sets is of a broken pipe, a mile under water spewing tens of thousands of gallons of oil and natural gas with no easy or immediate solution in sight. I would just analogize that to a major cyber attack where we could have a broken network or networks spewing tens of thousands of bits of information on critical infrastructure, National security and mission-critical data, financial and personal data, et cetera. It could be as devastating or more devastating than the environmental catastrophe that is unfolding on our TV sets.

Does anyone disagree with this? No. Right.

So as Mr. Baker said, "We are going to have a meltdown." I see this as urgent business. It is nice to talk about how we could reorganize things, but I think we need to try to catch the problem, not just chase the problem, as Mr. Skinner said we are presently doing.

This is not a criticism of you gentlemen, and it is not a criticism of the Members of the committee either. We have all been trying to get our arms around this. But we don't have our arms around this yet. Am I correct? Right. Okay.

So let me say a couple of things. First of all, I agree with Mr. King that the Lieberman-Collins bill is excellent, and he and I have been talking about this. I have also talked to the Chairman about it. I just want to tell Mr. King that I do plan to cosponsor the bill with him.

Mr. KING. Will the gentlelady yield for one second?

Ms. HARMAN. Sure.

Mr. KING. I will be the lead cosponsor on your bill.

Ms. HARMAN. Did I just hear him giving me some power over something?

Mr. KING. You are getting it.

Ms. HARMAN. My, my. Bipartisanship thrives in this institution. At any rate, thank you. But I think it is an excellent effort. I am sure it will change as it goes through the legislative process, but it will be a good thing to work with our counterparts in the Senate on this as we worked with our counterparts in the Senate on the SAFE Ports Act. Mr. Lungren remembers that. To good end. We ended up with a very good law.

At any rate, I think it will give the Government new powers and new focus and perhaps, I hope, provide the sustained leadership that Mr. Skinner said we urgently need.

But I also want to ask about something else. I don't think, as we have been discussing this this morning, and perhaps I missed a little bit of the conversation although I was trying to hear it, that we have adequately addressed the other side of this. We need to protect our systems. We need to get our arms around this problem and act aggressively. I believe that, and I will support efforts to do that.

But we also need to make sure that we don't overdo it, that we are considering the fact that as we protect our security, we also want to protect our liberty. I have often said that security and liberty are not a zero sum game. We either get more of both or less of both. In saying that, I borrow from Ben Franklin, who thought of this 230 years ago.

So that raises a question of something this administration has not acted on, and that is standing up the Privacy and Civil Liberties Oversight Board that was mandated in the 2004 intelligence reform law that has been on the books for 6 years. The last administration made some effort at this, but we have not yet seen any names proposed for the confirmable positions for this board, and I just want to ask you, in my last 45 seconds, any of you who would like to address this issue of civil liberties and the need for the Privacy and Civil Liberties Oversight Board.

Mr. SCHAFFER. I would certainly chime in to say that the Department of Homeland Security believes that civil rights and civil liberties is a critically important part of how we address the cybersecurity issue, and we try to build a program that is focused on that from the start rather than trying to bolt it on at the end. We have resources within my office and within the Department that focus on everything that we are doing in that space. We have published several privacy impact analysis statements. We certainly believe that that is a critical part of the puzzle, and we very much want to make sure that we are focused on it as we go forward.

Ms. HARMAN. Thank you. Any other comments?

Mr. SKINNER. I would just like to add that during the course of our review, we did validate, in fact, the Department is, takes very, very seriously the CR/CL, the civil rights/civil liberties, and the privacy of individuals as they build these systems.

Ms. HARMAN. Thank you, Mr. Skinner. Anyone else?

Mr. BAKER. I will simply add that some of that hand-wringing that I think the lawyers are doing about oh, can we really look at and reject packets that are coming in is based on the fear of pri-

vacy concerns. So at a minimum, we have to have a mechanism for having these privacy issues raised and resolved quickly and not let them hang up important action too long.

Ms. HARMAN. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. The Chairman now recognizes the gentleman from California, Mr. Lungren, for 5 minutes.

Mr. LUNGREN. Thank you very much, Mr. Chairman. Thank you for having this hearing. This is one of the most important issues we have facing us.

Cybersecurity is the last among the various categories of security that we are really dedicating ourselves to. That is not a criticism of this committee. It just is a fact. The urgency that we need in responding to all of the threats out there in this new terrorist world is missing, unfortunately, across this country, and no more than in this particular place.

Mr. Smith—excuse me—Mr. Baker, I have not bought your book, but I have read chapters because people should know they go to his website. I happened across it by accident, but once I saw those eyebrows I knew it was you, and fascinating and very informative and very, very effective.

One of the things I think we ought to make clear is when Mr. Schaffer talks about 278,000 attacks per month, that is not a static number. That number is going up. It is almost exponential if you talk to people in the outside world about what is happening everywhere in the cyber world. So people ought to understand, 278,000 a month sounds big. Wait till next month and wait till next year. It is not just the Government sector, it is the private sector, and it is happening every single day.

Maybe we need to find ways to explain it to the public a little easier. I was just sitting here listening to some of the phrases we use. We want to get in front of the problem. We want to ramp up in this space. We want to stand this up. I appreciate that is the way we talk back here. No one talks like that back home. We have got a big problem that we have to deal with. Right now people ought to know how serious it is.

Mr. Baker, when you talked about the example of what happened to the Dalai Lama, and that he had a sophisticated network with all the protections in it and the damage that was done by a single person as a part of that network who received an e-mail from what he thought was a trusted individual who had an attachment and he clicked on to that attachment and that invaded the whole system and eventually allowed somebody from the outside to capture the system.

Mr. BAKER. That is right.

Mr. LUNGREN. That is not unusual or idiosyncratic to that network, correct?

Mr. BAKER. Oh, we are all subject to this.

Mr. LUNGREN. Let me ask you this. With respect to that particular attack, what success has there been in attributing those attacks to its origins, do you know?

Mr. BAKER. The people who did the study, some of them announced that they believed that it was the Chinese Government.

Others refused to make that conclusion but presented evidence that suggested that the Chinese Government was behind it.

Mr. LUNGREN. But it is not an easy thing to see the origin.

Mr. BAKER. It is almost impossible.

Mr. LUNGREN. That is what people have to understand. You might be able to see the attack, but once you find the attack and even deal with the attack, sometimes it is difficult to find out who did it and they move on to another potential attack.

Look, we could always have more money and have more people. I mean, everybody who comes before us says that. I understand that. I just want to ask the four of you, with the money we have now, with the authority that exists now, with the personnel that exists now under the authority given to you by this Congress, given to the Executive branch by this Congress, can we do a better job? Can we do a significantly better job? Or is the answer always going to be we could do a better job if we had more money and we had more personnel? In other words, are we doing the best we can with those we have? I don't mean this as a criticism of this administration. I have lauded this administration for giving real leadership to this area. But I am just asking current status.

Mr. WILSHUSEN. No, sir, we are not doing as best as we can to secure our systems. On our engagements we consistently find that security has not been effectively implemented on devices. It is not due to not having the particular tool or the capability. It is just the controls are available, it is a matter of configuring specific devices to be more secure than what they presently are.

Mr. LUNGREN. Getting people to use them, right?

Mr. WILSHUSEN. Getting them to use them and implement the security so——

Mr. LUNGREN. We just started with passwords in this Congress about 6 months ago. I have had more static from Members on the fact that the password has to be entered within 30 minutes. I have had Members ask for 12 hours, 24 hours. If Members can't understand, and what I would like perhaps Mr. Baker and Mr. Schaffer to talk about is, some Members say to me, well, look. No one's interested in the information I have here. I don't have secure information on here.

What are the potential for someone being able to latch on to one of these machines and be able to access it with Members who don't have classified information on the instrument?

Mr. BAKER. I would say first, you are going to take that machine and plug it into the entire network in order to download and sync up your e-mail. So you are, whatever happens to your machine will happen to the entire network.

Second, we all have things that we would just as soon not see in the newspaper. If you hand over those secrets to someone who is hostile to the United States and they are in a position to at some point either embarrass someone who is opposed to them, or help somebody that has done them a favor, or to blackmail them with a secret, that is a disaster for U.S. networks.

Mr. LUNGREN. What about an analogy to what happened to the Dalai Lama? They were able to listen to his negotiating position.

Members of Congress might have information that can be heard over this just talking about what they understand the negotiating

position of the administration to be, what they have heard from a witness, or what they believe the position of the administration ought to be.

Mr. BAKER. You are carrying around something that, if compromised, will tell whoever has compromised it where you are every second of the day and will allow them to turn it on and listen to you while you are talking to people and you won't even necessarily know that is happening.

Mr. LUNGREN. That is not just with our system in the House of Representatives. This is virtually all systems that are out there.

Mr. BAKER. There are security holes in virtually every one of them.

Mr. LUNGREN. Would you agree, Mr. Schaffer?

Mr. SCHAFFER. I would. I guess I would also say that it is not just about what is on an individual device because that device, if compromised, can be used as an attack vector against other devices. So if we all size our risk management to what we have on the device, we will not get enough security for the society as a whole. That is one of the challenges that we have in this space.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I just wanted people to understand the nature of this crisis as it directly affects everybody here. If it affects us in this way, it affects the Executive branch and it affects the private sector, financial services, every industry out there.

Thank you very much, Mr. Chairman.

Chairman THOMPSON. Thank you. The Chairman now recognizes the gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. I thank the witnesses for appearing today. Your testimony has been quite revealing and, to a very limited extent, somewhat frightening. You are probably as old as I am, and I suspect you are familiar with the movie, the sci-fi movie, "The Day the Earth Stood Still." It seems that we may be heading toward a scenario similar to that, perhaps not that same one, unless we act expeditiously.

The ability to intrude brings along with it the ability to manipulate. Intrusion can be very harmful, but manipulation can be deadly. We have got to thwart the ability to manipulate not only information, but also manipulate machines, as we have identified the phone earlier, but devices, trains, planes, and to a certain extent, automobiles because of the way the technology is advancing with the automotive industry.

So the first question I have for you is, is this more a question of will or is it more a question of way in terms of getting to the ultimate solution? If we had 100 percent of the will necessary to do this, can we find the way to thwart intrusion, given that the technology for intrusion metamorphoses on a daily basis? So help me, please, Mr. Baker. Is this more a question of will or way?

Mr. BAKER. Let me say I think your observation that intrusion can lead to manipulation is a critical one. This is a two-fer for foreign governments. First they spy on us using our systems, and then when we go to war they take down the systems when we need them. So it is a very serious problem.

I do think that this is more a matter of will than way, that we can solve some of these problems. We are going to need to take ac-

tion to make sure that we can actually respond to attacks and attribute the attacks to the people who are making those efforts. That means probably architectural changes in our approach to the internet. We need to be able to track back and find the people who actually launched that attack. That is going to require substantial changes in our architecture, but we can do it. If we do that we can deter a lot of these attacks.

Mr. GREEN. Would anyone else care to respond?

Mr. WILSHUSEN. I would agree that certainly will is a key part of it because the capabilities to protect many of the systems and networks that we have are available. But at the same time, I think you are right on. In terms of the manipulation and integrity of data it is critical. We often talk about the disclosure of information and how that can be very harmful. But if you are able to manipulate data it can have even more devastating impact to agencies and to military during conflicts, so I think you are right on track with that line of questioning. I do agree that it is probably more will than way. But way also has an aspect, too, because technology tends to outpace security.

Mr. GREEN. Anyone else?

Mr. SCHAFFER. I would echo that thought that there is a big will portion, but there is a way portion as well. The technology that we have today, the way that we are constructed enterprise-wide for the internet, has some challenges that will have to be addressed and fixed. If you look at the studies that have been done about applying known security technologies, they usually say that that would cover 80 percent of the intrusion sets. There is some percent that we don't have current technology to eliminate and we have got to focus some research and development efforts in those spaces in order to get to that last percentage.

Mr. GREEN. Well, my time is nearly up, so I will just conclude with thank you again for sharing with us. My hope is that we will take to heart what you have called to our attention and make the necessary changes so that we will have both will and way and thwart these efforts. I yield back.

Chairman THOMPSON. Thank you very much. The Chairman now recognizes the gentleman from Pennsylvania, Mr. Dent, for 5 minutes.

Mr. DENT. Thank you, Mr. Chairman. Good morning.

Mr. Baker, I would like to talk about the issues of fragmentation and you know, how do we really address the fragmentation in Federal agencies. Specifically, you know, how is the Federal Government's overall cybersecurity effort affected by the ability of the diverse number of agencies and departments such as the FTC, the SEC, and others to issue directives and rulings that establish cyber standards.

Mr. BAKER. I think there is a serious fragmentation problem both in terms of authority of DHS and the CERT over Executive branch agencies. In the private sector we long ago would have unified a number of the security measures and networks that different agencies have. But I also believe that both the FTC and the FCC have slightly distorted people's security priorities. The FTC has made it extraordinarily painful to allow anybody's Social Security number ever to escape your system. Now that is a serious problem, but it

is nowhere near as serious as some of the other attacks that people are not prioritizing today because they are focused principally on the privacy regulations that the FTC administers.

Mr. DENT. My follow-up question deals with, do we need to address the authority of the White House Coordinator for DHS?

Mr. BAKER. To my mind, no. At the end of the day, the coordinator speaks for the President and he reflects the President's priorities. If he makes it clear that he expects people to respond quickly to the coordinator's requirements, it will happen. So I am not convinced that large changes in his authority are essential.

Mr. DENT. Okay. In the Ghostnet case study that you discussed in your testimony, you portray an astonishingly intrusive intelligence operation that was carried out against the Dalai Lama through a cyber attack to the point that the hackers had knowledge of every on-line activity carried out by the attacked parties. What success has there been in attributing those attacks to its origins?

Mr. BAKER. There is no absolute attribution that has been made. There was a lot of evidence that suggested that the people who were carrying out that attack were also looking for intelligence from a number of other targets that would be highly of interest to the Chinese Government. But there was no absolute determination of who was responsible for that attack.

Mr. DENT. Thank you. To Mr. Wilshusen, GAO has noted several deficiencies for securing Federal information infrastructure, such as inadequate testing, certification, and accreditation of systems, failure to enter interagency agreements. As an overall trend, are the Federal Government's cybersecurity efforts improving? What do you think is the greatest obstacle towards realizing stronger security?

Mr. WILSHUSEN. I think to answer your first question first in terms of what are some of the challenges or obstacles, one is just the complexity and dynamic nature of the Federal computing environment. It is geographically dispersed, in many cases technologically diverse. As well as there is a large number and evolving threat, vulnerabilities and business practices that all impact the ability to secure information on Federal systems. There are a number of initiatives underway that are intended to help improve the security over those systems. The other Members, or the other witnesses have talked about some of those, particular, Einstein; another one is the Federal Desktop Core Configuration Initiative, as well as the Comprehensive National Cyber Security Initiative. We reviewed each of those initiatives and found challenges with each of those particular initiatives in terms of being able to effectively implement security and made some recommendations on that. But there are efforts under way. There is progress being made, but again, it is a major obstacle to overcome.

Mr. DENT. Mr. Schaffer and Mr. Skinner have an observation on that question?

Mr. SKINNER. Yes. I do believe it begins with the basics. It begins with the employees. I think we have to have a very robust oversight program. We have to have a robust accountability program. That is, if you are not complying, then you need to be held accountable. It begins at the lowest levels, not at the highest levels. I think it is something we have to continually hammer home to all employ-

ees that you, as an individual, have been given certain rights. You have certain responsibilities that go with those rights and that we will provide you the oversight to ensure that you are helping us help the Government secure its systems.

Mr. SCHAFFER. I would certainly say that the scope of the problem and the complexity of the networks and the different levels of capability within the departments and agencies to execute is one of the challenges that we will all face as we move forward in this space. At the Department we have been increasing our capability both in terms of people, resources, and otherwise to work with the departments and agencies to improve security across a range of programs that have been mentioned before.

FISMA changes are coming that will allow us to focus on not a paper exercise but real operational continuous monitoring kind of solutions to know where we are within the departments and agencies, but the departments and agencies themselves need to have the resources in order to execute on the advice and recommendations and remediation steps that DHS can try to put forward. But they have got to be able to execute within their own network environments. As mentioned, very diverse.

Mr. DENT. I see my time has expired and I would just like to, Mr. Chairman, extend my support to the cybersecurity initiative of Senators Lieberman and Collins. I think the Chairman, Ranking Member rather, and Representative Harman have also expressed similar support, and Mr. Lungren too. Thank you.

Chairman THOMPSON. Thank you. The Chairman now recognizes the gentlelady from New York, Ms. Clarke, for 5 minutes.

Ms. CLARKE. Thank you very much, Mr. Chairman. The Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology have done a great deal in this space over the past year and a half. We have coordinated many hearings, roundtable discussions, and briefings on this topic, and I want to thank you, Mr. Chairman, and the Ranking Member, Mr. King, for holding this full committee cybersecurity hearing today. It is good to see Assistant Secretary Schaffer, who has been instrumental in providing guidance to me and the other Members during our many roundtable discussions and briefings on the Hill, and I want to thank you, Assistant Secretary, and the other Members of the panel for joining us today.

I know this hearing is more focused on domestic affairs and efforts, but as we all know, cyberspace has no borders and no boundaries. I would like to add another dimension to our discussion this morning. Our ability to protect U.S. networks is inextricably linked to our ability to coordinate with our international partners on cybersecurity. There is a growing awareness of the problem of international cyber attacks, although the pace of the development is slower and irregular.

This March I introduced H.R. 4962, the International Cyber Crime Reporting and Cooperation Act, which would enhance America's cooperation with other countries to combat cyber crime and keep America safe. Chairman Thompson, Ranking Member King, Ms. Loretta Sanchez of California, and Ms. Laura Richardson of California are among the bipartisan cosponsors that also serve on

this committee. Senators Gillibrand and Hatch are the lead Senate sponsors of the bill on the Senate side.

Recent foreign-based attacks on the computer systems of U.S. Federal agencies and commercial companies highlight the vulnerability of the interconnectedness of the networks that comprise the internet, as well as the need to adequately address the global security and governance of cyberspace. Federal law and policy give a number of Federal entities responsibilities for representing U.S. cyberspace interests abroad in collaboration with the private sector.

More recently, the President appointed a National Cybersecurity Coordinator charged with improving the Nation's cybersecurity leadership. The Chairman, Ranking Member, and I requested a forthcoming GAO study to identify, among other things, challenges to effective U.S. involvement in global cyberspace security and governance efforts.

I wanted to take this opportunity to highlight this issue, so I will begin my line of questioning on this issue. Mr. Wilshusen, what obstacles remain between the United States and our international allies on the subject of global cybersecurity information sharing, and what can the United States do to overcome those obstacles?

To Mr. Schaffer, what is DHS doing to foster international coordination and information sharing on cybersecurity?

Mr. WILSHUSEN. Well, I guess I will start. Thank you. Well, one of the obstacles is just making sure that we have a coherent, cogent strategy for dealing with the international parties and making sure that the various different parties involved with the Federal Government have their roles identified and that they are working collaboratively with the international bodies.

It is also important that as we look at various different aspects related to international security arrangements, it deals with just some of the issues related to, for example, at securities incidents attribution and being able to identify perpetrators of such attacks across borders, particularly making sure we have the arrangements in place with other nations in order to foster and promote active investigations of those incidents. So making sure that those arrangements in place are going to be very important, too.

Mr. SCHAFFER. Congresswoman, the Department of Homeland Security is definitely focused on international as being a critical part of what we need to do in order to be successful. As you point out, it is impossible to protect our networks without having the assistance of our international partners.

I traveled to Spain not too long ago for an EU ministerial with the Secretary, where cyber is one of the topics that we discussed with the European Union. We are working extensively with members of the international watch and warning network, 15 nations that are engaged with us on incident response level work for cyber and who will be participating with us in the Cyber Storm III exercise so that we can look at how our CERT capabilities can leverage and be working with our international partners during an incident.

We also participate in the Meridian Conference. We hosted last year a group of international visitors focused on cybersecurity, particularly in the nature of industrial control spaces, and we do lots of bilateral meetings on the international realm as well to try to address cybersecurity issues.

As you know, there is not a consistent base of capability in all of the countries who are our partners and we are trying to provide assistance where we can and to learn lessons from those who are more sophisticated that may have done some things that we haven't done yet. So we are working hard to work with our international partners to make progress.

Ms. CLARKE. Thank you very much, gentlemen. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you. The Chairman now recognizes the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. I, too, add my appreciation to the full committee Chairman and Ranking Member for holding this hearing and to the witnesses as well. I want to be probative on maybe some of the same questions that have been asked but maybe all have not asked them, and to try and probe as to where we are. So I would like to focus my attention on Mr. Skinner; just make this comment that we rushed to establish Department of Homeland Security in the wake of 9/11. Just as a moment of history, we started with a select committee in this House, and then we developed the structure as the Senate did for the Department and merging a number of different distinct disciplines in one big, if you will, umbrella, under one big umbrella, and we rushed to do it.

So my question to you, Mr. Skinner, is: What did we do wrong at the very beginning as it relates to cybersecurity and the priority that was given when the Department was established, just on your historical perspective?

Mr. SKINNER. Those were very emotional times and I think when we brought the Department together back in 2003, 2002–2003 time frame, I believe the attention was on protecting our air security and protecting our borders to ensure that we did not have a physical attack, a repeat. Cybersecurity, while everyone recognized that was an issue to be dealt with, I don't think just elevated at that point in time in our psyche as something that we needed to address immediately. Time has passed. Over time we are now learning that we cannot ignore cybersecurity. The technology is moving so fast and our reliance and dependability on that technology has become increasing daily and we are beginning to realize that if we want to protect our borders, we have to protect our cybersecurity. That is so important. I think it is something that we are starting to recognize and we are starting to do. We have come a long way with regards to our border security.

Ms. JACKSON LEE. So in essence, the start of our focus was air security. This traveled, when we speak of the Government, this traveled through the Bush administration. This was no different in terms of the issue of staffing and focus. This sort of is an on-going problem. Is that my understanding?

Mr. SKINNER. That is correct, yes.

Ms. JACKSON LEE. So we now have a moment in history where the technology has risen to a level of ultimate superiority and it is at a crisis point at which you believe there may be some action.

So let me just focus in something that is very troubling to me, and that is the question of DHS not being able to enforce the other agencies to protect their systems.

Tell me, in a very quick answer, what that means. What are you saying?

Mr. SKINNER. That means, essentially they do not have statutory authority to compel their stakeholders, the other Federal agencies that they make recommendations to and provide guidance to, to compel them to respond to or correct problems that are being identified.

Ms. JACKSON LEE. Which means that it leaves us vulnerable in certain important areas. For example, and I am just calling these agencies' names, not pointing them out. But we have got the Department of Justice, we have got the CIA, we have got NASA, we have got agencies that hold proprietary information, Department of Transportation, that would be vulnerable if they were not responding.

Let me ask the Secretary: What do you do now with respect to trying to get our Federal agencies to enforce and protect their cyber systems?

Mr. SCHAFFER. The process today when we identify a vulnerability or we see information coming over the Einstein system that suggests that an attack has been focused on a particular department or agency is to provide the information about the attack, to provide mitigation strategies, to work with the department or agency on methodologies and best practices to avoid the attacks in the future. But as Mr. Skinner points out, we do not currently have the authority to require the department or agency——

Ms. JACKSON LEE. But what specific authority do you need? I know legislation is moving. But what specific authority do you need?

Mr. SCHAFFER. The administration at this point is looking at the bill that has been discussed at length here. It has not established a position yet on that bill or what specific authorities may be necessary. We are continuing to work with the departments and agencies to execute well against the threats and vulnerabilities that we identify through the systems that we have. We are seeing good cooperation from a lot of the departments and agencies to make progress. But at this point we don't have an administration position that I can give you on specific authorities that we need.

Ms. JACKSON LEE. Well, I would encourage you to continue to work with this committee. I think we are at a crisis point where that position needs to be established. I think as we leave this hearing we can confirm that agencies are not listening or not responding to the lack of an authority that you have to enforce them protecting the most important assets that the American people have, and that is for proprietary information. So I look forward to you really getting back with this committee since the administration has made great strides and it needs to complete the task.

I yield back.

Chairman THOMPSON. Thank you. The Chairman now recognizes the gentlelady from California for 5 minutes, Ms. Richardson.

Ms. RICHARDSON. Thank you, Mr. Chairman. If you know anything about my district, you know that it is very infrastructure rich. In fact, when Secretary Napolitano had an opportunity to come to my district, she was shocked at the ports, the bridges, the water treatment facilities, surf plants, just on and on.

So I would like to start off my first question having to do with the National critical infrastructure. I have been a little disappointed that the last Secretary that we have had and the current one has not been a supporter of really true cargo inspection. I personally believe that that is going to be something that we will have to deal with. One of the things we are currently doing is we are relying upon, we do screening in terms of looking at the data, but we are not actually inspecting the cargo. So I would like to get your thoughts on what you think in terms of our potential vulnerabilities of really relying upon data and information, assuming that so and so, who we have never had a problem with, is sending such and such, which they say is cargo in there is A-okay, which is really we are relying upon data and not facts. I just wanted to get your thoughts.

Mr. SKINNER. Congresswoman, this is something that we are currently looking at. It does make us, if we do not have adequate verification, validation programs, and internal controls to ensure that these certifications that we are obtaining and that we can trust these people, yes, that makes us very, very vulnerable, and that is something that we are studying as I sit here today and hopefully to have a report out within the next year.

Ms. RICHARDSON. If you could keep this committee abreast of your progress and hopefully, before next year, but keep us abreast on our progress. Thank you, sir.

The second question I actually wanted to ask you, Mr. Skinner, the enforcement authority for Federal cyber security policy results with the OMB. With no disrespect to our other colleagues here, do you support this position, this line?

Mr. SKINNER. I can't comment. I am really not in a position to comment on that at this point in time. I will be happy to get back to you. I have to learn more about what their enforcement authorities are.

Ms. RICHARDSON. Okay. Then to you, Mr. Schaffer, in addition to being on Homeland Security, I am on Transportation and Infrastructure. One of the biggest new things that we are hoping will be here soon is NextGen. I wanted to get your thoughts that NextGen is the program, really the air traffic controllers' new system that will enable us to have more, better information and what we do, but again it makes us very vulnerable if someone were to take over the NextGen system and suddenly having planes going in all the wrong directions and such a reliance upon data which is moving away from pilots. I wanted to get your thoughts. Have you started looking at the potential cyber issues there? Cybersecurity issues?

Mr. SCHAFFER. Congresswoman, I would have to get back to you on the specific details. I do think that we are engaged with a group that is working on that program, but I don't know the details off the top of my head in terms of what our engagement has been.

I would just say that, as a practical matter, there are many systems that are looking to leverage new technology, and they all need to have security as a critical part of the development of the system rather than an add-on after the fact. So to the extent that we can bring a security mentality to the development of new technologies that are coming into the Federal Government, we will be in a much

better position in the future to have a more secure infrastructure than if we don't do that and then have to try to bolt security solutions on after the fact.

So I certainly would encourage thinking about those security issues at the early stages of the process. We will get back to you with exactly what our involvement has been thus far.

Ms. RICHARDSON. With no discouragement to the company that is actually designing it, what will you be doing to ensure that just because the company says, like what we are living through right now with the spill in the Gulf, what will you be doing to ensure that there is, in fact, true security and protection versus just a company telling you so?

Mr. SCHAFFER. Again, I will have to get back in terms of what our role in that process will actually be, but we will certainly get that information to you.

Ms. RICHARDSON. Okay. Then finally I would just like to follow up on something that Representative Jackson Lee said. One thing I am learning from watching the results of the oil spill is, you didn't say that there was any additional authority that you thought you needed or could share with us at this time. What I would say is that I am learning it is we better know in advance. So rather than us waiting and then all of sudden we have to decide whether we really have authority to do some things, if things don't go right we need to be prepared to step up and we need to give you the authority to do so.

Thank you very much. I yield back.

Chairman THOMPSON. Thank you very much. I have a couple of questions I would like to ask before we close this hearing.

Mr. Skinner, your report mentions the fact that a number of agencies said that they have not received sufficient training on the Einstein system, and that for some reason Homeland isn't sharing this data with them. Are you aware of that?

Mr. SKINNER. I know what you are referring to. As far as training, yes, there were some of these stakeholders that felt that the training could have been more intense or face-to-face and they thought that presented a problem to them. As far as information sharing is concerned, there are those agencies that said that they would like to have more information with regards to reported breaches as they come through. The problem with that, and I am sure the Assistant Secretary Schaffer can address this better than I, is that this is a lot of raw data. A lot of it is false leads. Many of the agencies that are asking for this may not have the capability to analyze it themselves, and we can inundate them with unnecessary information that could really not help their cause but slow their cause down.

Chairman THOMPSON. Okay. So what is the fix for that?

Mr. SKINNER. What we are suggesting is the Department explore with other agencies what can we share. Who is capable of handling this information. Who has the clearances, who has the security clearances that allow them to look at this data. That is the other thing. A couple of these agencies did not have security clearances, and yet they wanted to look at classified documentation.

So I think, No. 1, we have to sit down with our partners and explore what can be shared and educate our partners as to why certain things can't be shared and why you don't want it to be shared.

Chairman THOMPSON. Mr. Assistant Secretary.

Mr. SCHAFFER. Mr. Chairman, we definitely have a plan to expand our ability to provide information to our Government customers as we go forward, and that includes building portals that will allow them to get access to certain kinds of information that we can provide that wouldn't violate the classification rules obviously. We also have plans to put in place resources, human resources that will be able to be dedicated to individual departments and agencies so that they will have a single resource that they can reach out to and ask questions of at any time and get the answers that they need in order to execute well.

But Mr. Skinner is quite right that the volume of data is definitely an issue in terms of raw data that needs to be processed. As everyone has noted, the need to have highly skilled and capable individuals who can analyze that data and turn it into information that is executable is one of the challenges for US–CERT, and one of the things that we are doing better all the time. But to expect each department and agency to be able to do that independently as well is probably a big lift, and that is one of the challenges here.

Chairman THOMPSON. Well, I guess not independently, but at some point you should be able to move something that is of importance to that agency.

Mr. SCHAFFER. Yes, sir. We do that today. We share the information. Once we have processed and we have got real information as opposed to raw data, we are pushing that information to the departments and agencies so that they have actionable things that they can go execute against. It is access to the raw data that we find probably wouldn't be useful to them because of the volume and because of the need to do all of this extensive analysis.

Chairman THOMPSON. Back to a question Ms. Richardson and Ms. Jackson Lee talked about relative to OMB and their enforcement of US–CERT requirements. Mr. Baker, since you might be one of two people who can answer that question on the panel without any—take a shot at that. I mean, what do you think the problem with that approach is?

Mr. BAKER. The difficulty with telling other agencies what they have to do in this area is you are basically telling them to spend money that they were planning to spend on something else on computer security, which isn't going to make their lives any easier at all. So they are just—it feels like they are taking a budget cut. Therefore, you need OMB's support before you can do that. Either OMB is going to say we can find money for you to do that or they are going to say I am sorry, you are just going to have to take the cut. So without OMB being part of this process it isn't actually going to work. My suggestion would be that it may be that DHS needs bigger negotiating tools in this area, but we are never going to get OMB out of this process and we shouldn't be trying. That would be my suggestion.

Chairman THOMPSON. Mr. Wilshusen.

Mr. WILSHUSEN. Well, certainly OMB does have that role with the budget and approving budgets for agencies. It also is respon-

sible under the current law, FISMA, for approving and/or reviewing and approving or disapproving agencies' information security programs. So they have that authority now to go through and review agencies' security programs and approve them.

Has it been doing it? Not really. It is something we have commented on in the past about their ability to actually review and approve agencies' security programs. Basically that is happening now through the FISMA reporting process. We have commented in the past that the measures and security metrics that OMB has established for agencies to report under that process have really not been sufficient to really gauge the effectiveness of agency and security programs. Those measures generally just address compliance issues and how many systems have been tested and evaluated, how many individuals have been given training, for example, without really addressing how effective those security protections and measures are.

So OMB certainly has a role and has had a role in trying to assure that agencies have adequate information security programs. But it has not really done that to the extent that it probably should have done in the past.

Chairman THOMPSON. Mr. Assistant Secretary.

Mr. SCHAFFER. Mr. Chairman, I will just point out that OMB has recently issued a letter that gives to DHS some of the responsibilities with respect to executing on some of those reporting pieces. So we are going to be moving in a direction that gets away from what is a paper-based compliance, once-a-year process to a much more operationally focused, continuous monitoring kind of solution. We will have interviews with the departments and agencies to make sure we understand what they are actually executing on. We will have benchmarking capabilities that will let us see what other departments and agencies are doing and show the individual departments what they have got, and we will have continuous reporting out of the actual management systems that are used by the departments and agencies to look at their own systems flowing into the FISMA reporting tool.

So I think we are moving in a direction that will address some of those challenges that we have had historically.

Chairman THOMPSON. With respect to the authority to enforce compliance, are you of the opinion that you need that authority?

Mr. SCHAFFER. Mr. Chairman, as I said, I apologize that I am not in a position to answer a question on what authorities we might need at this point. The Department and administration are working through the process of coming up with our answer to the authorities question and when we can do that I am sure it will be provided.

Chairman THOMPSON. I am certain. Mr. Skinner.

Mr. SKINNER. Yes. We do believe they need that authority. What we haven't defined and I think what needs to be worked out is: How do we exercise that authority and how do you compel compliance?

Chairman THOMPSON. Mr. Wilshusen.

Mr. WILSHUSEN. One of the issues under FISMA has been even within a particular agency, not even looking at across the Federal Government, is that FISMA required and gave authorities to the

agencies' individual CIOs. Even in FISMA it just said that CIOs and their certified information security officers, I'm sorry, are responsible for ensuring compliance but did not include enforcing compliance. That one word even made a difference within agencies, particularly larger departments that may have multiple components. In some instance, for example, like VA, a number of years ago, the central chief information security officer really did not have that much authority to compel or enforce compliance with policy issues across the Department. So the enforcement is really a key consideration in this particular respect.

Chairman THOMPSON. Mr. Baker.

Mr. BAKER. Of course they need that authority. It is an unnatural act for another department to take binding guidance from another department and until Congress makes it clear and the President makes it clear that, by God, they are going to have to do it, they are not going to do it.

Chairman THOMPSON. Three out of four in agreement is not bad. I understand, Mr. Assistant Secretary, believe me, but I have to ask the question. I thank the committee. You have been absolutely excellent with your responses to the questions of the committee at this point, and I want to thank you for your testimony.

Before concluding, I would like to remind our witnesses that the Members of the committee may have additional questions for you and we will ask that you respond expeditiously in writing to those questions. There have been some requests of certain witnesses here today. Hearing no further business, the committee stands adjourned.

[Whereupon, at 12:00 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON OF MISSISSIPPI FOR GREG SCHAFFER

Question 1a. The IG report states that US–CERT does not have sufficient staff to meet its mission. Although US–CERT's authorized positions were increased from 38 in 2008 to 98 in 2010, as of January 2010, only 45 positions are filled.

Would you give us an update on how many of the 98 authorized positions for fiscal year 2010 have been filled?

Answer. Of the 98 authorized positions, the United States Computer Emergency Readiness Team (US–CERT) currently has 56 full-time positions filled and 22 positions with selections in the on-boarding pipeline. It is important to note that the 98 positions is the target for the end of the fiscal year—in fiscal 2009, we tripled the number of cybersecurity personnel within NPPD, and we are doubling that number again this fiscal year. The snapshot staffing number in the IG report was already outdated by the time it was released; our numbers will continue to increase as we continue to grow.

Question 1b. What is the reason for the slow process in addressing US–CERT's staffing needs?

Answer. There are inherent challenges with rapidly on-boarding and recruiting technical experts; chief among the reasons is the need for high-level clearances, skills required, and competition for higher-paying jobs in the private sector. However, hiring is the National Protection and Programs Directorate's (NPPD's) No. 1 management priority. We have more personnel in the hiring process for NPPD than ever before. Internally, NPPD has been working closely to streamline the overall hiring process, and within the National Cyber Security Division (NCSD), overall Federal employees have increased from 43 at the end of fiscal year 2008 to 198 current Federal employees.

Question 1c. Of the personnel increase from 38 to 98, how many can be attributed to the Secretary's Balanced Workforce Strategy to convert contractors to authorized FTEs?

Answer. NCSD has focused recruitment efforts for these positions on hiring the best and brightest from a large and diverse pool of candidates. NCSD has, therefore, looked to a variety of sources to fill Government positions. Approximately 20 percent of the individuals hired to fill converted positions previously held the positions as contractors.

Question 2a. The IG reported that due to the staffing shortage at US–CERT, contractors are used to augment the staff.

How many contractor personnel currently work on US–CERT program activities?

Answer. Currently, the National Cyber Security Division (NCSD)/United States Computer Emergency Readiness Team (US–CERT) has 185 contractors supporting US–CERT program activities, 86 of which are currently on-site.

Question 2b. How many contractor positions are slated for conversion to Government positions as part of the Secretary's Balanced Workforce Strategy in fiscal year 2011?

Answer. NCSD is currently assessing staffing requirements beyond the number of personnel authorized in the President's fiscal year 2011 budget request to address staffing shortages.

Question 2c. How many additional positions did the administration request for fiscal year 2011 to properly address the critical staffing shortage at US–CERT's?

Answer. With the projected fiscal year 2011 budget approval, NCSD requested a total of 42 new positions of which 22 are to support US–CERT.

Question 2d. Who are the contractors tasked to support US–CERT?

Answer. Currently, Booz Allen Hamilton (BAH), General Dynamics (GD), MITRE, ESP Group LLC, and CMU Software Engineering Institute (SEI) support US–CERT through existing contracts.

Question 2e. What type of support do these contractors provide? Can these support activities be in-sourced?

Answer. The contractors provide a wide variety of support including: Program management, financial management, and performance management; 24/7/365 integration and reporting (meaning there is someone operationally staffed every hour of every day of the year); and operations support services (such as incident handling, continuity of operations, malicious code analysis, contingency planning, and trend tracking, etc.).

US–CERT also receives contract support to assess and recommend improvements to applications, tools, and business processes related to identification, analysis, and publication of timely information about critical cyber threats; vulnerability analysis support; technical mentoring and conference support; acquisition planning; incident investigations; and identification of emerging technologies.

NCSD believes that a balanced approach to staffing, which includes a mix of contractors and Federal employees, is the most effective method for resource allocation. We are aggressively growing our Federal workforce, and looking closely at how best and most appropriately to augment our expanding team with contract support. As such, NCSD is developing a needs assessment to ensure the right ratio of contractors to Federal employees is hired in the out years.

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON OF MISSISSIPPI FOR GREG SCHAFFER

Question 1. What are the technical analyst's responsibilities?

Answer. Responsibilities include testing and implementing latest tools and technologies to improve the capabilities of the Einstein Program, performing administrative oversight to ensure that the Einstein program complies with applicable laws, and creating and testing new signature profiles to track and detect potential threats against the Federal civilian Government network infrastructure. Other responsibilities include:

- Examining raw data from a wide variety of information sources (e.g. malware and digital media) to detect potential attacks and vulnerabilities and recommend mitigation strategies on potential attacks and vulnerabilities detected. Technical analysts also perform a thorough technical analysis of data to understand the nature of the attacks, threats, and vulnerabilities.
- Providing temporary on-site incident response assistance to investigate, respond, and analyze suspicious activities at departments/agencies.
- Preparing various reports to summarize the initial findings and detailed analysis of the malware or incidents that contains mitigation strategies to improve situational awareness.
- Providing malware guidance to incident handling operations staff as necessary.
- Providing peer review for quality assurance of dynamic and static analysis activities.

Question 2. What specifically are these additional duties?

Answer. As of January 2010, US–CERT has filled only 45 of its authorized 98 positions. Additional duties for some GS–9 technical analysts include acting in a management capacity, instead of examining and analyzing network traffic for suspicious activities and coordinating cyber defense with other agencies. Other duties include developing standard operating procedures, providing on-the-job training to new staff, and mentoring junior staff and obtaining systems access to perform their job functions. However, we believe the mentoring and on-the-job training should be provided by managers or supervisors, not technical analysts.

Question 3. Would you consider these duties inherently Governmental?

Answer. Staff supervision such as providing mentoring to junior staff is considered inherently Governmental. However, the functions should be performed by supervisors. The technical analyst's responsibilities listed below may be performed by contractors:

- Examining raw data to detect potential attacks and vulnerabilities and recommend mitigation strategies on potential attacks and vulnerabilities detected.
- Performing thorough analysis of data to understand the nature of the attacks, threats, and vulnerabilities.
- Providing temporary on-site incident response assistance to investigate, respond, and analyze suspicious activities at departments/agencies.
- Preparing various reports to summarize the initial findings and detailed analysis of the malware or incidents that contains mitigation strategies to improve situational awareness.
- Providing malware guidance to incident handling operations staff as necessary.

- Providing peer review for quality assurance of dynamic and static analysis activities.

Question 4. Should new positions be created to perform these duties?

Answer. More resources can always help US–CERT to perform its mission. However, the technical analysts are performing these duties because US–CERT cannot fill its authorized positions. Creating additional positions will not mitigate US–CERT's inability to hire and retain qualified staff. US–CERT's staffing shortage is primarily caused by leadership turnovers and the Department's rigorous suitability clearance process.

For example, US–CERT has had four directors in the past 5 years. Further, due to the Department's rigorous suitability clearance process, it takes US–CERT a significant amount of time to fill its critical positions. According to a former director, it takes 9 to 12 months for new applicants to begin working at US–CERT even if they already have a top secret clearance. As a result, staffing shortages force current analysts to perform additional duties, instead of fulfilling the technical analyst role for which they were hired.