CYBERSECURITY: A REVIEW OF PUBLIC AND PRIVATE EFFORTS TO SECURE OUR NATION'S INTERNET INFRASTRUCTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 23, 2007

Serial No. 110–59

Printed for the use of the Committee on Oversight and Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

43–198 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

TOM LANTOS, California
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY MCCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho
JIM JORDAN, Ohio

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
DAVID MARIN, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

WM. LACY CLAY, Missouri, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
JOHN A. YARMUTH, Kentucky
PAUL W. HODES, New Hampshire

MICHAEL R. TURNER, Ohio
CHRIS CANNON, Utah
BILL SALI, Idaho

TONY HAYWOOD, *Staff Director*

CONTENTS

CYBERSECURITY: A REVIEW OF PUBLIC AND PRIVATE EFFORTS TO SECURE OUR NATION'S INTERNET INFRASTRUCTURE

TUESDAY, OCTOBER 23, 2007

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:06 a.m. in room 2154, Rayburn House Office Building, Hon. Wm. Lacy Clay (chairman of the committee) presiding.

Present: Representatives Clay, Hodes, Yarmuth, and Turner.

Staff present: Darryl Piggee, staff director/counsel; Jean Gosa, clerk; Adam C. Bordes, professional staff member; Nidia Salazar, staff assistant; Michelle Mitchell, legislative assistant, Office of Wm. Lacy Clay; Charles Phillips, minority counsel; Patrick Lyden, minority parliamentarian & member services coordinator; and Benjamin Chance, minority clerk.

Mr. CLAY. The subcommittee on Information Policy, Census, and National Archives will now come to order. Today's hearing will examine how well DHS is fulfilling its role as the leading Federal agency charged with coordinating response and recovery efforts in the event of a major Internet disruption. In addition, we will review the roles and responsibilities of private sector stakeholders in the development of Internet recovery plans and hear their recommendations for improving our current cyber security policy framework.

Without objection the Chair and ranking minority member will have 5 minutes to make opening statements followed by opening statements not to exceed 3 minutes by any other Member who seeks recognition. And without objection Members and witnesses may have 5 legislative days to submit a written statement or extraneous materials for the record.

I will begin with an opening statement and then recognize the ranking member. Then we will adjourn after that while we vote and then we will come back and take the testimony. Just be patient with us, please.

Securing our Nation's economic and global interests relies upon having a resilient Internet infrastructure. A recently released study by the Business Roundtable summarized that there is a probability of between 10 percent and 20 percent for a major Internet breakdown over the next decade. At an estimated global cost of approxi-

mately $250 billion, an event of this magnitude would prove devastating to our domestic industries and international trading partners.

Despite spending millions of dollars, the Department of Homeland Security has failed to develop an effective Internet recovery plan to rely upon for emergency response and recovery efforts.

Furthermore, their lack of adequate progress in developing appropriate models for measuring the levels of risk facing each sector has left policymakers unable to determine which sectors are most vulnerable to major cyber network disruptions.

It is my hope that today's witnesses will provide an update on DHS' efforts to remedy its deficiencies and provide recommendations for strengthening partnerships that will best secure our Internet infrastructure.

That concludes my opening statement and I will recognize Mr. Turner of Ohio for his opening statement. Mr. Turner.

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

Opening Statement of Rep. Wm. Lacy Clay (D-MO), Chairman
Subcommittee on Information Policy, Census, and National Archives
House Committee on Oversight and Government Reform
Hearing on Internet Recovery Efforts

October 23, 2007

GOOD AFTERNOON. TODAY WE WILL EXAMINE THE ROLES OF PUBLIC AND PRIVATE SECTOR STAKEHOLDERS IN DEVELOPING EFFECTIVE INTERNET RECOVERY PLANS. SECURING OUR NATION'S ECONOMIC AND GLOBAL INTERESTS RELY UPON HAVING A RESILIENT INTERNET INFRASTRUCTURE.

A RECENTLY RELEASED STUDY BY THE BUSINESS ROUNDTABLE SUMMARIZED THAT THERE IS A PROBABILITY OF BETWEEN 10% AND 20% FOR A MAJOR INTERNET BREAKDOWN OVER THE NEXT DECADE. AT AN ESTIMATED GLOBAL COST OF APPROXIMATELY $250 BILLION, AN EVENT OF THIS MAGNITUTE WOULD PROVE

DEVASTATING TO OUR DOMESTIC INDUSTRIES AND INTERNATIONAL TRADING PARTNERS.

DESPITE SPENDING MILLIONS OF DOLLARS, THE DEPARTMENT OF HOMELAND SECURITY HAS FAILED TO DEVELOP AN EFFECTIVE INTERNET RECOVERY PLAN TO RELY UPON FOR EMERGENCY RESPONSE AND RECOVERY EFFORTS.

FURTHERMORE, THEIR LACK OF ADEQUATE PROGRESS IN DEVELOPING APPROPRIATE MODELS FOR MEASURING THE LEVELS OF RISK FACING EACH SECTOR HAS LEFT POLICY MAKERS UNABLE TO DETERMINING WHICH SECTORS ARE MOST VULNERABLE TO MAJOR CYBER NETWORK DISRUPTIONS.

IT IS MY HOPE THAT TODAY'S WITNESSES WILL PROVIDE AN UPDATE

ON DHS'S EFFORTS TO REMEDY ITS DEFICIENCIES AND PROVIDE RECOMMENDATIONS FOR STRENGTHENING PARTNERSHIPS THAT WILL BEST SECURE OUR INTERNET INFRASTRUCTURE.

Mr. TURNER. Thank you, Chairman Clay. I want to thank you for holding today's hearing on Cyber Security: A Review of Public and Private Efforts to Secure Our Nation's Internet Infrastructure.

The Internet is a key critical infrastructure asset and has an enormous impact on communications as well as the economy. It is important that this asset is protected, much like other critical infrastructure assets. It seems, however, that due to a number of factors, the Internet isn't as secure from catastrophic events as it could be.

I look forward to reading the testimony from today's witnesses on how DHS can better prepare our Internet infrastructure from potential catastrophic events, such as national disasters and terrorist attacks.

I am interested in how DHS plans to address the concerns listed in the 2006 GAO report on DHS' efforts to coordinate an Internet infrastructure recovery plan. And I am particularly interested in learning about the legal barriers that DHS faces in providing assistance to private sector entities which own or operate Internet infrastructure in the event of disaster.

Mr. Chairman, I want to thank you again for your leadership and your effectiveness in the oversight of the important Federal policy issues of information policy. Thank you.

Mr. CLAY. Thank you, Mr. Turner. And at this time, the subcommittee will recess and reconvene at the conclusion of the three votes that we will take now on the floor. The committee stands in recess.

[Recess.]

Mr. CLAY. If there are no additional opening statements, the subcommittee will now reconvene and we will receive testimony from the witnesses before us today.

I want to start by introducing our first panel, which will consist of Mr. Greg Garcia, who is the Assistant Secretary for Cyber security and Communications at the Department of Homeland Security. In his position, Mr. Garcia oversees the operations and strategic planning activities of the National Cyber Security Division, the Office of Emergency Communications and the National Communications System. Prior to joining DHS, he represented the information technology on Capitol Hill, and before that served as a staff member of the House Science Committee.

We also have joining us Mr. Greg Wilshusen, who is a Director of Information Security Issues at GAO. He is a long time expert on the topic of information security and has testified before this panel numerous times on cyber security issues and Federal information security management practices.

And to round out the panel, Mr. Dan Ross serves as the chief information officer for the State of Missouri. And prior to his appointment in 2005, Mr. Ross served under then Secretary of State Matt Blount in the capacity of executive deputy secretary of State. He holds a bachelor's degree in industrial relations from Lincoln University and a master's degree in public administration from the University of Missouri.

Welcome, Mr. Ross. We know you came further than others. And also welcome to the other two witnesses. And thank you all for appearing before today's subcommittee.

And it is the policy of the Committee on Oversight and Government Reform to swear in all witnesses before they testify. And I would like to ask you all to stand and raise your right hands.

[Witnesses sworn.]

Mr. CLAY. Thank you. You may be seated. Let the record reflect that the witnesses answered in the affirmative.

Mr. Hodes, did you have an opening statement that you would like to offer?

Mr. HODES. No, I will defer.

Mr. CLAY. OK. Thank you so much. I ask that each of the witnesses now give a brief summary of their testimony and to keep the summary under 5 minutes. Your complete written statement will be included in the hearing.

Mr. Garcia, we will begin with you. Before you do that, I know that you come today to explain how seriously DHS and the administration takes its cyber security responsibility. I must admit that it is a little disappointing that you waited until 11:30 this morning to deliver your written testimony for members of the subcommittee to adequately prepare.

With that said, you have 5 minutes to summarize your statement.

STATEMENTS OF GREGORY T. GARCIA, ASSISTANT SECRETARY FOR CYBER SECURITY AND COMMUNICATIONS, DEPARTMENT OF HOMELAND SECURITY; GREGORY C. WILSHUSEN, DIRECTOR OF INFORMATION SECURITY ISSUES, GAO; AND DANIEL S. ROSS, CHIEF INFORMATION OFFICER, STATE OF MISSOURI

STATEMENT OF GREGORY T. GARCIA

Mr. GARCIA. Thank you, Mr. Chairman, and members of the subcommittee. I appreciate the opportunity to discuss the Department of Homeland Security's efforts to promote the resilience of America's Internet infrastructure.

Let me just say at the outset, Mr. Chairman, that I do apologize for the lateness of our testimony. It is more than a little disappointing to me, as well. It in no way reflects the seriousness with which DHS takes the mission of cyber security. And it is very much important for you, the members of the committee and the staff to have the benefit of advance reading of our testimony so that we can have an informed discussion. So, please accept my apology for that.

We are endeavoring, in our process at DHS and interagency, to ensure that we bring testimony up to the Congress in a timely fashion.

Mr. CLAY. Thank you for that.

Mr. GARCIA. Sir, it is fitting that you are holding this hearing during National Cyber Security Awareness Month. It helps to raise public consciousness about the importance of Internet security to our economy and to our way of life.

Over 200 million Americans use the Internet at home and in the workplace. The Internet facilitates communications, and supports Government and business operations. Although the Internet has yielded tremendous efficiencies, organizations and individuals remain vulnerable to disruptions in service and loss of sensitive data.

Both the private sector and Government play a role in securing our Internet infrastructure. The private sector builds, owns and operates most of the cyber infrastructure and ensures the availability and functionality of the Internet. The Federal Government has the responsibility for ensuring the continued operation of essential Government functions, securing their timely restoration if they fail, and minimizing the impact to the Nation.

As such, it is incumbent upon the Federal Government to help protect against Internet disruptions and to ensure a coordinated response to incidents. I would like today to highlight a few of our efforts in these areas.

First, we are strengthening our ability to prevent Internet disruptions. Under the National Infrastructure Protection Plan [NIPP], the availability of the Internet and its associated services is identified as a shared key resource of the information technology and communications sectors. As the sector's specific agency for both, we work with the sectors to develop their Sector-Specific Plans [SSP], which were released in May of this year.

The IT SSP defines six critical functions that support the sector's ability to produce and provide resilient products and services. Of these, two critical sector functions relate directly to the Internet.

Similarly, the communications Sector Specific Plan identifies critical architectural elements of the Internet. Through implementation of their SSPs, the IT and communications sectors are continuing to work together to assess the risk to the Internet.

Although the availability of the Internet is primarily the responsibility of the IT and communications sectors, all sectors rely on the Internet. And DHS, together with the Partnership for Critical Infrastructure Security [PCIS], established the Cross Sector Cyber Security Working Group [CSCSWG], comprised now of more than 90 Government and private sector experts from across the critical infrastructure sectors.

This group provides a forum to assess, among other things, how critical sector operations could be impacted by disruptions and to develop appropriate mitigation strategies.

Improving situational awareness is a critical component of preparedness. The U.S. Computer Emergency Readiness Team [U.S. CERT], within my organization, coordinates with the private sector and Government entities to increase situational awareness of network conditions.

We developed a program called Einstein that provides Federal agencies with early cyber incident detection so that they can respond more rapidly to mitigate threats. It has slashed the time it takes us to gather and share critical data on IT security risks from days, as it used to be, to hours.

The U.S. CERT also engages with private sector Information Sharing And Analysis Centers [ISACs], to share information on cyber threats, vulnerabilities and incidents. This includes collaboration with the IT-ISAC and the Multi-State ISAC to raise the level of cyber security readiness in each State.

Our ability to protect against and prepare for Internet disruptions is further enhanced through exercises. We are currently planning for the Cyber Storm II Exercise in March 2008, which will in-

clude a focus on Internet disruption and recovery and involve Federal, State, local, international and private sector entities.

Second, we are enhancing public and private collaboration to ensure effective response capabilities. The National Response Framework [NRF], which was recently released for public comment, articulates how our Nation will respond to all hazard disasters. My office has responsibility for Emergency Support Function No. II [ESF–2], the Communications Annex and the Cyber Incident Annex. We undertook an in-depth review of these components, and incorporated updates to them.

In support of the NRF, the National Cyber Response Coordination Group [NCRCG], serves as the primary Federal interagency mechanism for coordinating Cyber Incidents. Recently, the NCRCG addressed the denial of service attack against the government of Estonia. The NCRCG co-chairs convened to discuss the situation and determined that an operational response was indeed needed. And we coordinated that through the National Coordination Center and U.S. CERT.

To sum, my office is now implementing a plan to co-locate the U.S. CERT and the NCC, the IT and Communications to further facilitate collaboration among IT and communications experts. We are working side-by-side with them to make it easier to obtain situational awareness, to identify threats and coordinate response activities.

To conclude, both Government and the private sector are taking proactive measures to address Internet resilience, and to prepare for and respond to Internet disruptions. Government and business leaders must continue to ensure that sectors, organizations and individuals all understand their dependence on the Internet, the impact that a disruption could have and actions that can be taken to mitigate the consequences.

Sir, thank you for your time today. I appreciate the opportunity to discuss this issue and will be happy to answer questions.

[The prepared statement of Mr. Garcia follows:]

Statement for the Record
Gregory Garcia
Assistant Secretary for Cybersecurity and Communications
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on
Information Policy, Census, and National Archives
October 23, 2007

Good morning Mr. Chairman and Members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss the role of the Department of Homeland Security (DHS) and our efforts both within government and with the private sector to ensure the security and resilience of the cyber infrastructure, as well as Government's role in responding to significant incidents that may disrupt the functioning of the Internet.

Protecting the Nation's critical infrastructure and key resources (CI/KR) is among DHS' highest priorities. The Nation's CI/KR sectors rely on the availability and resilience of the Information Technology (IT) and Communications Sectors. We recognize that IT and communications play a central role in the command, control, and operations of government; the economy; and other critical infrastructures. The IT industry produces the hardware, software, and services that create the foundation of networks and systems. The communications industry provides the necessary infrastructure, technology, and services that enable the transmission of information essential for the successful execution of any organization's mission.

DHS recognizes the significance of the convergence of IT and communications through the Internet. In response, DHS created the Office of Cybersecurity and Communications (CS&C) within the Department, bringing together the National Cyber Security Division (NCSD), the National Communications System (NCS), and, more recently, the Office of Emergency Communications, under unifying leadership. NCSD and NCS work collaboratively with the IT and Communications Sectors and maintain both strategic and operational programs that seek to address the challenges associated with preventing and responding to a disruption of the Internet.

As the Assistant Secretary for Cybersecurity and Communications within DHS' National Protection and Programs Directorate, I oversee our mission to prepare for and respond to incidents that could degrade or overwhelm the operation of our Nation's IT and communications infrastructure. CS&C's strategic goals include preparing for and deterring catastrophic incidents by achieving a collaborative risk management and deterrence capability through a mature partnership between Government and the private sector. This strategic goal also encompasses tactical efforts to secure and protect the Nation's cyber infrastructure from attacks and disasters by identifying and mitigating threats, vulnerabilities, and consequences. CS&C's efforts have resulted in successful and timely responses to cyber incidents, the development of technological solutions to enhance our response and communications capabilities during incidents, and trusted

relationships and partnership mechanisms that facilitate preparedness and operational response activities.

Securing our Nation's Cyber Infrastructure

Multiple entities play a role in ensuring the security of our Nation's cyber infrastructure and in responding to significant incidents that threaten the functioning of the Internet. State and local governments are often owners and operators of network infrastructure. The private sector builds, owns, and operates most of the cyber infrastructure. The Federal Government has the responsibility of ensuring that government functions continue to operate, securing their timely restoration if they fail, and limiting any impact to national security, the economy, public health and safety and public confidence. Because so many organizations have significant roles in the protection of cyberspace, the key to success is strategic partnering.

Even though the private sector bears most of the responsibility for protecting the cyber infrastructure it owns, CS&C takes an active role in protecting and increasing the resilience of our Nation's cyber infrastructure. By building interagency and public-private partnerships for infrastructure protection and by facilitating efforts to raise cyber security awareness, identify cyber research and development requirements, exchange information, and manage cyber risk, CS&C has made significant advances in improving the security posture of our Nation's cyber infrastructure.

For example, through our Einstein program we have reduced the time it takes to gather and share critical data on cyber threats and attacks facing Federal networks. We can now obtain and share information in a matter of hours rather than days. Einstein is currently deployed in 13 Federal agencies, and CS&C is actively working to obtain memoranda of understanding with other agencies for its further deployment.

CS&C has provided resources to meet the training, education, and certification needs of IT security professionals, including development of an IT Security Essential Body of Knowledge, which was recently released for public comment through the Federal Register. Our efforts have also resulted in training nearly 7,000 IT and control systems professionals in the last year on a range of topics related to vulnerabilities, risk assessments, and standards-based mitigation measures. Working with our public and private sector partners, we have also developed common procurement language that owners and operators can incorporate into contracts to ensure the cyber security of the products and services they acquire. The long term goal is to raise the level of security through the application of robust procurement requirements. Our efforts have received very positive feedback from users, and our documents have averaged more than 450 downloads per month.

Preventing and Preparing for an Internet Disruption

We have also taken steps to minimize the impact of incidents with the potential to disrupt the functioning of the Internet. For example, we are developing a Priority Telecommunications Service (PTS) for operation in the next generation network (NGN) that will provide our Nation's leadership with the capability to communicate during network disruptions. CS&C's outreach

efforts for cyber security have had real-world outcomes: over one million people have signed up for our National Cyber Alert System and are receiving alerts, bulletins, and other information on cyber threats, vulnerabilities, and incidents, further enhancing our ability to prepare for and respond to Internet disruptions.

Further, our operational response centers, the United States Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center (NCC) for Telecommunications provide the detection, warning, and response capabilities necessary to coordinate public and private sector response to Internet disruptions in the U.S. and around the world. These entities gather information, identify sources of attacks, and share information with the private sector, Federal, State, and local government entities, and our international partners to take actions to neutralize attacks and to mitigate the consequences from attacks.

These operations centers demonstrate the value of the Federal role in response to an attack on the Internet. For example, in July 2007 the country of Estonia came under a national cyber attack from botnets, an automated computer program, that were flooding the country's IT systems with traffic, causing a denial of service for many of their government sites. The Estonian government contacted the U.S. Government as a North Atlantic Treaty Organisation (NATO) member for incident response assistance. US-CERT coordinated with its Federal, international, and private sector partners to identify over 2,500 unique sources of the attacking botnets originating from 21 NATO countries. US-CERT contacted U.S. Internet security providers and major telecommunications carriers to share information regarding U.S.-based Internet Protocol (IP) addresses involved in the attack. In addition, US-CERT provided NATO countries involved in the incident with information to assist military, intelligence, law enforcement, and computer emergency response team personnel responding to the incident in their respective countries.

The Estonia attack is one of many—from October 1, 2006, through August 31, 2007, US-CERT handled over 34,700 incidents, an 88 percent increase since US-CERT first began tracking incidents in 2005. This can be attributed to not only the increased attacks on the Nation's public and private networks but also increased situational awareness levels and reporter rates.

It is incumbent on the Federal Government to enable the development of mechanisms to ensure coordination and operational information sharing across various stakeholder communities and to facilitate appropriate preparedness activities in advance of a disruption, as well as the appropriate response activities should a disruption occur. Coordination and collaboration rely on meaningful and trusted partnerships, as well as on mechanisms and procedures tested across government and with industry. I will highlight in my testimony efforts to partner with the private sector and undertake activities to protect against Internet disruptions and to build and sustain capabilities to ensure a coordinated incident response.

Collaborative Efforts to Secure Cyberspace

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of CI/KR protection into a single national program so that investment across sectors is applied where it offers the most benefit for mitigating risk. Under the NIPP framework, the availability of the Internet and its associated services are identified as a shared key resource of

the IT and Communications Sectors, reflecting the convergence of voice and data communications networks and services.

Homeland Security Presidential Directive 7 designates DHS as the Sector Specific Agency (SSA) for both the Communications and IT Sectors. DHS has identified two of CS&C's components—NCS and NCSD—as the organizations to carry out the SSA responsibility for the Communications and IT Sectors, respectively. NCSD is also responsible for addressing the cyber element across all of the sectors. In May 2007, both the IT and Communications Sectors recently released their Sector Specific Plans (SSP), which are planning documents developed jointly by industry and government through the respective IT and Communications Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC). The SSPs focus on overall sector preparedness, including managing risk to the sectors' critical functions and infrastructures that support homeland, economic, and national security.

Public and private security partners worked together to define six critical sector functions in the IT SSP that support the sector's ability to produce and provide high assurance products, services, and practices that are resilient to threats and rapidly recovered. Of the six functions, two critical sector functions are related to the Internet: 1) Provide Internet-Based Content, Information, and Communications Services and 2) Provide Internet Routing, Access, and Connection Services. The IT SSP presents an approach for assessing risk to those functions, as well as the other four critical IT Sector functions.

Similarly, the Communications SSP addresses the identification of architectural elements of the Internet and the incorporation of specific components into the sector's national risk assessment process. Both plans include similar actions to facilitate additional IT and Communications sector collaboration to assess risk to the Internet. The two sectors are currently participating in each other's SSP implementation activities, including the respective risk assessment working groups. This collaboration provides an opportunity to assess both strategic and operational risks to the Internet and develop and implement short- and long-term protective measures as well as research and development requirements necessary to prevent a major Internet disruption.

Although the availability of the Internet and its associated services is the responsibility of the IT and Communications Sectors, all CI/KR sectors rely on the Internet. Sectors must assess their dependence on the IT and Communications Sectors and the Internet. To assist in this process and to provide a forum for addressing cross-sector cyber security perspectives, DHS and the Partnership for Critical Infrastructure Security established the Cross Sector Cyber Security Working Group (CSCSWG). The CSCSWG brings together government and private sector cyber security experts together to collaboratively address systemic cyber risk across the CI/KR sectors. As one of several focus areas, the working group will analyze cyber dependencies and interdependencies to assess how the 17 CI/KR sectors depend upon IT and Communications Sectors. Through an understanding of each sector's dependence on the IT and Communications Sectors, sectors can assess how critical business operations could be impacted by disruptions or degradation of services and develop appropriate mitigation strategies.

While the public-private collaboration achieved through the IT and Communications SCCs, GCCs, and Information Sharing and Analysis Centers (ISAC), and the CSCSWG have enabled

DHS to address Internet resilience in conjunction with larger critical infrastructure protection efforts, internal efforts have also been brought to bear on the issue of preventing and preparing for Internet disruption. CS&C established the Internet Disruption Working Group (IDWG) to address the resilience and recovery of Internet functions in the event of a major cyber incident. The IDWG, co-chaired by NCSD and NCS, engaged with public and private sector and academic and international Internet security experts to examine risks and improve preparedness and situational awareness, identified measures that public and private entities can take to protect against nationally significant Internet disruptions, and worked to confront the security challenge presented by a growing reliance on IP-based communications by promoting Internet resilience. The IDWG activities resulted in recommendations and findings that CS&C has integrated into IT and Communications sector efforts.

Because a major Internet disruption could potentially occur not only from a cyber attack or major disaster but also from a sudden and substantial increase in usage, CS&C evaluated a scenario based on increased telework-related usage during a pandemic outbreak. The study focused on the viability of the telecommuting strategy, which has been identified as a key component of the national response to a pandemic influenza and on the need to identify necessary preparations should an outbreak occur. Telecommuting is increasingly relied on as an alternative method of conducting business. However, CS&C's study found that, based on the existing Internet infrastructure, the technical feasibility of widespread telecommuting has not been established. Furthermore, a surge in telecommuting traffic could cause significant congestion. Although it is believed that the network backbones would tolerate a surge usage from telecommuting and would experience minimal congestion, residential Internet access networks and enterprise networks are likely congestion points of concern with regard to the telecommuting strategy.

The pandemic study was conducted in coordination with subject matter experts in government and industry in the fields of communications, IT, cyber security, epidemiology, business continuity, financial services, and emergency response and relied on NCS' Network Design and Analysis Capability (NDAC). The NDAC, comprised of modeling and analysis tools, communications datasets and subject matter experts, supports the analysis and assessment of both data and voice networks. The NDAC has proven extremely valuable in assisting the NCS in understanding the vulnerabilities of the communications networks. As traditional circuit-switched communications networks transition to packet-switched networks, the NDAC has begun analyzing the implications for the resulting NGN. NDAC has begun to evaluate the performance of multiple NGN architectures under various scenarios, including damage and congestion. For the pandemic study, CS&C used the NDAC to analyze network congestion resulting from telecommuting which would be similar to congestion resulting from a disruption to the Internet. Lessons learned through similar studies will inform the manner in which we plan for and respond to Internet disruptions and will provide actionable recommendations for government and industry partners.

While the NDAC work focuses on understanding networks in advance of a disruption, it can also be used to model the effects of known or likely damage after a disruption has occurred. Another CS&C program, designed to mitigate the effects of a communications network disruption, is the NCS' Priority Telecommunications Service. PTS was developed to ensure our Nation's leadership could communicate in times of congestion in the public network. Through

partnerships with communications providers, PTS has developed programs which provide priority access to both the wireless and wire line networks. As these networks are transitioning to IP-based, packet switched networks, the NCS has begun development of PTS for operation in the resultant Next Generation Network. As noted earlier, this capability will ensure our Nation's leadership continues to have priority access to voice communications in times of network congestion. Additionally, the NCS is developing plans for features such as priority email and priority video teleconferencing. The NCS is determined to ensure these vital capabilities are available for our Nation's leadership as communications networks continue to rapidly evolve.

To understand the effectiveness of these planning and modeling efforts, CS&C sponsors exercises to rehearse, test, and refine key cyber processes and mechanisms for coordination and information exchange; and identify interdependencies, overlaps, and gaps in existing plans and processes. The National Cyber Exercise, Cyber Storm II, scheduled for March 2008, will include a focus on Internet disruption and related recovery. Cyber Storm II will examine the capabilities of participating organizations to prepare for, protect from, and respond to the potential effects of cyber attacks; exercise strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures; validate information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information; and examine means and processes through which to share sensitive information across boundaries and sectors, without compromising proprietary or national security interests. Cyber Storm II will also provide an opportunity to exercise Concepts of Operations and Standard Operating Procedures that have been developed or updated based on the findings from Cyber Storm I.

NCSD's Cyber Storm II planning team is working with the IT and Communications SCCs and ISACs and other subject matter experts from government and industry to contribute to the scenario development. Scenarios will include Internet and communications disruption and stakeholder-specific issues requiring a coordinated incident response. The adversary framework may ultimately include organized crime, a terrorist organization, and a nation-state, and will be refined based on the capabilities an adversary would need to conduct the scenario-specific attacks. Cyber Storm II provides a mechanism for CS&C together with a wide variety of public and private entities to improve cyber security preparedness and incident response capabilities and refine roles and responsibilities.

Delivering Capabilities to Respond to and Recover from Internet Disruptions

Cyber Storm II will also provide an opportunity to exercise response and recovery plans from the recently released draft National Response Framework (NRF), the successor to the National Response Plan. The Framework, which focuses on response to a national emergency and short-term recovery, articulates the doctrine, principles, and architecture by which our Nation responds to all-hazard disasters across all levels of government and all infrastructure sectors. The Framework incorporates a number of key recommendations from more than 700 individuals representing Federal, Tribal, State and local governments, non-governmental agencies and associations, and the private sector, who participated in the review process. As part of the NRF review, CS&C undertook an in-depth review of the NRF components, which seek to address incidents pertaining to communications and IT. These include Emergency Support Function

(ESF) #2 – Communications Annex and the Cyber Incident Annex. ESF#2, for which the NCS is a Coordinating Agency, supports the restoration of public communications infrastructure, supports responses to Cyber Incidents, and coordinates Federal communications support to response efforts.

For national incidents that are primarily cyber in nature, the Cyber Incident Annex provides the response and recovery framework. The Cyber Incident Annex, for which the NCSD is the Coordinating Agency, focuses on responding to, and recovering from significant cyber incidents requiring a coordinated Federal response ("Cyber Incidents"). The characteristics of a Cyber Incident may include incidents that impact critical government functions, threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation. The Cyber Incident Annex provides a framework for Federal Cyber Incident response coordination among Federal departments, agencies, and upon request, State, local, tribal, and private sector entities. When a Cyber Incident occurs, it could impact multiple infrastructure sectors or be targeted at a specific sector such as finance, energy, or communications. As such, a Cyber Incident could result in the activation of several or all of the ESF Annexes under the NRF. The Cyber Incident Annex is currently undergoing a public comment period to collect recommendations from government, non-governmental agencies and associations, and the private sector.

Consistent with the guidance in the NRF, ESF#2, and the Cyber Incident Annex, NCSD works with DHS' Incident Management Planning Team to develop the National Cyber Scenario Plan, one of fifteen National-level strategic plans being developed to guide the Nation's response to specific incidents. This planning effort will include input from the National Cyber Response Coordination Group (NCRCG), US-CERT, the Department of Defense (DOD), law enforcement, the intelligence community, State governments, international allies, and the private sector. Using the comprehensive capabilities of these entities, the plan will detail the roles and responsibilities and the capabilities available to the Federal Government to respond to a Cyber Incident.

The NCRCG serves as the principal Federal interagency mechanism to facilitate coordination of the Federal Government's efforts to prepare for, respond to, and recover from, cyber and physical incidents and attacks that have significant cyber consequences. The Cyber Incident Annex of the NRF identifies a role for the NCRCG, which is co-chaired by DHS, the Department of Justice, and DOD. The NCRCG is comprised of senior representatives from Federal agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from Cyber Incidents. The senior level membership of NCRCG helps ensure that during a significant national incident, the full range and weight of Federal capabilities will be deployed in a coordinated and effective fashion. For example, the NCRCG recently convened to address the denial of service attack against the Government of Estonia. Once the co-chairs were notified of the activity, and convened to discuss the situation, it was determined that an operational response was needed. This response was coordinated through CS&C's two operational arms—US-CERT and the NCC.

NCC and US-CERT are critically important to managing ongoing cyber incidents, and the two operations centers are positioned to work together to address cyber attacks, including those targeting the Internet. The NCC, established in 1984, has served as a forum in which the Federal

government and private sector communications providers interact face-to-face on a daily basis. In the NCSD's US-CERT, public and private sector entities collaborate with DHS to coordinate defense against and responses to cyber attacks across the Nation. Reflecting shifts in the Communications Sector, NCC membership has evolved over time to include satellite, cellular, cable, and IT companies in addition to the core telecommunications companies. In the event of an emergency involving the disruption of communications networks, the NCC, through its 24x7 operation, provides a forum for government and industry to coordinate incident response and recovery.

US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. To fulfill these responsibilities, US-CERT coordinates with a broad community of key private sector and government entities on topics ranging from Domain Name System (DNS) issues to core IP topics. For example, to bring greater attention to DNS and IP issues of national significance, US-CERT has been attending the North American Network Operations Group (NANOG) meetings for the last three years. Regular information sharing with public and private entities such as NANOG enables US-CERT to build situational awareness of network conditions, identify abnormal network activity, and initiate a response to prevent a more significant cyber incident. US-CERT also engages with the various sector ISACs to report, exchange and analyze sensitive information concerning cyber threats, vulnerabilities, incidents with strong and enforceable legal protections.

US-CERT works particularly closely with the IT-ISAC as the operational arm of the IT SCC. US-CERT and the IT-ISAC have instituted processes to regularly exchange information, analyze threats and vulnerabilities, and mitigate their effects. US-CERT and the IT-ISAC engage routinely through routine conference calls and other means and are working towards formalizing operating procedures. By working together in this manner, US-CERT and the IT-ISAC will ensure that the necessary mechanisms for collaboration are established and practiced.

To coordinate with government stakeholders, US-CERT also maintains robust collaborative arrangements. US-CERT works with the Multi-State ISAC to reach state and local government. The MS-ISAC serves as a mechanism for raising the level of cyber security readiness and response in each state. US-CERT also sponsors the Government Forum of Incident Response and Security Teams, which is a community of more than 50 Federal agency incident response teams that work together to secure U.S. Government networks.

US-CERT builds situational awareness of network conditions through its work with Federal departments and agencies utilizing its Einstein program. The Einstein program identifies abnormal network activity so that US-CERT and its partners can initiate a response to prevent a more significant cyber incident. Einstein enables strategic, cross-agency assessments of irregular or abnormal Internet activity that could indicate a vulnerability or problem in the system. The program passively monitors government agencies' gateways to facilitate the identification and response to cyber threats and attacks, improve network security, increase the resilience of critical electronically delivered government services, and enhance the survivability of the Internet.

These private and public sector engagements are critical to building trusted operational relationships that enable effective information sharing needed to respond in the event that a disruption occurs.

NCS and NCSD are working closely together to ensure that operational activities are coordinated, threats and vulnerabilities are jointly addressed, and the resources and expertise of each organization are brought to bear in this converged environment. CS&C is implementing a plan to co-locate the US-CERT and NCC watch and operations centers to ensure that IT and communications experts are working side-by-side to share situational awareness information and identify threats, attack vectors, and the implications of these threats and attacks across all infrastructure sectors. Towards this end, I also convened a joint industry-government task force to review the plans to further develop this integrated operational capability. The task force has completed its work and provided recommendations that I have begun to implement, such as the assignment of a program manager to implement the first phase of the recommendations, to include incorporating an IT industry representative into our operational framework.

CS&C is also working with DOD's Joint Task Force for Global Network Operations (JTF-GNO) to enhance information sharing and situational awareness between the two organizations to ensure the security and uninterrupted and unhindered access to the Internet. Joint operating procedures have been developed to describe US-CERT and JTF-GNO information sharing and response processes for addressing Federal and national Cyber Incidents. Plans include assignment of staff to the respective operations centers to increase coordination.

These efforts provide mechanisms for defending against, responding to, and recovering from incidents. Our collaboration with public and private sector entities is essential in these areas, and we must expand our work with others who share the need for cyber security. By doing so, we can promote the sharing of knowledge on active and strategic threats, awareness of exploits of specific vulnerabilities, and understanding of mitigation strategies.

Conclusion

Both Government and the private sector are taking action to address the resilience and recovery of Internet functions in the event of a major cyber incident. Effective collaboration with the private sector and other government entities provides a foundation for exchange of information and coordination of preparedness and response activities. We have established mechanisms to ensure that the Federal Government is prepared to handle the impact that an Internet disruption may have on our ability to achieve our mission and to respond in a timely manner to address and mitigate the consequences of a disruption. Similarly, the private sector has taken significant steps to manage risks to the Internet infrastructure and maintain its associated services and functions. Taken together, these efforts offer a framework for addressing Internet disruption now and in the future.

As we move forward, Government and the private sector must continue our collaborative efforts to prepare for and respond to Internet disruptions. To do this, senior business leaders across all industry sectors must be aggressive and take coordinated steps to assess their dependence on the Internet and our cyber infrastructure. Government departments and agencies must also ensure

that the Federal workforce understands its dependence on the Internet, the impact that a disruption could have, and steps that can be taken routinely to mitigate the consequences. Both Government and the private sector must have in place and regularly exercise continuity plans that can be implemented without the benefit of Internet or phone service. Ongoing assessment of the risk to the IT, Communications, and other CI/KR sectors will ensure that cyber security is an integral part of sector and organizational efforts to prepare for and respond to incidents.

I would like to thank the Subcommittee for its time today. I appreciate this opportunity to discuss this important issue.

Mr. CLAY. Thank you very much, Mr. Garcia. Mr. Wilshusen, you are next.

STATEMENT OF GREGORY C. WILSHUSEN

Mr. WILSHUSEN. Chairman Clay and members of the subcommittee, thank you for the opportunity to testify at today's hearing on public and private sector efforts to secure our Nation's Internet infrastructure.

Since the early 1990's, the world community has come to rely on the Internet as a critical resource supporting commerce, education and communication. While the benefits of this technology have been enormous, this widespread inter-connectivity poses significant risks to our Government's and Nation's computer systems and, more importantly, to the critical operations and infrastructures they support.

Today, I will discuss threats and vulnerabilities of the Internet, DHS' efforts in facilitating recovery from Internet disruptions and key challenges to such efforts.

Mr. Chairman, the Internet is vulnerable to disruptions in service due to threats of terrorists and other malicious attacks, natural disasters and technological problems or a combination of these things. Disruptions to Internet service can be caused by cyber and physical incidents, both intentional and unintentional. For example, over the last few years, fast-spreading worms and viruses coordinated denial of service against key root servers, 9/11 and Hurricane Katrina have caused local or regional disruptions or slowdowns.

Research organizations have pegged the annual worldwide costs of malicious code attacks as averaging about $14 billion for the 6-years ending in 2005, highlighting the importance of recovery planning. However, these incidents have also shown the Internet as a whole to be flexible resilient. Even in severe circumstances, the Internet has not yet suffered a catastrophic failure.

Nevertheless, is it possible that a complex attack or series of attacks could cause the Internet to fail or to undermine users' trust in the Internet, thereby reducing the Internet's utility.

In a June 2006 report, we noted that DHS had begun a variety of initiatives to improve the Nation's ability to recover from Internet disruptions, including developing an integrated public/private plan for Internet recovery, establishing working groups to facilitate coordination, and conducting exercises in which Government and private industry practice responding to cyber events.

However, these efforts were not complete, comprehensive or effectively coordinated. In that report, we also noted key challenges that impeded progress. First, it was unclear what Government entity was in charge, what the Government's role should be, and when it should get involved. For example, DHS' National Cyber Security Division and National Communications System had overlapping responsibilities. There is also a lack of consensus about the role DHS should play. The Government was pursuing the big plan approach with the NIPP and the National Response Plan while the private sector wanted to more of the short-term tactical role from the Government.

Furthermore, triggers to clarify when the Federal Government should be involved were unclear. Another key challenge is working in a legal framework that doesn't specifically address the Government's roles and responsibilities in the event of an Internet disruption. The Katrina recovery efforts also showed that the Stafford Act can create a roadblock when for-profit companies that own and operate critical infrastructures need Federal assistance during national emergencies.

In addition, the private sector was reluctant to share information with DHS because it did not always see value in sharing information, did not necessarily trust the Government and viewed DHS as an organization lacking effective leadership.

Until these challenges are addressed, DHS will have difficulty in achieving results in its role as a focal point in this area.

In our June 2006 report, we suggested that Congress consider clarifying the legal framework that guides roles and responsibilities for Internet recovery. We also made recommendations to improve DHS' ability to facilitate public/private efforts and planning for Internet disruptions. The Department agreed with our recommendations and since then has made progress in addressing many of them.

Still work remains to be done to ensure that our Nation is prepared to effectively respond to a disruption of the Internet infrastructure.

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

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Information Policy, Census, and National Archives, House Committee on Oversight and Government Reform

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, October 23, 2007

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-08-212T

October 23, 2007

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-212T, a testimony before the Subcommittee on Information Policy, Census, and National Archives, House Committee on Oversight and Government Reform

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan

Why GAO Did This Study

Since the early 1990s, growth in the use of the Internet has revolutionized the way that our nation communicates and conducts business. While the Internet originated as a U.S. government-sponsored research project, the vast majority of its infrastructure is currently owned and operated by the private sector. Federal policy recognizes the need to prepare for debilitating Internet disruptions and tasks the Department of Homeland Security (DHS) with developing an integrated public/private plan for Internet recovery.

GAO was asked to summarize its report on plans for recovering the Internet in case of a major disruption (GAO-06-672) and to provide an update on DHS's efforts to implement that report's recommendations. The report (1) identifies examples of major disruptions to the Internet, (2) identifies the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluates DHS plans for facilitating recovery from Internet disruptions, and (4) assesses challenges to such efforts.

What GAO Recommends

In its report, GAO made recommendations to DHS to strengthen its ability to help recover from Internet disruptions. In written comments, DHS agreed with these recommendations.

To view the full product, including the scope and methodology, click on GAO-08-212T. For more information, contact Gregory C. Wilshusen, 202-512-6244, wilshuseng@gao.gov.

What GAO Found

A major disruption to the Internet could be caused by a physical incident (such as a natural disaster or an attack that affects key facilities), a cyber incident (such as a software malfunction or a malicious virus), or a combination of both physical and cyber incidents. Recent physical and cyber incidents, such as Hurricane Katrina, have caused localized or regional disruptions but have not caused a catastrophic Internet failure.

Federal laws and regulations that address critical infrastructure protection, disaster recovery, and the telecommunications infrastructure provide broad guidance that applies to the Internet, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption. Specifically, key legislation on critical infrastructure protection does not address roles and responsibilities in the event of an Internet disruption. Other laws and regulations governing disaster response and emergency communications have never been used for Internet recovery.

As of 2006, DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts were not yet comprehensive or complete. For example, the department had developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure were not complete. As a result, the risk remained that the government was not adequately prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

Key challenges to establishing a plan for recovering from Internet disruptions include (1) innate characteristics of the Internet that make planning for and responding to disruptions difficult, (2) lack of consensus on DHS's role and when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to restore Internet service, (4) reluctance of many in the private sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. Until these challenges are addressed, DHS will have difficulty achieving results in its role as a focal point for helping the Internet to recover from a major disruption.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss public/private recovery plans for the Internet infrastructure. Since the early 1990s, the world community has come to rely on the Internet as a critical infrastructure supporting commerce, education, and communication. While the benefits of this technology have been enormous, this widespread interconnectivity poses significant risks to the computer systems of our government and our nation and, more importantly, to the critical operations and infrastructures they support.

Federal regulation establishes the Department of Homeland Security (DHS) as the focal point for the security of cyber space—including recovery efforts for public and private critical infrastructure systems.[1] Additionally, federal policy recognizes the need to be prepared for the possibility of debilitating Internet disruptions and tasks DHS with developing an integrated public/private plan for Internet recovery.[2] In June 2006, we issued a report[3] that (1) identifies examples of major disruptions to the Internet, (2) identifies the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluates DHS's plans for facilitating recovery from Internet disruptions, and (4) assesses challenges to such efforts. The report includes matters for congressional consideration and recommendations to DHS for improving Internet recovery efforts.

As requested, this testimony summarizes our June 2006 report and provides an update of DHS's efforts to implement our recommendations. The report that this testimony was based on contains a detailed overview of our scope and methodology and was

[1]Homeland Security Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection* (Washington, D.C.: Dec. 17, 2003).

[2]The White House, *National Strategy to Secure Cyberspace* (Washington D.C.: February 2003).

[3]GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006).

performed in accordance with generally accepted government auditing standards.

Results in Brief

A major disruption to the Internet could be caused by a physical incident (such as a natural disaster or an attack that affects facilities and other assets), by a cyber incident (such as a software malfunction or a malicious virus), or by a combination of physical and cyber incidents. Recent physical and cyber incidents have caused localized or regional disruptions, highlighting the importance of recovery planning. For example, a 2002 root server attack highlighted the need to plan for increased server capacity at Internet exchange points in order to manage the high volumes of data traffic during an attack. However, recent incidents have also shown the Internet to be flexible and resilient. Even in severe circumstances, the Internet did not suffer a catastrophic failure. Nevertheless, it is possible that a complex attack or set of attacks could cause the Internet to fail. It is also possible that a series of attacks against the Internet could undermine users' trust and thereby reduce the Internet's utility.

Several federal laws and regulations provide broad guidance that applies to the Internet, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption. Specifically, the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 provide guidance on protecting our nation's critical infrastructures. However, they do not specifically address roles and responsibilities in the event of an Internet disruption. The Defense Production Act and the Stafford Act provide authority to federal agencies to plan for and respond to incidents of national significance like disasters and terrorist attacks. However, the Defense Production Act has never been used for Internet recovery. In addition, the Stafford Act does not authorize the provision of resources to for-profit companies such as those that own and operate core Internet components. The Communications Act of 1934 and National Communication System authorities govern the telecommunications infrastructure and help ensure communications during national emergencies, but they have never

been used for Internet recovery, either. Thus, it is not clear how effective these laws and regulations would be in assisting Internet recovery.

As of 2006, DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts were not yet comprehensive or complete. Specifically, the department had developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure were not complete. In addition, DHS had started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. However, progress on these initiatives was limited, and other initiatives lacked timeframes for completion. Also, the relationships among these initiatives were not evident. As a result, the risk remained that the government was not adequately prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

Key challenges to establishing a plan for recovering from Internet disruption include (1) innate characteristics of the Internet (such as the diffuse control of the many networks that make up the Internet and the private-sector ownership of core components) that make planning for and responding to disruptions difficult, (2) lack of consensus on DHS's role and when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to entities working to restore Internet service, (4) reluctance of many in the private sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. Until these challenges are addressed, DHS will have difficulty achieving results in its role as a focal point for helping to recover the Internet from a major disruption.

Given the importance of the Internet infrastructure to our nation's communications and commerce, we suggested in our report that

Congress consider clarifying the legal framework guiding Internet recovery.[4] We also made recommendations to the Secretary of Homeland Security to strengthen the department's ability to serve effectively as a focal point for helping to recover from Internet disruptions by establishing clear milestones for completing key plans, coordinating various Internet recovery-related activities, and addressing key challenges to Internet recovery planning.

DHS agreed with our recommendations and has made progress in implementing them. Specifically, DHS has revised key plans in coordination with private industry infrastructure stakeholders, coordinated various Internet recovery-related activities, and worked to address key challenges in Internet recovery planning. However, further work remains to be done to complete these activities. For example, DHS has yet to complete recovery plans or to define the interdependencies among its various working groups and initiatives. Full implementation of these recommendations should enhance the nation's ability to recover from a major Internet disruption.

Background

The Internet is a vast network of interconnected networks that is used by governments, businesses, research institutions, and individuals around the world to communicate, engage in commerce, perform research, educate, and entertain. From its origins in the 1960s as a research project sponsored by the U.S. government, the Internet has grown increasingly important to both American and foreign businesses and consumers, serving as the medium for hundreds of billions of dollars of commerce each year. The Internet has also become an extended information and communications infrastructure, supporting vital services such as power distribution, health care, law enforcement, and national defense. Today, private industry—including telecommunications companies, cable companies, and Internet service providers—owns and operates the vast majority of the Internet's infrastructure. In recent years, cyber attacks involving malicious software or hacking have been

[4]GAO-06-672.

increasing in frequency and complexity. Attacks against the Internet can come from a variety of sources, including criminal groups, hackers, and terrorists.

Federal regulation recognizes the need to protect critical infrastructures such as the Internet. It directs federal departments and agencies to identify and prioritize critical infrastructure sectors and key resources and to protect them from terrorist attack. Furthermore, it recognizes that since a large portion of these critical infrastructures is owned and operated by the private sector, a public/private partnership is crucial for the successful protection of these critical infrastructures. Federal policy also recognizes the need to be prepared for the possibility of debilitating disruptions in cyberspace and, because the vast majority of the Internet infrastructure is owned and operated by the private sector, tasks DHS with developing an integrated public/private plan for Internet recovery. In its plan for protecting critical infrastructures, DHS recognizes that the Internet is a key resource composed of assets within both the information technology and the telecommunications sectors.[5] It notes that the Internet is used by all critical infrastructure sectors to varying degrees and provides information and communications to meet the needs of businesses and government.

In the event of a major Internet disruption, multiple organizations could help recover Internet service. These organizations include private industry, collaborative groups, and government organizations. Private industry is central to Internet recovery because private companies own most of the Internet's infrastructure and often have response plans. Collaborative groups—including working groups and industry councils—provide information-sharing mechanisms to allow private organizations to restore services. In addition, government initiatives could facilitate a response to major Internet disruptions.

[5]DHS, *The National Infrastructure Protection Plan.*

Federal policies and plans[6] assign DHS with the lead responsibility for facilitating a public/private response to and recovery from major Internet disruptions. Within DHS, responsibilities reside in two divisions within the Office of the Under Secretary for National Protection and Program, Office of Cybersecurity and Communications: the National Cyber Security Division (NCSD) and the National Communications System (NCS). NCSD operates the U.S. Computer Emergency Readiness Team (US-CERT), which coordinates defense against and response to cyber attacks. The other division, NCS, provides programs and services that assure the resilience of the telecommunications infrastructure in times of crisis. Additionally, the Federal Communications Commission can support Internet recovery by coordinating resources for restoring the basic communications infrastructures over which Internet services run. For example, after Hurricane Katrina, the commission granted temporary authority for private companies to set up wireless Internet communications supporting various relief groups; federal, state, and local government agencies; businesses; and victims in the disaster areas.

Prior evaluations of DHS's cyber security responsibilities have highlighted issues and challenges facing the department. In May 2005, we issued a report on DHS's efforts to fulfill its cyber security responsibilities.[7] We noted that while DHS had initiated multiple efforts to fulfill its responsibilities, it had not fully addressed any of the 13 key cyber security responsibilities noted in federal law and policy. We also reported that DHS faced a number of challenges that have impeded its ability to fulfill its cyber responsibilities. These challenges included achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness of cyber security roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with stakeholders, and demonstrating the value that DHS can provide. In that report, we also made

[6]These include the *National Strategy to Secure Cyberspace*, the interim *National Infrastructure Protection Plan*, the Cyber Incident Annex to the *National Response Plan*, and Homeland Security Presidential Directive 7.

[7]GAO-05-434.

recommendations to improve DHS's ability to fulfill its mission as an effective focal point for cyber security, including recovery plans for key Internet functions. DHS agreed that strengthening cyber security is central to protecting the nation's critical infrastructures and that much remained to be done.

Although Cyber and Physical Incidents Have Caused Disruptions, the Internet Has Not Yet Suffered a Catastrophic Failure

The Internet's infrastructure is vulnerable to disruptions in service due to terrorist and other malicious attacks, natural disasters, accidents, technological problems, or a combination of these things. Disruptions to Internet service can be caused by cyber and physical incidents—both intentional and unintentional. Over the last few years, physical and cyber incidents have caused localized or regional disruptions, highlighting the importance of recovery planning. However, these incidents have also shown the Internet as a whole to be flexible and resilient. Even in severe circumstances, the Internet has not yet suffered a catastrophic failure.

To date, cyber attacks have caused various degrees of damage. For example, in 2001, the Code Red worm used a denial-of-service attack to affect millions of computer users by shutting down Web sites, slowing Internet service, and disrupting business and government operations. In 2003, the Slammer worm caused network outages, canceled airline flights, and automated teller machine failures. Slammer resulted in temporary loss of Internet access to some users, and cost estimates on the impact of the worm range from $1.05 billion to $1.25 billion. The federal government coordinated with security companies and Internet service providers and released an advisory recommending that federal departments and agencies patch and block access to the affected channel. However, because the worm had propagated so quickly, most of these activities occurred after it had stopped spreading.

In 2002 and again in 2007, coordinated denial-of-service attacks were launched against all of the root servers in the Domain Name System. In the 2002 attack, at least nine of the thirteen root servers experienced degradation of service, while in the 2007 attack, six of

the thirteen root servers experienced degradation of service. However, average end users hardly noticed the attacks. The attacks were efficiently handled by the server operators and their service providers. The 2002 attack pointed to a need for increased capacity for servers at Internet exchange points to enable them to manage the high volumes of data traffic during an attack. The 2007 attack demonstrated that some of the improvements made since 2002 to improve the resilience of the Internet had worked.

Like cyber incidents, physical incidents could affect various aspects of the Internet infrastructure, including underground or undersea cables and facilities that house telecommunications equipment, Internet exchange points, or Internet service providers. For example, on July 18, 2001, a 60-car freight train derailed in a Baltimore tunnel, causing a fire that interrupted Internet and data services between Washington and New York. The tunnel housed fiber-optic cables serving seven of the biggest U.S. Internet service providers. The fire burned and severed fiber optic cables, causing backbone slowdowns for at least three major Internet service providers. Efforts to recover Internet service were handled by the affected Internet service providers; however, local and federal officials responded to the immediate physical issues of extinguishing the fire and maintaining safety in the surrounding area, and they worked with telecommunications companies to reroute affected cables.

In another physical incident, Hurricane Katrina caused substantial destruction of the communications infrastructures in Louisiana, Mississippi, and Alabama, but it had minimal affect on the overall functioning of the Internet outside of the immediate area. According to an Internet monitoring service provider, while there was a loss of routing around the affected area, there was no significant impact on global Internet routing. According to the Federal Communications Commission, the storm caused outages for more than 3 million telephone customers, 38 emergency 9-1-1 call centers, hundreds of thousands of cable customers, and more than 1,000 cellular sites. However, a substantial number of the networks that experienced service disruptions recovered relatively quickly.

Federal officials stated that the government took steps to respond to the hurricane, such as increasing analysis and watch services in the affected area, coordinating with communications companies to move personnel to safety, working with fuel and equipment providers, and rerouting communications traffic away from affected areas. However, private sector representatives stated that requests for assistance, such as food, water, fuel, and secure access to facilities were denied for legal reasons; the government made time-consuming and duplicative requests for information; and certain government actions impeded recovery efforts.

Since its inception, the Internet has experienced disruptions of varying scale—including fast-spreading worms, denial-of-service attacks, and physical destruction of key infrastructure components—but the Internet has yet to experience a catastrophic failure. However, it is possible that a complex attack or set of attacks could cause the Internet to fail. It is also possible that a series of attacks against the Internet could undermine users' trust and thereby reduce the Internet's utility.

Existing Laws and Regulations Apply to the Internet, but Numerous Uncertainties Exist in Using Them for Internet Recovery

Several federal laws and regulations provide broad guidance that applies to the Internet infrastructure, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption because some do not specifically address Internet recovery and others have seldom been used. Pertinent laws and regulations address critical infrastructure protection, federal disaster response, and the telecommunications infrastructure.

Specifically, the Homeland Security Act of 2002[8] and Homeland Security Presidential Directive 7[9] establish critical infrastructure protection as a national goal and describe a strategy for cooperative

[8]The Homeland Security Act of 2002, Pub. L. No.107-296 (Nov. 25, 2002).

[9]Homeland Security Presidential Directive 7 (Dec. 17, 2003).

efforts by the government and the private sector to protect the physical and cyber-based systems that are essential to the operations of the economy and the government. These authorities apply to the Internet because it is a core communications infrastructure supporting the information technology and telecommunications sectors; however, they do not specifically address roles and responsibilities in the event of an Internet disruption.

Regarding federal disaster response, the Defense Production Act[10] and the Stafford Act[11] provide authority to federal agencies to plan for and respond to incidents of national significance like disasters and terrorist attacks. Specifically, the Defense Production Act authorizes the President to ensure the timely availability of products, materials, and services needed to meet the requirements of a national emergency. It is applicable to critical infrastructure protection and restoration but has never been used for Internet recovery. The Stafford Act authorizes federal assistance to states, local governments, nonprofit entities, and individuals in the event of a major disaster or emergency. However, the act does not authorize assistance to for-profit companies—such as those that own and operate core Internet components.

Other legislation and regulations, including the Communications Act of 1934[12] and the NCS authorities,[13] govern the telecommunications infrastructure and help to ensure communications during national emergencies. For example, the NCS authorities establish guidance for operationally coordinating with industry to protect and restore key national security and emergency preparedness communications services. These authorities grant the President certain emergency powers regarding telecommunications, including the authority to

[10]Act of September 8, 1950, c. 932, 64 Stat. 798, as amended; codified at 50 U.S.C. App. Section 2061 *et seq.*

[11]Pub. L. No. 93-288, 88 Stat. 143 (1974).

[12]Communications Act of 1934 (June 19, 1934), ch. 652, 48 Stat. 1064.

[13]Executive Order 12472 (Apr. 3, 1984), as amended by Executive Order 13286 (Feb. 28, 2003).

require any carrier subject to the Communications Act of 1934 to grant preference or priority to essential communications.[14] The President may also, in the event of war or national emergency, suspend regulations governing wire and radio transmissions and authorize the use or control of any such facility or station and its apparatus and equipment by any department of the government. Although these authorities remain in force in the *Code of Federal Regulations*, they have seldom been used—and never for Internet recovery. Thus it is not clear how effective they would be if used for this purpose.

In commenting on the statutory authority for Internet reconstitution following a disruption, DHS agreed that this authority is lacking and noted that the government's roles and authorities related to assisting in Internet reconstitution following a disruption are not fully defined.

DHS Initiatives Supporting Internet Recovery Planning Are Under Way, but Much Remains to Be Done and the Relationships Among the Initiatives Are Not Evident

As of our June 2006 report, DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts were not complete or comprehensive. Specifically, DHS had developed high-level plans, including the *National Response Plan* and the *National Infrastructure Protection Plan*, for infrastructure protection and national disaster response, but the components of these plans that address the Internet infrastructure were not complete.

In addition, DHS had started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including establishing working groups to facilitate coordination, such as the *National Cyber Response Coordination Group* and *Internet Disruption Working Group*, and exercises in which government and

[14]Executive Order 12472 § 2; Communications Act of 1934, § 706, 47 U.S.C § 606.

private industry practice responding to cyber events. While these activities were promising, the responsibilities and plans for selected working groups had not yet been defined, and key exercises lacked effective mechanisms for incorporating lessons learned. In addition, the relationships among the initiatives were not evident. For example, the National Cyber Response Coordination Group, the Internet Disruption Working Group, and the North American Incident Response Group were all meeting to discuss ways to address Internet recovery, but the interdependencies among the groups had not been clearly established. As a result, the nation was not prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

Multiple Challenges Exist to Planning for Recovery from Internet Disruptions

Although DHS has various initiatives to improve Internet recovery planning, there are key challenges in developing a public/private plan for Internet recovery, including (1) innate characteristics of the Internet that make planning for and responding to a disruption difficult, (2) lack of consensus on DHS's role and on when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to restore Internet service, (4) reluctance of the private sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. Until these challenges are addressed, DHS will have difficulty achieving results in its role as a focal point for recovering the Internet from a major disruption.

First, the Internet's diffuse structure, vulnerabilities in its basic protocols, and the lack of agreed-upon performance measures make planning for and responding to a disruption more difficult. The components of the Internet are not all governed by the same organization. In addition, the Internet is international. According to private-sector estimates, only about 20 percent of Internet users are in the United States. Also, there are no well-accepted standards for measuring and monitoring the Internet infrastructure's availability

and performance. Instead, individuals and organizations rate the Internet's performance according to their own priorities.

Second, there is no consensus about the role DHS should play in responding to a major Internet disruption or about the appropriate trigger for its involvement. The lack of clear legislative authority for Internet recovery efforts complicates the definition of this role. DHS officials acknowledged that their role in recovering from an Internet disruption needs further clarification because private industry owns and operates the vast majority of the Internet.

Private sector officials representing telecommunication backbone providers and Internet service providers were also unclear about the types of assistance DHS could provide in responding to an incident and about the value of such assistance. There was no consensus on this issue. Many private-sector officials stated that the government does not have a direct recovery role, while others identified a variety of potential roles, including

- providing information on specific threats;
- providing security and disaster relief support during a crisis;
- funding backup communication infrastructures;
- driving improved Internet security through requirements for the government's own procurement;
- serving as a focal point with state and local governments to establish standard credentials to allow Internet and telecommunications companies access to areas that have been restricted or closed in a crisis;
- providing logistical assistance, such as fuel, power, and security, to Internet infrastructure operators;
- focusing on smaller-scale exercises targeted at specific Internet disruption issues;

- limiting the initial focus for Internet recovery planning to key national security and emergency preparedness functions, such as public health and safety; and
- establishing a system for prioritizing the recovery of Internet service, similar to the existing Telecommunications Service Priority Program.

A third challenge to planning for recovery is that there are key legal issues affecting DHS's ability to provide assistance to help restore Internet service. As noted earlier, key legislation and regulations guiding critical infrastructure protection, disaster recovery, and the telecommunications infrastructure do not provide specific authorities for Internet recovery. As a result, there is no clear legislative guidance on which organization would be responsible in the case of a major Internet disruption. In addition, the Stafford Act, which authorizes the government to provide federal assistance to states, local governments, nonprofit entities, and individuals in the event of a major disaster or emergency, does not authorize assistance to for-profit corporations. Several representatives of telecommunications companies reported that they had requested federal assistance from DHS during Hurricane Katrina. Specifically, they requested food, water, and security for the teams they were sending in to restore the communications infrastructure and fuel to power their generators. DHS responded that it could not fulfill these requests, noting that the Stafford Act did not extend to for-profit companies.

A fourth challenge is that a large percentage of the nation's critical infrastructure—including the Internet—is owned and operated by the private sector, meaning that public/private partnerships are crucial for successful critical infrastructure protection. Although certain policies direct DHS to work with the private sector to ensure infrastructure protection, DHS does not have the authority to direct Internet owners and operators in their recovery efforts. Instead, it must rely on the private sector to share information on incidents, disruptions, and recovery efforts. Many private sector representatives questioned the value of providing information to

DHS regarding planning for and recovery from Internet disruption. In addition, DHS has identified provisions of the Federal Advisory Committee Act[15] as having a "chilling effect" on cooperation with the private sector. The uncertainties regarding the value and risks of cooperation with the government limit incentives for the private sector to cooperate in Internet recovery-planning efforts.

Finally, DHS has lacked permanent leadership while developing its preliminary plans for Internet recovery and reconstitution. In May 2005, we reported that multiple senior DHS cyber security officials had recently left the department.[16] These officials included the NCSD Director, the Deputy Director responsible for Outreach and Awareness, the Director of the US-CERT Control Systems Security Center, the Under Secretary for the Information Analysis and Infrastructure Protection Directorate and the Assistant Secretary responsible for the Information Protection Office. DHS officials acknowledge that the current organizational structure has overlapping responsibilities for planning for and recovering from a major Internet disruption.

DHS Has Taken Steps To Implement Recommendations, but More Work Remains To Be Done

Given the importance of the Internet infrastructure to our nation's communication and commerce, our June 2006 report suggested a matter for congressional consideration and made recommendations to DHS regarding improving efforts in planning for Internet recovery.[17] Specifically, we suggested that Congress consider clarifying the legal framework that guides roles and responsibilities for Internet recovery in the event of a major disruption. This effort could include providing specific authorities for Internet recovery as well as examining potential roles for the federal government, such as providing access to disaster areas, prioritizing selected entities

[15]Pub. L. No. 92-463, 86 Stat. 770 (1972) codified at 5 U.S.C. app. 2.

[16]GAO-05-434.

[17]GAO-06-672.

for service recovery, and using federal contracting mechanisms to encourage more secure technologies. This effort also could include examining the Stafford Act to determine whether there would be benefits in establishing specific authority for the government to provide for-profit companies—such as those that own or operate critical communications infrastructures—with limited assistance during a crisis.

Additionally, to improve DHS's ability to facilitate public/private efforts to recover the Internet in case of a major disruption, we recommended that the Secretary of the Department of Homeland Security implement nine actions (see table 1). The department agreed with our recommendations and has made progress in addressing many of them. Still, work remains to be done to ensure that our nation is prepared to effectively respond to a disruption of the Internet infrastructure.

Table 1: DHS's Progress in Addressing GAO Recommended Actions

Recommended Actions	Status	DHS Progress
Establish dates for revising the *National Response Plan*—including efforts to update key components that are relevant to the Internet.	In process	DHS revised its *National Response Plan* (the revised version is called the *National Response Framework*) and released it for public comment in September 2007. As part of this effort, the agency revised segments that are relevant to the Internet, including the Cyber Incident Annex. However, DHS did not provide a date for when it expects to complete the Framework.
Use the planned revisions to the *National Response Plan* and the *National Infrastructure Protection Plan* as a basis to draft public/private plans for Internet recovery and obtain input from key Internet infrastructure companies.	In process	As noted above, DHS's *National Response Framework* has been updated and released for public comment, but has not yet been completed. In addition, DHS released the National Infrastructure Protection Plan's base plan in June 2006 and the sector specific plans in May 2007. Because both documents have been made available for input from key infrastructure companies, DHS expects that they should serve as the basis for public/private plans for Internet recovery.
Review the NCS and NCSD organizational structures and roles in light of the convergence of voice and data communications.	In process	DHS officials stated that the creation of the Office of Cybersecurity and Communications acknowledges the increasing convergence of the IT and Communications Sectors. Further, DHS officials stated that NCS and NCSD are working closely together to ensure that activities are coordinated, issues are jointly addressed, and the resources and expertise of each organization are utilized. Moreover, the officials stated that the Office of Cybersecurity and Communications is working to co-locate the US-CERT and the NCC watch operations centers to ensure that IT and communications experts are working side-by-side to share situational awareness information and foster the early identification of attack trends, as well as the implications of these attacks, across all infrastructure sectors. We are currently evaluating DHS's efforts to restructure its organization in light of the convergence of voice and data communications.

Recommended Actions	Status	DHS Progress
Identify the relationships and interdependencies among the various Internet recovery-related activities currently under way in NCS and NCSD, including initiatives by US-CERT, the National Cyber Response Coordination Group, the Internet Disruption Working Group, the North American Incident Response Group, and the groups responsible for developing and implementing cyber recovery exercises.	Not completed	DHS has reported the roles and responsibilities of its multiple working groups and initiatives, but has not fully described the relationships and interdependencies among the various Internet recovery-related activities currently under way.
Establish timelines and priorities for key efforts identified by the Internet Disruption Working Group (IDWG)	Not completed	DHS disbanded the IDWG because its functions are to be addressed by the IT and Communications Sector Specific Plans and the Cross-Sector Cyber Security Working Group. DHS officials reported that they may reconstitute the IDWG in the future if needed to address Internet resilience objectives that are not covered by other existing organizations.
Identify ways to incorporate lessons learned from actual incidents and during cyber exercises into recovery plans and procedures.	In process	DHS officials stated that they developed a Cyber Storm After Action Report, which was used to revise the NCRCG's operating documents, and the lessons learned were taken into account in the development of Cyber Storm II. DHS officials stated that exercises such as Cyber Storm and Cyber Tempest, as well as data from the Katrina After Action Report have been used in updating the *National Response Framework*. However, DHS has not yet developed a formal process for incorporating the lessons learned.
Work with private sector stakeholders representing the Internet infrastructure to address challenges to effective Internet recovery by: • further defining needed government functions in responding to a major Internet disruption (this effort should include a careful consideration of the potential government functions identified by the private sector earlier in this testimony), • defining a trigger for government involvement in responding to such a disruption, and • documenting assumptions and developing approaches to deal with key challenges that are not within the government's control.	In process	DHS officials stated that there are a number of ongoing initiatives within the department that seek to address the challenges to effective Internet recovery. • DHS reported that the strategic partnerships formed through the IDWG, the framework of the NIPP, implementation of the sector specific plans, the National Cyber Response Coordination Group, and operational activities conducted by US-CERT are helping to define the appropriate government functions in responding to a major Internet disruption. • An IDWG study examined the existence of incident triggers for responding to Internet disruptions and concluded that triggers or response thresholds vary from one private sector organization to another and that overall, the establishment of triggers would hold little value for infrastructure owners and operators. The study revealed that the development of triggers for the federal government could be useful if used across departments and agencies. Currently, US-CERT's incident levels provide the response categories that should guide department and agency involvement in responding to incidents. Moreover, the study demonstrated the need for greater understanding as to what the federal response would be in the event of an Internet disruption. • Agency officials stated that DHS is collaborating with the private sector to better understand existing operational and corporate governance policies. DHS acknowledges that more needs to be done to fully address these challenges.

Source: GAO analysis of DHS provided data.

In summary, as a critical information infrastructure supporting our nation's commerce and communications, the Internet is subject to disruption—from both intentional and unintentional incidents. While major incidents to date have had regional or local impacts, the Internet has not yet suffered a catastrophic failure. Should such a failure occur, however, existing legislation and regulations do not specifically address roles and responsibilities for Internet recovery. As the focal point for ensuring the security of cyberspace, DHS has initiated efforts to refine high-level disaster recovery plans; however, much remains to be done.

DHS faces numerous challenges in developing integrated public/private recovery plans—not the least of which is that the government does not own or operate much of the Internet. In addition, there is no consensus among public and private stakeholders about the appropriate role of DHS and when it should get involved; legal issues limit the actions the government can take; the private sector is reluctant to share information on Internet performance with the government; and DHS is undergoing important organizational and leadership changes. As a result, the exact role of the government in helping to recover the Internet infrastructure following a major disruption remains unclear.

To improve DHS's ability to facilitate public/private efforts to recover the Internet in case of a major disruption, we suggested that Congress consider clarifying the legal framework guiding Internet recovery. We also made recommendations to DHS to establish clear milestones for completing key plans, coordinate various Internet recovery-related activities, and address key challenges to Internet recovery planning. While DHS has made progress in implementing these recommendations, full implementation could greatly enhance our nation's ability to recover from a major Internet disruption.

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

If you have any questions on matters discussed in this testimony, please contact me at (202) 512-6244, or by e-mail at wilshuseng@gao.gov. Other key contributors to this testimony include Scott Borre, Vijay D'Souza, Nancy Glover, Colleen Phillips, and Jeffrey Woodward.

Mr. CLAY. Thank you very much. Mr. Ross, you may proceed for 5 minutes.

STATEMENT OF DANIEL S. ROSS

Mr. ROSS. Thank you, Chairman Clay and distinguished members of the subcommittee. I thank you for inviting me here to day to appear before you in both my role as Missouri State chief information officer, and also as a member of NASCIO, the National Association of State Chief Information Officers. NASCIO is a not-for-profit, non-partisan research and advocacy organization, of which I and most State CIOs are members.

I will briefly offer my perspective on efforts to secure my State and our Nation's Internet infrastructure. A lapse or shutdown of Internet availability would disable much of State government, rendering it unable to communicate, to deliver services and collect revenue for an extended period.

Regional conditions in Missouri illustrate some of the challenges natural disasters may pose. A large portion of eastern Missouri, including the city of St. Louis, lies in close proximity to the New Madrid earthquake fault. Missouri experienced over 200 tornadoes last year. In addition, we experienced ice storms, thunderstorms and flooding which damaged communications infrastructure.

In addition, the sheer pervasiveness and relentlessness of cyber-attacks is staggering. In the past fiscal year alone, Missouri's network and data center experienced nearly 5.6 million cyber-attacks. That's 29,000 per day, about 1,200 an hour. And in the few minutes that I am speaking with you today, we will experience about 100.

The evolving nature and sophistication of cyber-attacks is worrisome as well. State information technology infrastructure is now specifically targeted by criminal elements connected to organized crime. In addition, they are also increasingly international in origin, which makes apprehension and criminal prosecution highly unlikely.

What are we doing? In response to this, State CIOs are forging partnerships with State, Homeland Security, emergency management and public safety officials to plan for the potential of major disruptions and security breach events. We are also trying to secure the funding necessary to maintain our intrusion detection, spam filter and other technologies that were purchased previously with Homeland Security one-time grant funds.

A current concern State CIOs face is acquiring funding to build security and resilience into all new IT projects and to hire and retain knowledgeable, trained IT staff.

Some recommendations to fortify Internet communications infrastructure. First, there must be increased intergovernmental and private sector coordination. Business partners, stakeholders and all levels of government must coordinate actions, share best security practices, and plan for the potential of a major disruptive event.

Second, continued State involvement in the National Infrastructure Protection Plan and Cyber Security Information Technology Sector Specific Plan within it is essential.

Third, we must identify cyber vulnerabilities and fund their mitigation. Cyber security is not a tangible asset, and Federal pro-

grammatic funding rarely includes specific provisions for IT spending to protect Federal programs delivered by States. The creation of a funding pool for cyber security grants to specifically assist States in achieving a proper cyber security posture would be beneficial in raising the overall security level of critical IT infrastructure in the State government sector.

Fourth, we must include and address Internet dependent critical State functions and continuity of operations and recovery plans.

And finally, we have to partake of information sharing initiatives between NASCIO, the Multi-States Information Sharing and Analysis Center and Federal agencies.

In conclusion, Mr. Chairman, technology alone will not solve the security challenges that States face while trying to protect key information technology systems and information given the wide variety of cyber-attacks and security vulnerabilities today, it may be only a matter of time before a State's information systems and assets are compromised. Therefore, it is imperative that an investment in human and technology resources be an ongoing, proactive process, and not a reactionary response to a security event. The well publicized hard costs of security breaches as well as the soft costs of losing citizen confidence drive the need for providing sufficient resources for securing Government's information and infrastructure assets.

As CIO for Missouri and as a representative for NASCIO, I appreciate the work of this subcommittee in addressing this national challenge. The National Association of State Chief Information Officers stands ready to contribute to this subcommittee in a meaningful way as needed.

Thank you for your time.

[The prepared statement of Mr. Ross follows:]

TESTIMONY OF DAN ROSS
CHIEF INFORMATION OFFICER, STATE OF MISSOURI
MEMBER OF THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

TUESDAY, OCTOBER 23, 2007

Chairman Clay, Ranking Member Turner, and distinguished Members of the Subcommittee:

As a representative of the State of Missouri and member of the National Association of State Chief Information Officers (NASCIO), I thank you for inviting me to appear before the U.S. House of Representatives Subcommittee on Information Policy, Census, and National Archives today to offer my perspectives on efforts to secure our nation's Internet infrastructure and to present recovery and response efforts in the event of an Internet disruption. I appreciate the Subcommittee's attention to this important matter and willingness to get input from my viewpoint as the chief information officer (CIO) of the great State of Missouri and from the national perspective as a member of NASCIO.

As background, as the CIO for the State of Missouri I am responsible for the state's Information Technology Services Division, which is the central point for coordinating the information technology policies for the executive branch. The division also promotes economy and efficiency in the use of information technology (IT) and telecommunications for transaction of state business. In addition to my role as the Missouri State CIO, I have been an active member of NASCIO since 2004. NASCIO is the research and advocacy organization representing our priorities and interests. Founded in 1969, NASCIO is a not-for-profit, non-partisan association representing state CIOs and information technology executives from the states, territories, and the District of Columbia. The activities of this association are important because, in most cases, the state CIO is appointed by the Governor and the CIO has executive-level and statewide responsibility for information technology leadership.

As you are undoubtedly aware, the state's critical IT infrastructure, including the Internet, has become an indispensable tool vital to government business, the economy, citizens and national security. It has become the primary method by which the Missouri public receives information

from, or sends information to, government. The public's use of the Internet has replaced much of the traditional walk-in, mail-in, and phone-in structures that had been used throughout our history.

However, this more efficient and effective method of providing public services is not without risk. At the state level, disruption to critical IT applications, systems or a more wide-spread attack on the Internet could hinder, or completely disable state government in day-to-day operations. This could have a severe impact on those among us who are most in need. First responders may not be able to communicate with each other or with citizens during a natural or man-made disaster when time could cost human lives. Critical communications with other levels of government, especially local government jurisdictions, may be disrupted. Vital state-local communications may not be able to relay disease outbreak information in the event of a public health crisis or communicate with the Centers for Disease Control (CDC). A lapse or shutdown in Internet availability would disable a vital state-to-local communications mechanism that supports human services, public safety, revenue collections and many other functions that are state-administered and locally-delivered or purely local programs delivered to citizens via the Internet. The state may not be able to process and deliver important benefits such as family services, food stamp processing and health services to children. Citizens expect government to be at its best when their personal situation may be at its worst.

The regional conditions in my own state illustrate these challenges. A large portion of Eastern Missouri, including the city of St. Louis, sits in close proximity to the New Madrid earthquake fault; so we must remain cognizant of the catastrophic effects that an earthquake could have on the State's telecommunications capabilities. Missouri's capabilities for incident and disaster response depend heavily on the Internet and other wireless connectivity for the exchange of information with mobile response teams.

We must also acknowledge that the Internet was not designed to support the many activities such as public safety and vital health systems that currently rely on it for secure and reliable connectivity. This was emphasized during the past year when major telecommunications outages in Springfield, due to an ice storm, and in St Louis, due to a severe thunder storm, revealed that the State of Missouri is not yet sufficiently prepared to handle major outages to the public voice and Internet network. During these incidents voice communications were nearly impossible, Internet web sites were disabled and cellular communications were severely disrupted during a time when a large number of citizens needed responsive and reliable communication services.

As the nation becomes increasingly Internet and technology dependent, the need to avert a prolonged, large-scale loss or disruption of critical IT infrastructure or the Internet due to a cyber attack, natural disaster, or terrorist incident, becomes as basic as securing our homes, borders and modes of mass transportation. Technology is the common thread among the multiple sectors of the nation's critical infrastructure that provides these sectors' communications and processing capabilities. It allows all of the sectors, from financial institutions, to the energy sector, to the transportation sector, to function reliably and efficiently. However, should an Internet or network disruption take place, it is essential that we have effective and well-coordinated processes in place to ensure successful and rapid restoration of critical IT systems and applications as well as the Internet.

My testimony today will cover such themes, as well as discuss the role of the state CIO in addressing these matters for the enterprise of state government and NASCIO's perspective on the cyber security challenges facing our nation.

Role of the State CIO in Internet Disruption Prevention and Response

With an enterprise view of technology policy development, implementation and management, the state CIOs have emerged as key state resources in preventing and developing plans to respond to Internet and network disruptions. While it is difficult to derive a single organizational CIO "model" from the 50 states, protecting the Internet from increasingly virulent cyber threats, maintaining the continuity of critical state IT functions in the event of a disruption or attack, and seeking quick and effective solutions for Internet recovery in the event of a disruption are all intrinsic extensions to the state CIO's role. This is done in coordination and partnership with other state agencies and appropriate federal counterparts.

Missouri established a Cyber Security Office that works closely with our State Homeland Security Office and the U.S. Department of Homeland Security (DHS). We were also one of the founding states in the Multi State-Information Sharing and Analysis Center (MS-ISAC). Two members of my Cyber Security Office are heavily involved with this organization with one co-chairing the Legislative Committee and the other serving on the Operations Committee. Our involvement with the MS-ISAC has greatly facilitated the sharing of information and the tracking of activity that could be harmful to the state.

Disruption Prevention: Addressing the IT Threat Landscape

Cyber security is a critical concern of the state CIOs and is consistently a high priority agenda item of my state colleagues. IT security is not only necessary to preserve the states' ability to effectively serve citizens and preserve the privacy of personally sensitive information within the state IT infrastructure, but is a necessary component in securing our nation's Internet infrastructure. Effective IT security is also a foundational component for the technology that enables many homeland security functions.

Fortunately, in the past, Missouri has received State Homeland Security Grant funding from DHS, a portion of which were used to purchase the majority of the technology my organization currently uses to protect our systems from cyber attacks. Unfortunately, we are now struggling to obtain the dollars necessary to maintain the intrusion detection, spam filters and the other technologies originally purchased with the Homeland Security grants.

I know that each of you recognizes that today's IT security domain is in a constant state of evolution as new security threats are created and criminal elements on every continent are seeking to do us harm. Threats to the IT infrastructure are on the rise and hacks, botnets, Trojans, viruses, worms, Denial-of-Service attacks and other suspicious Internet activity continue to compromise the integrity of the Internet and the availability of critical state IT systems and applications. With many IT systems interconnected with each other and to the state

backbone, one incident, in one agency, has the capability to have a widespread impact on state government and beyond.

The sheer pervasiveness of the threats is staggering:

- In Missouri, in FY 07, there were 10,572,000 attacks on the state network and data center – an average of 29,000 per day. Our filters and firewalls block or intercept an average of 327,318 spam emails, 1,701 e-mail viruses and 5,209 web server take-over attempts daily.
- Another state in the Midwestern region has reported 777,606 "high severity" attacks over a three month period from July 2007 through September 2007. Over 80% percent of these "high severity" attacks were brute force attacks against state computer assets. For the same time period, the state reported 2,155,456 "medium severity" attacks, and 4,161,870 "low severity" attacks.
- In Michigan, on an average day, the state blocks 22,059 spam emails; 21, 702 e-mail viruses; 4,239 web defacements; and six remote computer take-over attempts.
- On an average day in Texas state government, there are reports of almost 250 ***successful*** attacks against the state's information resources. A major computer security incident that has significant financial and operational impacts is an annual event for most Texas organizations. Cyber-terrorists, spies, hackers, and thieves are not just targeting Texas computers, though. They are targeting the information that the state's networks store and transmit.

Moreover, the nature of the threats is more worrisome than ever due, in part, to the growing sophistication of attacks. Instead of being targeted by teenage hackers who just want to see which systems they can crack, state IT infrastructure is now being purposefully and maliciously targeted by criminal elements that are increasingly connected with organized crime. They also are increasingly international—attacking state government technology from foreign countries half-way around the globe. These criminals operate for a profit and in an environment where getting apprehended and criminal prosecution are highly unlikely. These trends identified by state security experts are supported by recent findings contained in the CSI (Computer Security Institute) /FBI (Federal Bureau of Investigation) 2007 Security Survey of entities from across the public and private sectors. The study found that financial fraud has overtaken viruses as the greatest source of financial losses and almost one-fifth of survey respondents who had suffered attacks had characterized the attacks as "targeted" to their organization or a subset of organizations.

While many attacks originate from outside state government, there has been rising concern in recent years over attacks and disruptions that originate from within state government. More employees across public and private sectors use technology to carry out their responsibilities and work on-the-go with mobile devices that connect back to workplace IT systems. Major break-downs, disruptions and even purposeful and malicious attacks can arise from within an organization. And, even a major power outage or failure of the electrical grid can impact IT systems on a regional basis.

IT Infrastructure and Internet Disruption Response: Continuity of Critical Operations and Internet Recovery

A key component of responding to an Internet and critical IT system disruption is effective planning and coordination. State CIOs are typically responsible for developing and maintaining the statewide communications infrastructure that supports multiple public agencies and institutions, and should be an integral part of any IT planning and coordination process. Increasingly, state CIOs and their IT security personnel forge partnerships with state homeland security, emergency management, law enforcement and public safety officials to plan for the potential of major disruptions and security events. State CIOs are not however, directly responsible for Internet restitution, which is in the hands of private sector carriers providing these communication services under contract to the state.

While state CIOs do play an important part in the security of state IT infrastructure and managing security incidents when they occur, many challenges are associated with this role. For example, some states have greater authority over state agency IT security than others. In states where the CIO may not have explicit authority over the security and resilience of critical IT systems, it may be more difficult for the state CIO to be the primary leader should those systems encounter a severe disruption. Another concern is that funding is necessary to purchase the appropriate security tools, build-in security and resilience into all new IT projects and hire and retain knowledgeable and trained IT security personnel. State IT security competes with other priorities and may suffer if funding is not adequate or sustained over time.

Recommendations for Improving Upon Current Efforts

In conclusion Mr. Chairman, I would like to provide the Subcommittee with some recommendations for improving upon efforts that are currently underway. As with most problems, there is no single overarching solution. There are however, a number of important recommendations that should be considered at the federal, state and local level to address Internet and IT infrastructure fortification efforts and to ensure that critical government operations can be quickly restored in the event of a disruption, especially one caused by a cyber attack.

Internet and IT Infrastructure Fortification

1. Increased Intergovernmental and Private Sector Coordination: While many at all levels of government are securing their critical IT infrastructure and use of the Internet, forums for the sharing of best practices and the facilitation of inter-governmental security efforts are needed. With more and more IT systems connected to the Internet and connected to each other, we can no longer view security from a narrow, single-organization perspective. Business partners and all levels of government must coordinate to share their best practices and plan for the potential of major, disruptive events.
2. Continued State Involvement in the National Infrastructure Protection Plan (NIPP) and the Cyber Security IT Sector Specific Plan (IT SSP) within it: The NIPP strategy has gone to great lengths to provide instructions on how to mitigate potential attacks that could disrupt government operations in general or homeland security-related, mission-critical systems specifically. In addition, it has helped in setting national preparedness

priorities, identifying responsible parties for specific tasks, and will help to effectively allocate funding and resources to critical infrastructure in need.

3. Identify and Fund Cyber Vulnerabilities: Cyber security is not a tangible asset, and thus, is often not considered a high priority in funding decisions. Federal programmatic funding most often does not include specific provisions for IT security spending to protect federal programs delivered by states. Because of this reality at the state level, there are gaps and inconsistencies in the levels of cyber preparedness. Such gaps make some states and regions more vulnerable to a cyber attack of state systems or Internet disruption. The creation of a funding pool for cyber grants to specifically assist states in achieving their desired IT security posture would be beneficial in raising the overall security of critical IT infrastructure within the state government sector.

Internet and IT Infrastructure Recovery Planning and Coordination

1. For planning purposes, a baseline effort is needed that would assist in prioritizing state government services that demand priority attention in the event of a major incident. Make a list of critical state functions that are Internet-dependent. High priority functions that are critical to citizens in need and the most basic governmental functions include:
    - Emergency Response and Communications
    - Communications with First Responders
    - Intergovernmental Coordination during an Emergency
    - Delivery of Human Services (including WIC, food stamps, TANF and other programs intended for those in need)
    - Homeland Security and Public Safety
    - Public Health
    - Communicating with Citizens
    - Law Enforcement, Corrections and Administration of Court Systems

2. Address Internet dependent critical state functions in state continuity of operations and recovery plans
3. Engage with critical private sector entities such as telecommunications carriers, Internet service providers, financial institutions and major IT vendors as well as other levels of government to ensure that physical Internet infrastructure restitution plans have been laid out. A lack of clarity on the roles that the government and the private sector must each play in Internet and critical system restoration is a major weakness. Citizens expect government—whether at the federal, state, or local level—to work with the private sector and with each other when necessary. Internet and IT system restoration councils made up of relevant public and private sector entities should be established to encourage collaboration and increase clarity in the roles that each sector must play.
4. Partake in information sharing initiatives with NASCIO and the MS-ISAC. NASCIO plays an advocacy role with respect to cyber security policy and the role of the state CIOs in protecting critical parts of the nation's critical infrastructure. NASCIO also seeks to ensure that states are integrated with and can provide insight and expertise regarding federal-level cyber security efforts. The MS-ISAC plays a role in coordinating among the states to share threat information and best practices for securing states' IT infrastructure.

Concluding Remarks

Technology alone will not solve the security challenges that states face while trying to protect key IT systems and information. Security is highly dependent on policies for information handling coupled with appropriate and reinforced education for all state personnel--not just the information technology staff responsible for handling and protecting the state's information assets. Given the wide variety of security vulnerabilities today, it may only be a matter of time before a state's information systems and assets are compromised. Therefore, it is imperative that an investment in human and technology resources be an ongoing, proactive process; not a reactionary response to a security event. The well-publicized hard costs of security breaches, as well as the soft costs of losing citizen confidence, drive the need for providing sufficient resources for securing the government's information assets and infrastructure.

As the CIO for the State of Missouri and as a representative of NASCIO, I appreciate the work of the Subcommittee in addressing this national challenge. NASCIO is a willing partner in advancing efforts to secure our nation's Internet infrastructure and stands ready to contribute to the Subcommittee in a meaningful way, as needed.

Mr. CLAY. Thank you so much for your testimony, Mr. Ross.

We will start the first round of questions and the gentleman from New Hampshire is recognized for 5 minutes. Mr. Hodes.

Mr. HODES. Thank you, Mr. Chairman. And thank you for holding this very, very important hearing. Given the Information Age that we are living in, there probably is nothing that is more important these days in some way to the security of this Nation than the issues that we are discussing today. As the use of the Internet and cyberspace blossoms, it is becoming ever more important to us.

Mr. Garcia, I noted with appreciation your sense of regret that your testimony wasn't supplied earlier to us, and I take that you will be able to take steps in the future so that when you come back before us, we will have enough time to review your testimony.

Mr. GARCIA. Absolutely, sir. We do strive to give you the best quality product we can, as well, which may account for some of the delay and the review process.

Mr. HODES. I appreciate that. Prior to your appointment, Mr. Garcia, the previous Director of the NCSD, Andy Purdy, was hobbled because there were conflict of interest questions due to his continued employment with his original employer, Carnegie Mellon University, which was involved with several DHS, cyber-related projects at the time. My understanding is that he was actually drawing a salary while working also for the NCSD, which created real problems, as you can imagine.

And it is my understanding that currently, a significant amount of the work that is being undertaken by NCSD is being carried out by other contractors. Private contractors, including Booz-Allen. As a member of the Oversight and Government Reform Committee, we have been exercising oversight in a number of areas where the Government is making significant use of private contractors, most notably in the news in connection with the war in Iraq and the flap that has developed around Blackwater.

And I understand the role of contractors in assisting agencies with program administration, but I also understand that contractors aren't supposed to play any role in inherently governmental or policy-focused activities. We recognized that as a potential conflict with Mr. Purdy, and we remain concerned that there may continue to be conflicts at the NCSD. And I note in your testimony, at pages—especially at 4 and 6, where you talk about the collaboration that exists in the public/private partnership that is ongoing.

So, there are relationships here, which while important are fraught with potential problems. Can you tell us how many full-time governmental employees there are within NCSD, NCS, and the other DHS units under your authority?

Mr. GARCIA. Sir, I don't have the exact number. We have approximately 100 individuals in NCSD and NCS, and about that number in contractors. So we do rely on contractors. It gives us the resilience we need to respond to urgent initiatives. It enables us to surge and to pull back our resources as necessary.

Mr. HODES. And when you say 100 contractors, do you mean 100 employees who are the employees of contractors, or 100 separate different companies?

Mr. GARCIA. I can give you that exact number—I can get back with you on that specifically.

Mr. HODES. I would appreciate having the documents that reflect that. And Mr. Chairman, if I may, request that the record stay open long enough to have that information submitted.

Mr. CLAY. Without objection, the gentleman will do everything to get us those records.

Mr. GARCIA. Absolutely.

Mr. HODES. Off the top of your head, who are the largest contracting entities who are supplying these contractors to those agencies of which you spoke?

Mr. GARCIA. The most number of contractors from any one organization, I cannot be certain on that answer, likely to be Booz-Allen.

Mr. HODES. And what is your sense of the size of Booz-Allen's commitment in terms of a percentage of that number of approximately 100 who are working?

Mr. GARCIA. I can get that for you, as well.

Mr. HODES. You don't have any sense today?

Mr. GARCIA. Not an accurate sense for you. No, sir.

Mr. HODES. And what are the roles and responsibilities of those contractors at your agency, versus the responsibilities of the Government employees?

Mr. GARCIA. None of the contractors are in managerial positions. So, they serve in a support role for all of our activities.

Mr. HODES. And who is supervising them? And who is responsible for their day-to-day activities? Is it the employees at your agency, or is it the providing companies?

Mr. GARCIA. The Government employees under my organization are responsible for supervising the activities that the contractors support.

Mr. HODES. May I continue with one further question, Mr. Chairman? I see my time is up.

Mr. CLAY. The gentleman is recognized for 2 additional minutes.

Mr. HODES. Thank you. Now, Mr. Garcia, I take it you would agree that conflict of interest policies are critical to ensuring the integrity of the work done for the Government?

Mr. GARCIA. Yes, sir.

Mr. HODES. And are there written conflict of interest policies in place at the agencies you supervise to ensure that those coming to work for your division remain free from decisions that may potentially impact former employers or clients? And I am talking about both full-time employees as well as consultants working under your direction.

Mr. GARCIA. Yes, sir. I believe there is. And I can get back with you on that and supply that with you.

Mr. HODES. Similarly, Mr. Chairman, I would ask that the record be held open to accept that submission.

Mr. CLAY. Without objection, and we would appreciate it if we could have it in 5 legislative days.

Mr. HODES. Thank you, Mr. Chairman. And just one final quick question. As a former lobbyist for the Information Technology Association of America, how have you yourself made sure that you are remaining free from any conflicts concerning issues of importance to your former employer?

Mr. GARCIA. My mission, Congressman, is in total support for the Department of Homeland Security and to the Nation that we protect. My former employer was a trade association, and my former employer was also the U.S. Congress. So, my mission is quite clear and that is to promote the security and resiliency and the availability of the Nation's communications and information infrastructure.

Mr. HODES. I understand that is what your mission is, and what have you done with your former employer to make sure that you yourself have taken the proper steps to ensure there is no conflict of interest?

Mr. GARCIA. We work with them. I have no conflict of interest with my former employer. We work with them as we do with any other major trade association in information technology as a major partner of the Department of Homeland Security. We cannot do our work without partnership from industry, from IT, from communications, from financial services. But they are but one of many, many stakeholders and players in this process. And I am focused squarely on our mission.

Mr. HODES. Thank you. Thank you, Mr. Chairman.

Mr. CLAY. Thank you, Mr. Hodes. Mr. Yarmuth of Kentucky, 5 minutes.

Mr. YARMUTH. Thank you, Mr. Chairman. When I listened to the testimony, it kind of reminds me of the now infamous words of Secretary Rumsfeld when he said, "There are things we know we know, and things we know we don't know, and things we don't know that we don't know."

It sounds to me like there are a lot of things about the threats facing the Internet that we know, and threats that we don't know that we know, and we don't know that we don't know. And anyone can attack this problem. Is our biggest problem in this area threats that we don't even know exist, or are we still at the point where we don't know to combat the threats we know about?

Mr. GARCIA. I think it is a matter of both, Congressman. We over the past couple of years, I believe, have made tremendous progress in terms of understanding the threats facing the Internet infrastructure. Our visibility into the Internet infrastructure is increasing.

For example, my U.S. CERT collects incident reports from private sector and Government entities. Last year, we received 37,000 reports. The year before that, 24,000 reports. Is that because the incidents are increasing or is it because the reporting is increasing? It is probably a little bit of both.

But the threat is still there. So much is happening under the radar. There are so many attacks and probes happening across our networks that we are not seeing. And so, a big part of my mission is to work with the owners and operators of those infrastructures, whether it is IT or communications or financial services, transportation, electricity, to build awareness. And to build investment in the systems and the process that will raise the level of visibility into what is happening in our networks so that we can take the steps to mitigate them.

Mr. YARMUTH. Is that ultimately the measure of whether you are successful or not? Whether the incidents that you know about are reported to you are declining? Or is there some other metric that

you can come up with to allow you and us to know whether we are actually making progress?

Mr. GARCIA. Yes, sir. We have many metrics, and none of them taken by themselves is going to be sufficient. Increasing the number of incident reports. That is a measure of success. That means people are paying attention and they are reporting it. They are sharing sensitive information.

The amount of investment is also a measure of success, the investment in cyber security and information technology is increasing. We are looking at the number of students going into information security as a curriculum pursuit in universities.

So, there are many measures, but we still are not going to be able to measure all the attacks that are happening without our seeing them. The threat is constantly evolving. The adversaries are very sophisticated. And we have to evolve with them.

It is an ongoing technological chess match, if you will, except that there is no check mate. So, this is going to be ongoing. And we can take one measure at a time, and measure our success and hope that we don't take any steps back.

Mr. YARMUTH. I am curious also, and this may not even be related to—well, it relates to a certain extent, to the ultimate goal of the hearing. But the issue of motivation. Is there any way to gauge whether these—what percentage of the attacks are motivated by people who just want to see if they can figure it out? Kind of intellectual curiosity or whether they actually have evil motives, if you will. Evil intent.

Mr. GARCIA. I will let Mr. Wilshusen elaborate, but I think what we—and indeed Mr. Ross, since he is also on the front lines—but we do see a variety of motives. It used to be that hacking, as it were, was very much a joy ride exercise. Teenagers seeing what they can get away with. Motivations related to "hactivists"—those relating to political motives, as perhaps what we saw in Estonia.

But the adversaries are becoming more sophisticated and more focused on very specific targets. And that includes the desire for information, whether it is from companies or from governments. It includes the pursuit of money through cyber crime, through financial services networks or through identity theft.

So, they are becoming very sophisticated and very targeted with multiple intents.

Mr. YARMUTH. Mr. Wilshusen.

Mr. WILSHUSEN. Yes. And I would just like to add, too—I agree with everything that Mr. Garcia just mentioned regarding the threats—is that there are criminal activities and criminal elements out there that do have a financial motivation.

In addition, there are also foreign nation-states that also have an interest in obtaining intelligence information about their potential adversaries, including, of course, the United States.

I would also like to point out, too, that the threat is evolving and indeed the vulnerabilities are also increasing. Just to give you a statistic, the National Vulnerability Data base has identified over 26,000 software flaws or mis-configurations that could be exploited to provide an avenue for someone to gain unauthorized access. That total, according to the National Vulnerability Data base, is increasing by 16 every day. The vulnerabilities are legion. The

threats are adaptive, and they are constantly evolving, and it is quite a challenge to be able to protect computer systems against that.

Mr. CLAY. Thank you.

Mr. YARMUTH. Thank you, Mr. Chairman.

Mr. CLAY. Thank you, Mr. Yarmuth. Mr. Wilshusen, since the original GAO Report on Internet Infrastructure and Recovery Plans came out last year, can you identify the areas in which DHS has demonstrated significant progress? How about the areas in which progress is lagging or that have been just totally ignored?

Mr. WILSHUSEN. Yes, sir. Well, as Mr. Garcia mentioned in his opening remarks, some of the areas for progress included that DHS released its Sector Specific Plans for the IT and Communications Sectors. It also developed and revised its National Response Plan or framework to assure and make sure that it addresses cyber incidents that require Federal response.

In addition, DHS has also led these private/public exercises, Cyber Tempest, Cyber Storm, that examine response and coordination mechanisms to simulated cyber events. These exercises add value. And the after action reports provide useful information on lessons learned during those exercises. Of course, the next step though is taking those lessons learned and actually implementing them into the plans.

Now, some areas where DHS is lagging, if you will, is that it has not yet developed a private/public plan for Internet recovery. Nor has it set a date when that plan would be completed.

In addition, DHS also disbanded the Internet Disruption Working Group, and it is not clear exactly how well that group's functions and responsibilities will be addressed by other groups that DHS is working with.

And one other thing. As Mr. Garcia mentioned, there are a number of working groups addressing this area of Internet recovery. However, the interrelationship among these groups is not certain.

Mr. CLAY. Have there been appropriate triggers established to determine what type of Internet disruption would merit a Government response?

Mr. WILSHUSEN. Well, there have been efforts, I believe. A couple of the working groups have looked at those triggers, but as of now, the specific triggers have not yet been fully developed or implemented.

I might also want to point out, too, that one of the key aspects in order to make these triggers work is to make sure there is an effective analysis and warning capability. And DHS does have, for example, U.S. CERT, and as Mr. Garcia mentioned earlier, the use of the Einstein network monitoring tool, which can help provide information supporting those triggers. But Einstein has not yet been implemented across the Government.

Mr. CLAY. Thank you for that. As part of GAO's review of DHS' Internet recovery responsibilities, it cited a lack of DHS leadership and stability throughout its management ranks. Has this improved since the report was released last year?

Mr. WILSHUSEN. Well, one area where it has improved is indeed the appointment of Mr. Garcia as the Assistant Secretary for Office of Cyber Security and Communications, and the Assistant Sec-

retary has spelled out some key priorities for the Department, including preparing and deterring attacks, responding to cyber-attacks of potentially national importance or significance, and also building awareness among the various different stakeholders in cyber security.

However, DHS continues to be hampered by its inability to retain key officials in the cyber security area. For example, the Director of the National Cyber Security Division has recently left, as have other key officials related to cyber security control systems and officials responsible for cyber-related exercises.

Mr. CLAY. Thank you so much for that. Mr. Ross, as the CIO from Missouri, has your office sought to prioritize the State networks and critical infrastructures that are most critical in an emergency incident? And if so, how was it done?

Mr. ROSS. Yes, sir. We are always looking to find that single point of failure, which if taken out, will take the whole system down. You know, we have identified the essential functions Government has to do, which is communicate, pay people, pay bills, buy things, provide medical services, direct people in emergencies and so, in working with the Department of Homeland Security, the State Department of Homeland Security, the State emergency management folks, we are putting together a plan to do that.

Now, in my own shop and the IT folks, we have identified vulnerabilities in the State network and we are working to patch those. We have recently signed a contract with AT&T to manage the State-wide network to give us that resiliency and that disaster recovery ability because of their large network and their redundancy.

So, that in combination with State assets—which do include 1,700 miles of fibers that the Highway Department owns, that we leverage for them—all come together to give us a resilient backbone to keep running in times of emergency.

We are not there yet because we have just signed the agreement with AT&T and are moving into that relationship with them. But I look forward to that. That will provide not only the tremendous wide highway to operate on, but also the back-up and disaster recovery we have been after.

Mr. CLAY. Thank you. What are the greatest strengths and weaknesses of the Multi-State ISAC? Are its activities related to information sharing and threat analysis of cyber incidents providing you with adequate information for decisionmaking?

Mr. ROSS. Mr. Chairman, Missouri is one of the two founding States in that organization. We are extremely active in that. One of my security officers is co-chair of the Legislative Committee and another member of his team is on an Operations Committee, I believe.

So, we are actively engaged with them, in contact with them nearly every day. Phone calls and then certainly when an event or a vulnerability is identified, that network fires up very quickly. So, we depend on and use them very heavily.

Mr. CLAY. OK. Thank you for that. Mr. Hodes, did you have a second round of questioning? Please proceed for 5 minutes.

Mr. HODES. Thank you, Mr. Chairman. Mr. Wilshusen, I am looking through the statement you provided, your testimony here.

And I note on pages 9 and 10, in dealing with the questions of the existing laws and regulations and their application to Internet recovery, some issues arise.

You point out, for instance, that the Stafford Act authorizes Federal assistance to States, local governments, not-for-profits, in the event of a major disaster or emergency, but doesn't apply to for-profits.

Do you see a revision of that as necessary, desirable? Something else, is it absolutely required? Would it provide an incentive for some kind of conduct on the part of for-profits, which has been problematic up until now? Would you comment? Thanks.

Mr. WILSHUSEN. Yes, I would be glad to. During this review that we conducted last year, we did a number of case studies over key Internet cyber events. One of them had to do, of course, with Hurricane Katrina. And it was during that event where key infrastructure owners needed to gain access to the resources or to their facilities and have the ability to have basic food, water and other necessities in order to more quickly restore service operations—their service capabilities.

However, the Federal Government was not able to help them or to provide the short-term tactical support that was needed in order for them to actually gain access to their facilities. And so, part of that was due to the Stafford Act, because the Federal Government cannot provide assistance to these for-profit organizations.

Mr. HODES. So, had the Federal Government been able to provide that short term tactical assistance, the response of those for-profits in coordinating the effort to recover, would have been much quicker?

Mr. WILSHUSEN. And would have been enhanced. Yes, sir.

Mr. HODES. Turning to the Communications Act of 1934, there is an implicit suggestion in your written statement that needs to be revised to address the new threats, the new concerns, that the cyber infrastructure has created since 1934 and whatever amendments there have been. Am I correct that you see that as something that Congress needs to look at?

Mr. WILSHUSEN. Yes, because we see that as a Communications Act that does not address specifically the Internet and certainly not the roles and responsibilities for Internet recovery from disruptions or major disruptions.

Mr. HODES. Thank you. Mr. Garcia, it was recently reported that one vendor, a major DHS IT vendor, Unisys, had been concealing a number of significant cyber security incidents and attacks on Department systems, including many that apparently exposed the entire DHS enterprise to significant cyber-threats. Could you explain your role in responding to the incidents as they were reported to DHS leadership?

Mr. GARCIA. Sir, that particular issue, we have a separation of responsibilities. The Office of Cyber Security and Communications is responsible for a national outreach on cyber security policy and implementation, whereas the protection of the DHS network itself, that responsibility resides within the Office of the Chief Information Officer [CIO]. So, neither I nor was my office was directly involved in that particular issue.

Mr. HODES. So, it is not your job?

Mr. GARCIA. That is correct.

Mr. HODES. Did you coordinate at all with the Chief Information Officer on what happened?

Mr. GARCIA. Yes. So our role within the U.S. CERT is in fact, to treat the DHS networks as we do all of our Federal agency customers, if you will, particularly through our outreach and information sharing in the Einstein program, we work to try to help agencies see what is happening on their networks and to exchange information with them and ultimately to correlate activities to find trends that are happening across the Federal network. And that goes with the CIO's office as well.

So, we are in close contact with the Office of the CIO as incidents happen, in the DHS networks or any other Federal agency network.

Mr. HODES. So, I am assuming that because it is an agency with which you are involved and that you must be in touch with the CIO about these kinds of incidents, what happened to Unisys? What was done? Were they sanctioned? And what steps were taken by the CIO to prevent these kinds of incidents from happening in the future?

Mr. GARCIA. I certainly would defer to the CIO to answer those questions for you, as I was not directly involved in that.

Mr. HODES. May I just followup for one quick moment?

Mr. CLAY. Please. Go ahead.

Mr. HODES. Did you have any conversations with the CIO about what was going on with this breach by Unisys and how it was being handled and what effect it would have on the agencies that you do deal with?

Mr. GARCIA. Our U.S. CERT facility was in contact with his office, and I can get back with you as to exactly what the interaction was. I personally was not involved. That also deals with a contracting matter with the CIO's contract with Unisys.

Mr. HODES. So, to the extent there are any documents within your purview, control, constructive control, or custody, I would like you to provide to this body any and all documents reflecting any interaction, discussion or contact you or your agency, or anybody in it had with the CIO about the response to Unisys over this breach. Will you provide that to us?

Mr. GARCIA. Certainly.

Mr. HODES. Mr. Chairman, I request that the record stay open so that those documents may be provided.

Mr. CLAY. Without objection, for 5 legislative days.

Mr. HODES. Thank you, sir. Thank you, Mr. Garcia.

Mr. CLAY. Mr. Yarmuth.

Mr. YARMUTH. Just one followup question. And this is mostly for my own understanding. I would like to try again to clarify the difference between for-profit and the not-for-profit world. And also, the difference between the infrastructure world and the software world, because presumably most of the software out there is produced by for-profit companies and you have a security aspect of the software and a security aspect of the infrastructure. I am just curious as to where you draw the line as to where the Government's interest and responsibility begins and where it ends.

Mr. GARCIA. If I understand your question, the way we look at it is that 85 percent to 90 percent of the critical infrastructure is owned by the private sector. So, they are managing the networks and the private sector is developing the hardware that runs on and runs those networks. It is our job to coordinate with those who are owning and operating and those who are using those systems to ensure that we have a proactive way of dealing with attacks and vulnerabilities as we find them.

Mr. YARMUTH. What I am trying to understand the difference between the relevance of for-profit and not-for-profit where the Stafford Act issues arise.

Mr. GARCIA. I am not exactly sure of the answer to that question, sir.

Mr. YARMUTH. OK. Well, I am not sure that I know enough to ask any more. Thank you.

Mr. CLAY. OK. The gentleman yields back. Mr. Garcia, Mr. Wilshusen pointed out that one of the issues that your Department has is retaining key officials in cyber security. What do you think is the solution to the revolving door there? What are the main issues and why do you lose so many key people?

Mr. GARCIA. Thank you, sir. I honestly would not characterize it as a revolving door. In fact, some of our more recent departures were strictly for personal reasons. Two major staff wanted to relocate closer to family across country and south of here. And to be honest, the DHS environment and our mission is a very high intensity one, and very fast paced and long hours. And given that, we make every effort to first recruit the best talent we can and then to retain them, and to reward them, and to make their experiences and their challenges meaningful.

So, we are acutely aware of the need to have the best talent we can and we are actively filling those posts that have been vacated.

Mr. CLAY. Are many leaving for private corporate cyber security positions?

Mr. GARCIA. I am not sure exactly where they went. Probably to the private sector, but more toward a different way of life, closer to family.

Mr. CLAY. I see. Let me go another direction. According to GAO's 2006 Report on Internet Infrastructure, one of the significant obstacles facing DHS is the conflicting or overlapping roles of the National Cyber Security Division and the National Communications System, which seems to have undefined and conflicting roles in response to a major Internet disruption or cyber-attack. As the person in charge of both the NCSD and NCS, can you explain to us how the roles and responsibilities of both units are distinct or different?

Mr. GARCIA. Absolutely. Very good question. The National Cyber Security Division is responsible for the security of the information infrastructure. The National Communications System is responsible for ensuring that the Government, that the Nation, has the ability to communicate in times of national emergency.

So you think of the NCS and communications as the pipe, the telecommunications pipe, and the NCSD as dealing with the software and the technology that controls the operations of those pipes and sends information through those pipes. So, NCSD and NCS

have very complementary roles. Certainly not conflicting. Sometimes overlapping, but overlapping for the better.

My role is to try to bring those—by the way, NCS is a 40 year old organization, and NCSD is a 4-year old organization. So they have much different histories, but they work very closely together. For example, in the Estonia distributed denial-of-service attacks, NCS and NCSD worked very closely.

Second, I am working to bring together, to co-locate the U.S. CERT operations with the NCS operations, which is called the NCC, the National Coordinating Center for Telecommunications, that is a 24/7 watch operation as well, that serves the communications infrastructure involving communications companies and Government employees.

So, we are bringing them together so that the IT and Communications can have a more synthesized view of what is happening on our information and communications infrastructures.

Mr. CLAY. Let me ask you, as voice and data transmission networks continue to converge, wouldn't combining NCSD and NCS prove to be more efficient for agency operations?

Mr. GARCIA. I think certainly a good number of the functions have already converged. That when we look at the convergence of communications from the traditional circuit switch to packet switch technology, security is going to equal availability, and availability is going to equal security. So we can't bifurcate those functions.

There are unique and distinct functions within the National Communications System and NCSD that may remain unique, but by and large, you are absolutely right, Mr. Chairman, functionally NCS and NCSD will over time converge.

Mr. CLAY. Thank you for that response. It is my understanding that NCSD recently released a draft of what it called the Information Technology Security Central Body of Knowledge, competency and functional, A Framework for IT Security and Workforce Development. Isn't this the type of work usually undertaken by the private standards-setting community, such as the ISO standards organization? How is this work unique to what has already been developed by the standards community?

Mr. GARCIA. Very good question, and I thank you for that. Yes, the Essential Body of Knowledge [EBK], is our attempt to bring together actually a number of those security skills, training skills standards that have been put out by a number of different organizations and really find the common elements among all of those. What we can do is provide as a reference for academia, for the practitioners, a synthesized set of work force skills and training standards to develop curricula or to develop training within the enterprise.

So, in no way is it intended to supplant the other private sector-developed security standards. It is instead intended to sort of deconflict among those and provide a much higher level reference for those who are trying to distinguish between one or the other type of standard that they ought to be using. So we are quite enthusiastic about it.

Mr. CLAY. OK. Thank you. Mr. Wilshusen or Mr. Ross, do you have anything else to add?

Mr. ROSS. Thank you, Mr. Chairman. I might go back to a previous point that Mr. Yarmuth mentioned. And that is the evolving nature of threats. We are always having to—what we see in Missouri is, we will see low-level threats. Low-level probes of our data center and our network. We will see hundreds of thousands of these low-level threats and probes but little variations on each other, and then at the end of that period, we will see a heavy strike on our data center in an attempt to bring down servers or communication equipment and the like.

And to get to your other point, Representative, it is not teenagers hacking anymore. It is coming from other countries. Our forensic tools can track it down to continents and to countries, and it is coming from all over the world. But it is very focused. States have extremely valuable information. Financial information, health information, driver's license, Social Security number-type information and they are after that.

A recent example I heard a presentation about. If you can just get hold of a CD copy of all the freshmen coming into the University of Missouri, either the law school of the finance school or accounting or the like, that is probably worth $2,000 going in. Then years down the road, when it is actually—when they are income-producing people, that information is extremely valuable, and that is when they use it. So that type of information is what people are after.

Mr. CLAY. Do you ever make any successful apprehensions?

Mr. ROSS. Outside the country? No. Inside the country, we do.

Mr. CLAY. OK. Mr. Wilshusen, anything to add?

Mr. WILSHUSEN. No.

Mr. CLAY. No? Thank you. I want to thank the entire panel for their testimony and answering questions. This panel is dismissed. Thank you.

As soon as this panel is up, we would like the second panel to come forward to be sworn in.

Thank you. On our second panel, we have a distinguished group of individuals who are highly qualified to address the issues associated with cyber security and Internet architecture from a variety of important perspectives.

Mr. John T. Sabo is the current president of the Information Technology Information Sharing and Analysis Center [IT-ISAC], as well as the director of Global Government Relations for CA, Inc. In addition to IT-ISAC, Mr. Sabo represents CA in a number of security and privacy focus industry organizations and is an appointed member of the U.S. Department of Homeland Security Data Privacy and Integrity Advisory Committee. Welcome.

Mr. Larry Clinton is the president of the Information Security Alliance, which has over 500 corporate members on four continents representing virtually every major segment of the economy. Mr. Clinton is a member of several boards and advisory committees, including the National Partnership for Cyber security, the Internet Education Foundation and the Advisory Board of the U.S. Congressional Internet Caucus, the IT Sector Coordinating Council and the DHS Critical Infrastructure Protection Advisory Council.

Prior to coming to IS Alliance, he was a vice president at the U.S. Telecom Association, served as a legislative director, in the House of Representatives. Welcome back, Mr. Clinton.

Mr. Ken Silva is the chief security officer of VeriSign. VeriSign's chief security officer and VP for Networking and Information Security. He oversees the mission critical infrastructure for all network security and production IT services for VeriSign. He also serves on several boards and advisory committees, including Information Technology, Information Sharing and Analysis Center. He is the chairman of the board of the Internet Security Alliance. Thank you for being here.

Ms. Catherine T. Allen is the chairman and CEO of the Santa Fe Group, a strategic consulting firm specializing in technology and innovation issues facing the critical infrastructure. Ms. Allen has long been recognized as a leading expert on technology issues facing the financial services sector and other critical infrastructure industry. Prior to her current position with Santa Fe, she served as the founding CEO of BITS, a technology-focused consortium led by the CEOs and CIOs of our Nation's top 100 financial institutions. She is a graduate of the University of Missouri, where she also received an honorary Doctorate of Humane Letters in 2005. Congratulations and welcome.

Ms. Kiersten Todt Coon is a VP of Good Harbor Consulting, where she focuses her efforts on developing risk management solutions for IT infrastructure and homeland security clients. Prior to joining Good Harbor, Ms. Todt Coon worked as a policy advisor to several senior Government and private sector leaders, including the Governor of California and former VP Al Gore. She also served as a professional staff member on the U.S. Senate Committee on Governmental Affairs, where she was responsible for drafting the Science and Technology Infrastructure Protection and Emergency Preparedness Directorate section of the Homeland Security Act of 2002. A graduate of both Princeton and Kennedy School of Government at Harvard, Ms. Todt Coon currently serves as a term member of the Council on Foreign Relations.

I welcome all of you. It is the policy of the committee to swear in all witnesses before you testify. And I would like to ask you to stand, please, and raise your right hands.

[Witnesses sworn.]

Mr. CLAY. Thank you. Let the record reflect that all of the witnesses answered in the affirmative. You may be seated. And we will start with Mr. Sabo to begin his testimony. And you have 5 minutes, and we like summaries.

STATEMENTS OF JOHN T. SABO, PRESIDENT, INFORMATION TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER AND DIRECTOR OF GLOBAL GOVERNMENT RELATIONS, CA, INC.; LARRY CLINTON, PRESIDENT, INFORMATION SECURITY ALLIANCE; KEN SILVA, CHIEF SECURITY OFFICER AND VICE PRESIDENT FOR NETWORKING AND INFORMATION SECURITY, VERISIGN; CATHERINE T. ALLEN, CHAIRMAN AND CEO, THE SANTA FE GROUP; AND KIERSTEN TODT COON, VICE PRESIDENT, GOOD HARBOR CONSULTING

STATEMENT OF JOHN T. SABO

Mr. SABO. Mr. Chairman, and members of the subcommittee. I am John Sabo, director of Global Government Relations for CA. It is one of the world's largest software companies. More importantly for this hearing, I am a board member and president of the Information Technology Information Sharing and Analysis Center [IT-ISAC]. I am also a member of the separate IT Sector Coordinating Council, and I chair the ISAC Council, which is composed of 13 ISACs addressing cross-sector information sharing issues.

I want to thank you and the subcommittee for the opportunity to share our views on public/private sector responsibilities with respect to preventing and addressing Internet disruptions.

The IT-ISAC is a not-for-profit organization. We were founded in 2001. We fund an operation center. We monitor and address threats, vulnerabilities and attacks on the IT infrastructure and we have processes in place allowing us to address these issues collectively across the member companies when issues rise to a level requiring joint analysis or action.

The IT Sector Coordinating Council and DHS formally recognize the IT-ISAC as the operational, informational sharing mechanism for our sector. The IT-ISAC is financed entirely by member companies through our membership dues and represents a significant by leading companies in the IT sector who have stepped to the call for industry action.

The GAO and the Business Roundtable have released reports, both of which have been referenced, expressing significant concerns about the ability of the Nation to respond and recover from a significant Internet failure.

Despite the fact that the Internet has to date proven resilient, these reports reinforce the imperative to plan for events that exceed our current understanding of threats. History often proves us wrong and surprises us with the unthinkable. The IT sector strategy to address these challenges is outlined in the IT Sector specific plan and at the heart of this plan is the need to protect key IT sector functions. And this is a very distinct concept from the physical asset focus of many other sectors. We are looking at IT functions.

The plan identifies in great detail a number of areas that need to be strengthened and in the statement we have addressed a number of them. I only touch on two here.

The first includes a number of steps that Government can take to enhance the public/private operational capability.

Leveraging the expertise of the IT-ISAC and other fully functional ISACs instead of turning to policy councils for operational purposes.

Stabilizing U.S. CERT and providing it with adequate funding in scale with its overall national mission, defining and clarifying the relationship among the U.S. CERT and other DHS analytical and operational components and programs.

Programmatically encouraging companies to join ISACs as a best practice, something which the Roundtable did in its report.

Supporting the cross-sector operational information sharing projects initiated by the ISAC Council, with equal energy and level of resources with which DHS supports policy and planning initiatives. Providing regular classified briefings to ISAC operational experts and not just to sector policy representatives.

And finally, in this area, organizing more effectively in response to the growing convergence between traditional IT and telecommunications. And we welcome the physical co-location of the U.S. CERT and the NCC watch that Assistant Secretary Garcia mentioned, and in fact appreciate his invitation for the IT-ISAC to have representation.

[The prepared statement of Mr. Sabo follows:]

Statement for the Record

John T. Sabo
Director, Global Government Relations, CA, Inc.
and
President, Information Technology-Information Sharing and Analysis Center (IT-ISAC)

Before the

Committee on Oversight and Government Reform
Subcommittee on Information Policy, Census, and National Archives
United States House of Representatives

Tuesday October 23, 2007
2:00 p.m.
Rayburn House Office Building, Room 2154

Mr. Chairman and Members of the Subcommittee

I am John Sabo, Director of Global Government Relations for CA, Inc., one of the world's largest software companies. I represent CA in a number of security and privacy-focused industry organizations including serving as the President of the Information Technology-Information Sharing and Analysis Center (IT-ISAC) and as a member of the IT-Sector Coordinating Council. I also serve as Chair of the ISAC Council, which addresses cross- sector information sharing issues.

I am here today in my capacity as the elected President of the IT-ISAC. On behalf of the IT-ISAC and its members, I want to thank you for the opportunity to share our thoughts on these critical issues.

Before I begin the substance of my testimony, I want to acknowledge and thank Assistant Secretary Garcia for his leadership. The Office of Cyber Security and Communications, specifically the National Cyber Security Division (NCSD), have been very supportive of our efforts. Indeed we have an excellent relationship with Greg and his team. Our challenge - and our goal - is to achieve similarly strong relationships with other parts of the Department of Homeland Security which also have operational responsibilities impacting the IT sector.

The Information Technology Sharing and Analysis Center (IT-ISAC)

An ISAC is an information sharing and analysis center. It provides a trusted, collaborative, information/intelligence sharing and analysis capability for critical infrastructure owners and operators. ISACs enable industry experts to establish working relationships, build trust, share sensitive vulnerability, threat, and mitigation information, conduct informed analysis, and collaborate with other sectors and government in an organized manner. The most advanced ISACs, such as the IT-ISAC, maintain operations centers, have multi-layered capabilities in terms of situational awareness and incident response, and have mechanisms in place to ensure the protection of sensitive information. If there is a single unifying vision across the ISAC community—and we do have a community and a Council—it is the continuing belief that, through our collaborative efforts and application of subject matter expertise, ISACs can prevent loss of life and economic value that would result from attacks against America's Critical Infrastructures.

The IT-ISAC was founded in 2001, after several years of development stemming from the discourse on Critical Infrastructure Protection (CIP) following the President's Commission and Report in 1998, the issuance of PDD-63 in June of 1998, and the accelerated interest in CIP during the Y2K era. The IT-ISAC is a non-profit organization which provides robust and trusted ISAC functionality for the IT sector. Our members include major IT corporations: BAE Systems IT; CA, Inc.; Cisco Systems Inc.; Computer Sciences Corp; eBay, Inc. Ernst & Young; EWA-IIT, Inc.; Harris Corporation; HP;

IBM; Intel Corporation; Juniper Networks; Microsoft Corporation; National Datacast, Inc.; Oracle USA, Inc.; Symantec Corporation; Unisys; USi, Inc.; and VeriSign, Inc.

Our central mission is to help protect the Information Technology infrastructure that propels today's global economy by identifying threats, vulnerabilities, and attacks on the infrastructure, and working in a trusted and collaborative environment to perform the analysis necessary to quickly and properly address them. The IT-ISAC shares information and intelligence with other sector-specific ISACs, U.S. CERT and with other government agencies.

The IT-ISAC also addresses physical threat issues affecting member company operational facilities and interdependencies, and has a growing capacity to share information associated with both physical and cyber issues enabling member companies to take appropriate action in response to threats and imminent attacks.

The IT-ISAC represents a significant, ongoing investment by the IT companies who are its members. IT-ISAC operations and operations center, security controls, Web site and communications protocols are entirely funded by member company dues. Additionally, the IT-ISAC relies on the dedicated commitment of member resources and expertise for analysis, collaboration, planning, and operational policy development.

The IT-ISAC extends its resources to support other sectors on cyber security issues, for example by initiating daily cyber security calls with as many as nine other ISACs (such as water, surface transportation, public transit, multi-state and financial services) and US CERT. We also work collaboratively as a member of the IT-Sector Coordinating Council (IT-SCC), where the IT-ISAC is formally represented on the Executive Committee. This in turn provides access to the valuable cross-sector policy work of the Partnership for Critical Infrastructure Security (PCIS), which is the umbrella policy organization across all SCC's. The IT-ISAC is also a member of the ISAC Council, which currently includes 13 ISACs, enabling us to address operational issues of common concern and value across critical infrastructure sectors.

All together, the trusted relationship among our members; the routine collaboration among them, our operations center, and other sectors; the expertise that resides within our member companies; and our mission of protecting the Internet Infrastructure provide the motivation and the capability to collectively address our sector's operational responsibilities on cyber security. We take this responsibility seriously, and have been recognized by both the IT Sector Coordinating Council and the Department of Homeland Security's National Cyber Security Division, our IT Sector Specific Agency, as the operational arm of the sector.

The Embedded Internet

The United States has always recognized the unique role communications plays in ensuring the national security and emergency preparedness posture of the country and protecting its citizenry. Telecommunications systems are also very robust – but for more

than a century they have planned, practiced, and prepared for recovering and reconstituting operations. In the aftermath of the Cuban Missile crisis and during the height of the cold war America took steps to bolster its plans and programs to support the recovery and reconstitutions vital to it economy, security, and defense.

Likewise, the criticality of the Internet must receive equivalent attention. The Internet has become part of the DNA of the modern economy. It is vital to communications, commerce, and defense of every developed nation. Internet "true believers" are sometimes dismissive of catastrophic scenarios that could result in serious degradation or Internet interruption. Despite the fact that the Internet has proven resilient in the face of both physical and cyber incidents, we should not ignore the imperative to plan for events that exceed our current understanding of threats. History often proves us wrong and surprises us with the "unthinkable."

However, unlike in the Telecommunications sector where there is a long history of collaboration, cooperation and coordination within industry and government on emergency preparedness, response, and national security issues, there is a growing concern that the U.S. lacks key capabilities for recovering and reconstituting Internet functions in the event of a catastrophic disruption. The Government Accountability Office (GAO) and the Business Roundtable have both released reports expressing significant concerns about the ability of the nation and its largest corporations to respond to and recover from a significant Internet failure in an effective and efficient manner. The table below summarizes some of the significant and systemic challenges to recovering or reconstituting key internet functions in a crisis.

Table 1: Report Summaries on Internet Recovery Challenges

RECENT REPORTS	INTERNET RECOVERY CHALLENGES
Government Accountability Office: *INTERNET INFRASTRUCTURE: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan (GAO-06-672 and GAO-06-1100T)* June/September 2006 http://www.gao.gov/new.items/d06672.pdf and http://www.gao.gov/new.items/d061100t.pdf	Key challenges to establishing a plan for recovering from an Internet disruption include (1) innate characteristics of the Internet (such as the diffuse control of the many networks that make up the Internet and the private-sector ownership of core components) that make planning for and responding to disruptions difficult, (2) lack of consensus on DHS's role and when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to entities working to restore Internet service, (4) reluctance of many in the private sector to share information on Internet disruptions with DHS, and(5) leadership and organizational uncertainties within DHS.

Business Roundtable, Two Reports: *Essential Steps to Strengthen America's Cyber Terrorism Preparedness* June 2006 http://www.businessroundtable.org/pdf/20060622002CyberReconFinal6106.pdf --- *Growing Business Dependence on the Internet: New Risks Require CEO Action* September 2007 http://www.businessroundtable.org/pdf/Security/BR_Internet_Business_Dependence_Report_09252007.pdf	* Inadequate early warning system – The US lacks an early warning system to identify potential Internet attacks or determine if the disruptions are spreading rapidly. * Unclear and overlapping responsibilities – Public and private organizations that would oversee recovery of the Internet have unclear or overlapping responsibilities, resulting in too many institutions with too little interaction and coordination. * Insufficient resources – Existing organizations and institutions charged with Internet recovery should have sufficient resources and support. For example, little of the National Cyber Security Division's funding is targeted for support of cyber recovery. --- * Internet dependence – CEO's need to address this as a major risk. Recommendations include making cyber security a CEO-level issue, addressing it in more complete business continuity plans, improving communications with industry partners and government, and participating in ISACs in sectors where ISACs are operational.

Industry-Government Planning Process – Operational Goals

The cautionary findings of those reports are largely correct. However, we have already started working to address them, in most cases in collaboration with the government and those who depend on the Internet.

The IT Sector's strategy is outlined in the IT Sector Specific Plan (IT SSP), which many of my colleagues in both the IT-ISAC and the IT-SCC collaborated with NCSD during the drafting process. The IT SSP is designed to provide a framework on how to enhance the security of the IT Sector. At the heart of this plan is the need to protect key IT sector operational functions (as opposed to specific physical assets). The plan focuses on enhancing national capabilities for

(1) Prevention and protection through risk management
(2) Situational awareness, and

(3) Response, recovery and reconstitution of America's information technology infrastructure.

It is appropriate to point out at this point that many of the individuals who are Board members or other leaders in the IT-ISAC also hold positions of trust in our Sector Coordinating Council. While participating in many IT-SCC policy efforts, they bring the views and expertise of the IT-ISAC to the table. These interlocking relationships help provide consistency in vision across the policy and operational components of cyber security issues and enhance the visibility of these issues with our government colleagues.

During the development of the IT SSP, government and industry participants, including many experts from the IT-ISAC membership, identified key challenges that need to be strengthened to achieve the sector's goals. Four of these challenges impacting response and reconstitution are shown in the following table.

Table 2: Critical Challenges and Needed Capabilities (source IT SSP)

Critical Challenges	Needed Capabilities
Robust Coordinated Response Capabilities	The capability to respond to and recover from a nationally significant event is critical to promoting the resilience of the IT Sector and other CI/KR sectors. An all-hazards operational response and recovery capability is needed to bring public and private sector security partners together to coordinate activities. Emergency communications, collaboration, and analytical tools could enhance effective response; this may include bolstering existing public and private sector resources and capabilities.
Reconstitution of Communications Services and Networks	A protective program initiative may be developed to assist with implementation of Federal Government authorities under Section 706 of the Communications Act applicable to key Internet functions. This program should also include developing the plans, programs, and mechanisms for identifying and refining requirements and developing reconstitution capabilities.
Reconstitution of Data	Data reconstitution tools and techniques are needed to ensure the integrity and availability of data. Development of a protective program should be linked closely to R&D activities designed to develop and pilot capabilities that enable key public and private sector systems to reconstitute rapidly data that could be corrupted, either intentionally or unintentionally.
Out-of-Band Data Delivery Capability	A protective program initiative is needed to provide mechanisms for delivering patches and other software to critical users if key Internet/network functions are not available. Such programs could include procuring space on satellites or unused television spectrum for moving software (e.g., critical patches or software) to key sites during a crisis or network congestion/failure.

I will briefly discuss some of the issues associated with these challenges and needed capabilities.

Strengthening Response Organizations

A key element of responding to attacks on the Internet Infrastructure is ensuring that we have organizations within industry and government with the collective expertise to organize a response to and effectively manage an incident. Development of this response capability is concomitant to the IT-SSP planning process, but is a distinct component. However, a recurring frustration for many of us in the operational space is the disproportionate amount of resources and energy DHS expends, and to which industry contributes, in a continuous planning cycle

compared with the quite limited focus and resources allotted to implementing the plans and supporting operational capabilities. We recognize the value of participation in the policy and planning process, and have made significant contributions working via the IT-SCC, but we strongly believe there must be an equivalent commitment to implementation. As President Eisenhower once said as a General, "In preparing for battle I have always found that plans are useless, but planning is indispensable."

There are specific actions government can take, consistent with existing plans, to leverage and enhance the value of the operational capabilities of industry's and government's information sharing and response capabilities.

- **Leverage the expertise within the ISACs on a more consistent basis.** The ISACs work on operational issues on a daily basis. For operational purposes, DHS should leverage the expertise within these organizations, instead of consistently turning to policy councils. When there is a fire in your town, you don't call the city council – you call the local fire department or 911 emergency number. Unfortunately, some DHS components routinely bypass sector-designated ISACs and do not make use of their information sharing capabilities or work with them on operational matters. These practices must change in order to reflect sector decisions.

- **Stabilize US CERT:** The US CERT cannot play its intended role if it lacks the necessary resources – people, expertise and budget to do the job outlined in both the Cyber strategy and HSPD 7. The US CERT's effectiveness is first and foremost dependent upon its people. The loss of the US CERT director and other departures of key staff concern industry and create uncertainty about the stability of the partnership planning and operational understandings we have reached.

- **Increase Funding for US CERT:** The US CERT budget should be examined to see if it is actually in scale with its overall mission. Congress may want to consider fencing off the US-CERT budget – which supports a national mission -- so that it cannot be taxed by other parts of DHS for non cyber related activities.

- **Define and Clarify the Role and Relationship Among the US CERT and other DHS Analytical Entities:** We question use of the Homeland Infrastructure Threat and Risk and Analysis Center (HITRAC) - which has minimal cyber expertise – to develop threat cyber-focused reports that, unlike HITRAC physical threat reports and analysis, have limited value. Although the cyber threat analysis and reporting are vital, that responsibility would appear to be more appropriately undertaken by the US CERT working with their industry partners. At a minimum, the relationship among US CERT, HITRAC and other DHS analytical entities needs to be evaluated, defined and improved.

- **Actively Encourage Companies to Join the IT-ISAC.** The Business Roundtable released a report last month that listed joining and participating in industry specific ISACs as one of five key recommendations for the business community.

The government should recognize this as a best practice, and, as such, encourage IT Sector companies to actively participate in the IT-ISAC as well as follow in its spirit by using functioning ISACs such as the IT-ISAC for operational matters.

- **Support the Cross Sector Operationally-Focused ISAC Council in the Same Manner that it Supports the Cross- Sector Policy Entity (PCIS).** Much as the PCIS provides a forum for the sector coordinating councils to collaborate on cross-sector policy issues, the ISAC council, with 13 ISACs as active participants, provides a forum for sector specific operational entities to collaborate, share information and best practices, and develop and coordinate operational policy issues. This work is critical in fostering increased, effective sharing of information and intelligence across sectors and enhancing our ability to improve situational awareness and incident response.

  Although DHS support enables a contractor to host four meetings a year at their facility, for which the Council is appreciative, we believe that some DHS resources should be directed to support the substantive information sharing initiatives fostered by the Council which are carried out by ISACs. As an example, the ISAC Council has initiated a set of tangible projects involving improved emergency communications contact lists and information sharing product inventories which can have great benefit for the sectors and government, but are being done as volunteer efforts. DHS support for these as well as for the Council's "Framework for Information/Intelligence Sharing," formally provided to DHS in October 2006 and endorsed by the PCIS, would have great utility for our operational partnership.

- **Provide More Detailed and Frequent Briefings to Owners and Operators, Through the ISACs**. The ISACs include members who have employees with security clearances at all classification levels. In fact members of the IT-ISAC have taken advantage of a DHS program to support clearances at the Secret level for industry cyber experts. This makes sense, because under the NIPP, the ISACs and other sector designated operational arms are responsible for analyzing and sharing information about threats to specific sectors. Given the clearances held by many of our industry experts, DHS should have in place a regulararized program to brief operational staff. However, DHS typically organizes such briefings for policy representatives, and not ISAC members - operational experts who are positioned to address the specific operational threat or security issue that was discussed. As one example, in August DHS hosted a classified briefing on the National Intelligence Estimate. The ISACs were not invited to that meeting. Although we requested the same briefing for the ISACs and our members, neither the briefing nor a plan for regular ISAC briefings has yet been made available.

Information Technology and Telecommunications Convergence

The *National Strategy to Secure Cyberspace* – Which was recently reaffirmed by the by the White House in its *2007 Homeland Security Strategy* – stressed the need for a

National Cyberspace Security Response System. We believe that with convergence between traditional "IT" and "Telecommunications," it is important to build a joint, robust response capability that enables government and industry to work cohesively to monitor the integrity of and protect our cyber infrastructure.

As an initial first step, we welcome the physical collocation of the U.S. government's cyber and telecommunications watch-and-warning centers, the US CERT and NCC watch, on a common floor in a common building. Assistant Secretary Garcia has invited the IT-ISAC to have representation in this facility, and we look forward to working with his staff to make this happen as quickly as possible and to move beyond collocation toward a truly merged and integrated watch, including enhanced industry participation.

This initiative, directed by Assistant Secretary Garcia in collaboration with industry, represents precisely the kind of leadership that DHS is capable of bringing to address new operational requirements while leveraging ISAC capabilities.

Infrastructure Reconstitution

The IT-SSP highlights a critical need to develop capabilities to reconstitute data. We are not just dependent on access to the Internet to communicate, conduct commerce or defend ourselves – we are dependent upon data. Experts conceive of attacks that would seek to disrupt critical national functions by corrupting select sets of data in a particular sector or in critical points of the economy. The large scale disruption of data may not be a sudden event but may unfold slowly over a period of days and result in economic dislocations or service degradations that could rival more traditional cyber or physical attacks. The U.S. currently has no unclassified programs or efforts that have been shared with the IT-ISAC about how they are prepared to assist the private sector in the event that such an attack were to occur.

The reconstitution of the physical and logical elements essential to the Internet is, also critical. The current National Response Framework (NRF) attempts to address this with the Emergency Support Function 2 and the Cyber Annex. ESF 2 is largely concerned with the roles and responsibilities of the U.S. government's agencies in dealing with restoration of National Security/Emergency Preparedness (NS/EP) critical services provided by regulated wireline carriers and identifies the process they will use to prioritize service requirements. However, it is not clear that same processes would adequately support the IT networks' packet-based communications environment.

The NRF's Cyber Annex appropriately recognizes challenges that response entities will have to deal with when managing complex incidents. However, the cyber annex does not fully address key response challenges such as:

- Designating which public sector agency the private sector would turn to if it needed specialized equipment to be prioritized. Would they go to the Department of Commerce and ask the National Telecommunications and Information Administration (NTIA) to sponsor it through the Defense Priority Allocation

Service process that executes Defense Production Act authorities? Or would the sector turn to its Sector Specific Agency, the NCSD?

- Describing how industry and government would come together in response to a crisis. As with other ESFs and sector annexes, the Cyber Annex should outline procedures and protocols for response actions necessary to maintain connectivity, analogous to the proscriptions to agencies in the ESFs. The annex should define a high level organizational model that the private sector can use as a basis for an operational plan, including a robust communications protocol. For example, if the Critical Warning Information Network (CWIN) or some other means is deemed to be the key mode of communications in response to an event, then it should be stated explicitly and a Concept of Operations developed in concert with the IT and Communications sectors.

- Detailing how government agencies will support and work with the private sector in the event of a catastrophic cyber incident.

- Responding to cyber events that cause substantial national disruption, but still not meet the threshold for a Stafford Act declaration.

Out-of-Band Data Delivery to Ensure Internet Recovery Capabilities

In the event that there were a serious event that degraded key Internet functions and prevented critical infrastructures and critical government agencies from receiving patches or emergency software updates/programs through the Internet, the options for distributing the critical software updates as well as accompanying information are not attractive. Putting people in cars with boxes of compact disks and physically distributing software may be the ultimate fall-back distribution method, but it has obvious disadvantages. While such a solution might work for an individual enterprise or a small set of customers located in close proximity, it is not an acceptable solution for an Internet dependent nation.

Government's role is to ensure that an appropriate operational environment exists to support the recovery of the Internet. The government has done this for voice communications. Through the National Communications System, the government has maintained various programs designed to ensure wireline and some wireless communications in crisis situations and reconstitution of capabilities in the event of the loss of service or infrastructure. There is no tool that will facilitate the recovery of critical Internet functions. CWIN has been rolled out to some operations centers in the private sector, but its deployment is limited, there is no current operational Concept of Operations (CONOPS) for its use in the context of the ISAC community, and there is currently little confidence that this system would be usable in a real crisis, although we understand that work is underway to evaluate CWIN and its operational utility.

The IT SSP identified high level needs for a system that would allow the dissemination of software and recovery information when the network was disrupted or un-trusted. From

the IT-ISAC perspective, I would like to provide some thoughts on the key attributes that a successful out-of-band solution should:

- Be identified and tested by both government and the private sector;
- Be technology neutral, long-lasting and supported by the private sector.
- Leverage existing infrastructure that can reach both densely populated urban centers as well as remote critical infrastructure facilities.
- Have a CONOPS developed by government and industry, integrated with ISAC CONOPS, and be tested regularly.
- Enable industry, which will be providing the software patches and programs, to have authenticated and trusted access to the system.
- Have a clear and easily understood set of protocols.

If designed properly, such a system would be utilized in response to a widespread internet disruption, but could also be useful for other types of challenges stemming from concerns such as pandemic flu, or catastrophic physical events such as Katrina. A well-designed internet recovery backup communications system could assist public-private interests by providing flexible response options that could be valuable for response in many types of incidents.

With respect to all of these initiatives, a key responsibility is operational readiness and measurable performance. Tests, drills, and exercises are critical to readiness. The Cyber Storm series of exercises has proven to be very valuable for the IT-ISAC, and other organizations that participated in them. Planning for Cyber Storm II is well underway, and I encourage other elements within DHS that conduct exercises to use the Cyber Storm II planning processes as a model. However, we should not wait for major annual or bi-annual exercises before testing our response capabilities. We should train and conduct drills on a routine basis to test our capabilities and update our procedures. In fact this is one of the areas where the ISAC Council has focused.

Bring Balance to Operational Priorities

Finally, I want to re-emphasize that the gap needs to be closed between DHS' resource commitments to writing policy documents and its resource commitments for operational capabilities. We have a very mature policy development capability, in part because DHS makes large resource and funding commitments to develop plans, update plans, create annexes to plans, and evaluate plans. However, relatively few resources are made available for implementing plans and building the operational capabilities that we will need to adequately respond to incidents. Clearly a rebalancing is necessary.

Now that the various sector specific plans are in place, we have had a perfect opportunity to shift our priorities from "planning" to "implementing"-- building incident response and other capabilities that we called out in those plans. Nevertheless, we continue to see attention and resources devoted almost exclusively to policy development rather than to government-industry operational implementation. Although planning is clearly necessary, unless attention is paid to building, testing and measuring the effectiveness of operational components, the plans have very little value.

To help address this, we believe that a DHS top priority must be to support and leverage the significant operational investments made by the IT-ISAC and other ISACs, to strengthen the operational, information sharing and response capabilities of ISACs and government organizations, and to develop an out of band backup capability to distribute data to support Internet recovery, should a serious disruption take place. An obvious starting point would be for all DHS components to integrate the IT-ISAC and other sector-endorsed ISACs into their day to day operational processes.

Thank you again for the opportunity to be with you today on behalf of the IT-ISAC. I will be happy to answer any questions you may have.

Mr. CLAY. I am going to ask each remaining witness to summarize, if they can, in less than 5 minutes, their opening statements. We are going to try to get in all opening statements before we recess again.

Thank you, Mr. Sabo. Mr. Silva.

STATEMENT OF KEN SILVA

Mr. SILVA. Thank you, Mr. Chairman. I want to commend and thank you for holding this hearing. It is difficult to overstate the importance of amplifying and expanding our national focus on cyber security.

Richard Clarke famously warned of the potential of a digital Pearl Harbor in which critical components of the Nation's increasingly vital electronic infrastructure would be brought down by a coordinated electronic attack.

Since he expressed his concern, nothing really much has changed to make this any less dire. If anything, the threat grows greater every day. In fact, it has already happened to the country of Estonia earlier this year.

None of us in Government or the private sector can sit still on electronic security. Our defenses must always remain two steps ahead of potential holes and exploits. If we fail to maintain that focus and let it deteriorate, we will be holding a very different sort of hearing in the near future, one in which we are all called upon to answer the hard question about what happened and what could we have done to have prevented it.

I have been asked to offer a perspective on the efforts VeriSign and the Internet industry are taking to ensure that such a calamity never occurs. Make no mistake, it would be a major catastrophe for the Internet to experience such a significant failure.

Approximately 25 percent of America's economic value moves over network connections each day. And it is not just our economy that would suffer. Government agencies at every level rely on the Internet. Imagine today's Congress trying to operate without e-mail or any other network services.

What could cause such a failure? There are a couple of potential scenarios. The first is that we in the Internet community simply fail to expand the Internet infrastructure enough to meet the mounting demands placed upon it. The second potential for failure is that we fall short in adequate protection of our critical resources against a host of increasingly sophisticated cyber-attacks being directed against it.

Internet crimes are increasingly conducted by sophisticated international crime syndicates that reap huge profits by targeting the network and its users. Even more frightening is the rise of cyber-attackers backed by governments and other deep-pocketed enemies of the United States.

Today's attacks can cause damage 100 times more extensive than the attacks just a year ago. This is why investment in the infrastructure is so critical. Simply put, if we wait for usage to outpace the development or for sophisticated attacks to overwhelm our stagnant defenses, we are already too late.

We learned the cost of complacency as a country when we watched the damage done by Hurricane Katrina. By the time

Katrina hit the Gulf Coast, it was too late to strengthen its levees. We should not have to learn that lesson more than once. Critical resources should be reinforced long before there is a threat to their well-being.

The Internet continues to grow at dramatic rates, which means the infrastructure must scale to meet that demand. No one can take security and stability of these networks for granted; not VeriSign, not the ISPs or other private sector players, and certainly not the Government.

As the operator of the dot-com and dot-net domain registries, as well as a steward for 2 of the 13 root servers, VeriSign understands what is at stake. Over the last 8 years, VeriSign has operated its infrastructure with 100 percent in up-time. In other words, the systems that ensure Internet's core infrastructure remain functional have never gone down. VeriSign's primary computers that handle the dot-com and dot-net traffic are now capable of handling 10,000 the number of queries that they could handle in 2000.

And while the dot-com and dot-net systems currently process more than 30 billion queries a day, we will need to build a network infrastructure that can support 10 to 100 times that level of volume in the next few years.

That is why earlier this year, VeriSign announced a global initiative called Project Titan to expand and diversify its Internet infrastructure to those levels by 2010. These upgrades are vital to managing the surge in Internet interactions and protecting against cyber-attacks.

VeriSign is well on its way to meeting its goals under Project Titan and is already considering how to address this set of challenges.

Thank you.

[The prepared statement of Mr. Silva follows:]

Ken Silva

Testimony Before the
House Government Reform Committee

October 23, 2007

Good morning, Chairman Clay, Ranking Member Turner and distinguished Members of the Committee. My name is Ken Silva and I serve as Chief Security Officer of VeriSign.

VeriSign operates digital infrastructure that enables and protects billions of interactions every day across the world's voice and data networks. The company is headquartered in Mountain View, California and it has additional corporate facilities in Virginia, Kansas, Washington state and Massachusetts.

Thank you for the opportunity to testify today. I have a prepared statement, which I would request be inserted in the record.

I want to commend and thank you for holding this hearing. It is difficult to overstate the importance of amplifying and expanding our national focus on cybersecurity.

Former national cybersecurity Czar Richard Clarke famously warned of the potential for a "Digital Pearl Harbor," in which critical components of the nation's increasingly vital electronic infrastructure would be brought down by a coordinated electronic attack.

In the years since he expressed his concern, nothing has changed to make it less dire. If anything, the threat grows greater every day, as electronic attackers refine their tools and techniques, and the increasingly ubiquitous Internet becomes an ever more attractive target to wrongdoers.

None of us in government or the private sector can afford to sit still on electronic security. Our defenses must always remain two steps ahead of potential holes and exploits.

If we fail to maintain that focus and determination, we'll be holding a very different sort of hearing in the near future -- one in which we're all called upon to answer the hard questions about why the cornerstone of our digital economy failed, and what we could have done to prevent it.

I've been asked to offer perspective on the efforts VeriSign and the Internet industry are taking to ensure that such a calamity never occurs. And make no mistake; it would be a major catastrophe for the Internet to experience a significant failure.

Approximately twenty-five percent of America's economic value moves over network connections each day. A widespread Internet failure lasting just a few hours would trigger hundreds of millions of dollars in losses. A failure lasting a few days would be equivalent to a massive, nationwide work stoppage capable of crippling the economy.

And it's not just our economy that would suffer. Government agencies at every level rely on the Internet for law enforcement, maintaining national security, serving citizens and even legislating. Try to imagine today's Congress trying to operate without e-mail, Web or any Internet-enabled function, and extrapolate that mess out to the thousands of government agencies at the federal, state and local level that would be impacted by such a loss.

What could cause such a failure? There are two potential scenarios. The first is that we in the Internet community simply fail to expand the Internet infrastructure enough to meet the mounting demands placed upon it. The explosion of Internet-enabled devices and applications – text messaging, music downloads, VoIP, Blackberries and device-to-device communications – has created exponential growth in Internet traffic that far exceeds the traffic increase attributable to new human users. While the number of users has increased 300 percent since 2000, the volume of traffic on .com and .net has increased a stunning1,900 percent over the same period. The good news about this scenario is that it is entirely avoidable, so long as companies like VeriSign continue to invest, in robust, forward-looking improvements to our vital electronic infrastructure.

The second potential for failure is that we fall short in adequate protection our critical resources against the host of increasingly sophisticated cyber attacks being directed against it. As the Internet has evolved, so too have the threats to its continued stability.
The days in which most online troubles were caused by cyber-vandals, defacing popular Web sites for a few moments of fame are long gone. Internet crimes are increasingly conducted by sophisticated international crime syndicates that reap huge profits by targeting the network and its users. Even more frightening is the rise of cyber-attackers backed by governments and other deep-pocketed enemies of the United States.

Electronic threats like SPAM, Phishing, spyware, identity abuse, viral attacks, and denial-of-service exploits -- involving hijacked computers linked through broadband connections, can make use of massive bandwidth to deliver their malicious payloads. A spate of serious attacks last year reflects how these incidents have grown in frequency and sophistication. Today's attacks can cause damage a hundred times more extensive than the attacks of just a year ago.

This is why investment in the infrastructure is critical. Simply put, if we wait for usage to outpace development or for sophisticated attacks to overwhelm our stagnant defenses, we are already too late.

We learned the cost of complacency as a country when we watched the damage done by Hurricane Katrina. By the time Katrina hit the Gulf Coast, it was too late to strengthen the levies. We should not have to learn that lesson more than once. Critical Resources should be reinforced way before there is a threat to their well being.

The Internet continues to grow at dramatic rates, which means the infrastructure must scale to meet that demand. No one can take security and stability of these networks for granted; not VeriSign, not the ISP's or the other private sector players and certainly not the government, .

As the operator of the .com and .net domain registries, as well as the steward for two of the 13 root servers that serve as the nerve center of the Internet, VeriSign understands what's at stake. Over the last eight years, VeriSign has operated its infrastructure with 100 percent uptime – in other words, the systems that ensure the Internet's core infrastructure remain functional has never gone down.

VeriSign's primary computers that handle the .com and .net traffic are now capable of handling 10,000 times the DNS query volume they could handle in 2000. To put that in perspective, although that Moore's Law states that computing power doubles every 18 months, we have chosen to increase our capacity at 600 times that rate.

And while the .com and .net systems currently get more than 30 billion queries a day, we will need to build a network infrastructure that can support 10 to 100 times that level of volume in the next few years.

That is why earlier this year VeriSign announced a global initiative called Project Titan to expand and diversify its Internet infrastructure by to be ten times more robust by the year 2010. Under Project Titan, VeriSign is:

- Increasing its capacity ten times from 400 billion DNS queries a day to 4 trillion a day. By doing so, VeriSign will ensure that the infrastructure is prepared not only for attacks, but the dramatic increase in Internet usage driven by Internet-enabled mobile devices and social networking applications.

- Substantially expanding its infrastructure both domestically and internationally. VeriSign is in process of globally deploying over

70 DNS constellation sites. These sites will distribute Internet traffic and enable us to isolate attacks as they happen.

- Improving the monitoring infrastructure to provide a real-time, in-depth view of anomalous network activity, malicious or otherwise.

These upgrades are vital to managing the surge in Internet interactions and protecting against cyber attacks. VeriSign is well on its way to meeting its goals under Project Titan and is already considering how to address the next set of challenges.

I often get asked what about Internet security keeps me up at night.

I always say there are two things. The first is the volume and sophistication of attacks. The very devices and increased bandwidth that make the Internet more robust and user friendly are being deployed every moment of every day to compromise the Internet. Now that computers are always on, they are much more easily hijacked and turned to malicious ends by hackers and other abusers. And the increased bandwidth and computing power available literally gives hackers more ammunition to utilize against the infrastructure.

VeriSign projects that the volume of Internet attacks will increase by 50 percent in both 2007 and 2008. What deeply concerns me is a scenario in which terrorist attacks on a physical structure are combined with a cyber attack. Equally concerning, are the number of more subtle penetration attempts. We are literally constantly probed for vulnerabilities. If we let our guard down for even a few moments, the slightest weakness could be exploited to inflict damage far greater than that caused by a traditional denial-of-service-attack.

The second is the potential for what I call a well-meaning, self-inflicted wound. As we make vital improvements to build out the infrastructure and expand the Internet we must be careful that our efforts don't inadvertently Balkanize the network or confuse users.

The Internet community is currently discussing the important issue of Internationalized Domain Names (IDNs). These are domain names that can be entered using the letters or characters of local languages, such as Mandarin. This is an important step that can open up the Internet in new ways and to billions of users around the world. But implementing IDNs in a stable, secure manner requires resolving a host of technical and business issues . If we don't handle this issue correctly, we could create separate and confusing Internet "rules" that confuse Internet users. Worse, we could create the opportunity for oppressive regimes to establish new conditions on businesses impacting their

ability to realize the full potential of the Internet as a tool to promote openness and commerce.

Whether it's fortifying the infrastructure against cyber attacks or creating a framework to truly internationalize the Internet, it is vital that government and private industry take "long view" with a goal towards ensuring security, stability and user confidence that the Internet will continue to function as well or better than it has in the past.

As a steward of the Internet infrastructure, it is our job to ensure that the Internet remains reliable and always on and therefore available so that e-commerce flows, emails are delivered and users can visit the Web sites they want, whether they are at home or half-way around the globe.

To do so, the private sector must stay a step ahead of demand and the next wave of threats. The operators of this infrastructure must never take it for granted. We must be vigilant in understanding what is driving the growth of the Internet and the malicious efforts of those who wish to disrupt it.

Thank you for the opportunity to testify here today.

-30-

Mr. CLAY. Thank you.

STATEMENT OF LARRY CLINTON

Mr. CLINTON. I want to congratulate you, Mr. Chairman, on holding this hearing of the Government Reform Committee, because Government reform is clearly what is necessary.

The June 2, 2006 GAO Report got it exactly right. The problem is the inherent characteristics of the Internet. The Internet is unlike anything we have ever dealt with before. It is international, it is interactive, it is constantly on the attack. Consequently, it will require a security system unlike anything we have ever designed before.

We can't simply cut and paste previous government systems and put them into Internet security. Even if Congress enacted a brilliant statute, it would only go to our national borders. Even if a regulator came up with a brilliant solution, it would be outdated before you could put it into effect.

Fortunately, we need other things to attack the Internet. The committee has expressed some interest in the instance of Katrina, saying that we should model ourselves on that. There are major differences between cyber-attack and Katrina. Katrina, we could see it coming. Literally. From hundreds of miles away. The adequate analogy to Katrina is that the problem with Katrina wasn't the event itself. The problem with Katrina was that the systems weren't in place to properly handle the event.

Now, fortunately, we actually know a good deal about how to mitigate and manage a number of issues dealing with cyber security. The largest study ever conducted in this field found that the best practices group, people who follow the industry recognize best practices were able to have fewer incidents, less downtime, less financial loss.

What we need to do is find a way to get more people to follow the best practices that industry is already following. Industry is also not waiting for government to get its act together. Industry is aggressively moving forward with new products and services because, as it has already been pointed out, the problem has morphed.

We are no longer looking at these well publicized instances like Blaster and Love Bug that were designed to get publicity. Instead, what we are dealing with now are carefully targeted designer malware that can sit on a system for an extended period of time, cause tremendous damage and we don't even know it is there.

Fortunately, we are developing new systems to attack this. But there is a role for the government. And role for the government was pointed out in that 2006 GAO Report, where they pointed out that in the private sector, competitors were working together to deal with these incidents when they see that there is a direct business relationship benefit to that. And the NIPP, the National Infrastructure Protection Plan, also pointed out—and this is the one thing that I choose to read for you, Mr. Chairman:

> That the public private partnership called for in the NIPP provides for the foundation for effective critical infrastructure protection. The success of the partnership depends on articulating the mutual benefits to government and the private sector partners. While articulating the value to the proposition for the government is typically clear, it is often difficult to articulate the

direct benefits to the private sector. In assessing the value proposition for the private sector, there is a clear national security interest and homeland security interest in ensuring that the collective protection of the critical infrastructure goes beyond that of the business unit. Government can engage industry to go beyond efforts already justified by their corporate business needs and assists in a broad-scale critical infrastructure protection by creating an environment that supports incentives for companies to voluntarily adopt widely held best practices.

And I conclude my presentation by listing for you 10 steps that I would suggest that the committee consider for roles that the Government can embrace, which are not your traditional regulatory role, but are things like leading by example, using your market power instead of your regulatory power; supporting research and development that is not going to be undertaken by industry; using the market incentives that you have traditionally used in other areas; address the lack of cyber insurance; raise your aim in terms of awareness to focus on senior executives rather than individuals; adopt a coherent strategy for dealing with the private sector, something discussed before; clarify the roles and procedures for crisis management; and rethink your approach to information sharing.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Clinton follows:]

Thank you, Mr. Chairman.

I am Larry Clinton, President and CEO of the Internet Security Alliance. I also am a member of the DHS's Communications Sector Coordinating Council, the Critical Infrastructure Partnership Advisory Council and serve as an Officer on the IT Sector Coordinating Council. ISAlliance is a collaboration with the Carnegie Mellon University. We are a cross-sector trade association focused exclusively on information security. We have roughly 1,000 member companies. We provide our members with a range of services, including technical, business operational and public policy.

I want to congratulate the Chairman for holding this hearing of the Information Policy Subcommittee of the Government Reform Committee because government reform is clearly what is needed, as well as some private sector reform, to provide sustainable security from a serious and growing cyber threat.

The Internet Itself Demands Government (and Industry) Reform

Government reform is not necessitated by bad faith, corruption or incompetence of people charged with overseeing cyber security. Indeed, my experience is quite the opposite.

However, we need to change the way government, perhaps including Congress, thinks about and conceptualizes its role in assuring Internet security. In its June 2006 report, "Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan," the GAO got it right. It listed as the number one challenge we face the "innate characteristics of the Internet."

We need to realize that the Internet is unlike anything we have dealt with before. Consequently, it will require a security system unlike anything we have designed before.

How then is the Internet different?

- It transmits phone calls but it is not a phone line.
- It makes copies but it is not a Xerox machine.
- It houses books but it is not a library.
- It broadcasts images but it is not a TV station.
- It is critical to our national defense, but it is not a military installation.
- It is all these things and much, much more.

The Internet is international, interactive, constantly changing, constantly under attack, then changes and changes again.

It is not even really an "It." It is actually lots of "Its" all knitted together-- some public, some private--all transmitting information across corporate and national borders without stopping to pay tolls or check regional sensitivities.

We can not simply "cut and paste" previous governance systems from old technologies or business models and realistically expect that we will be able to manage this system effectively.

The regulatory model we have traditionally used to govern business has not changed much since we created it to deal with the breakthrough technology of 2 centuries ago--- the railroad.

To manage the railroad, Congress decided to create an expert agency, the ICC, to pass specific regulations. The ICC begat the rest of the alphabet soup: the FCC, the SEC, the FTC. And, that system has worked arguably well in most instances.

But that system will not work with Internet security. Even if Congress were to enact an enlightened statute, it would not have reach beyond our national borders and hence would not be comprehensive enough. Even if some agency wrote a brilliant regulation, it would likely be out-dated before it got through the process, a process that can be further delayed with court challenges.

And that assumes, unrealistically, that the political process inherent in a government regulation system doesn't "dumb-down" the eventual regulations so that we wind up with a campaign-finance-style standard where everyone can attest that they met the federal regulations, but everyone knows the system is really not working.

That may work in politics, but, frankly, we can't afford that when it comes to Internet security.

Yet, we can't stand idly by either. We must, together, develop a mechanism to assure an effective and sustainable system of security that will accommodate the global breadth of the Internet and still result in a dynamic and constantly improving system of mutual security.

Good News: There are Steps in the Right Direction

There is actually a fair amount of good news in the cyber security field.

To begin with, there has been a marked improvement is that the working relationship between industry and government on cyber security issues is improving.

Paramount in this area is the government's growing realization of the importance of cyber security.

You may recall some of us campaigned for years to establish a senior position in DHS, an Assistant Secretary for Cyber and Telecommunications, and once it was established it took some time to fill the post. We are extremely happy that the position has been filled by Greg Garcia. Greg, working with Assistant Secretary Stephan, has ushered in an era of true partnership consistent with the directives of PDD 67 and HLS Directive 7, as well as other planning documents calling for a true public-private partnership. This new approach has been felt at the ground level by the many private sector volunteers who are attempting to assist in this effort, and we are grateful for it.

Perhaps even more important, the role of cyber security in the defense of all our critical infrastructures has at long last been recognized. Early drafts of the NIPP treated cyber security as an afterthought of the telecommunications infrastructure. It has now been realized that virtually all our nation's key resources, not to mention the economy as a whole, are dependent on cyber security. As a result cyber security is now being integrated not just into the IT and Communications Sector Specific Plans but into all the sector plans. This is certainly a step in the right direction, but many more steps within the traditional sectors need to be continually encouraged.

In addition, DHS has shown important flexibility toward the private sector in recognizing that methods they are comfortable with in assessing physical sectors do not necessarily apply when we are discussing the cyber infrastructure.

A key example has to do with the currently on-going process of developing a risk assessment methodology associated with implementing the sector specific plans. In traditional infrastructures, such as power or chemical plants, such assessments usually begin with identification and cataloging of critical assets.

This sort of "bottom up" approach makes no sense in the cyber security field. The private sector had to engage in substantial education of our government partners to demonstrate to them that, in the cyber field, to do a useful risk assessment you need to take a top down approach, starting by identifying the key functions that must be maintained, not the physical assets (which maybe interchangeable). DHS's recognition of this perspective and our joint work as partners in that direction is truly encouraging.

Second, we already know a fair amount about how to prevent, mitigate and recover from cyber attacks.

The Committee has expressed a particular interest in major disruptions. It's important to understand that a major cyber event would probably be unlike a catastrophe like Katrina in several key respects.

To begin with, we could see Katrina coming, literally from hundreds of miles away. That is unlikely to be the case with a major cyber event. Terrorists or an enemy nation state could potentially place malware on critical infrastructure hardware or software that could lie dormant and undetected for an extended period of time waiting to be triggered unexpectedly by a seemingly unrelated event and timed to the worst possible moment of crisis. The results could be substantial electronic, property and human damage.

A useful analogy between Katrina and a major cyber event is that the tragedy of Katrina was not the event itself but the inadequacy of the systems designed to handle the event. Had the levies held, or the transportation and social services been properly maintained and managed the effects of Katrina could have been far less catastrophic.

My point is that the best way to manage the risk of a major cyber event is with an ongoing program of systematic maintenance and cyber monitoring coupled with following the ever evolving state of best practices that are continually being developed and modified.

Within the marketplace, there is a robust assortment of published regulations, standards, best practices and similar guidance that has already been produced that addresses the manner in which information security is to be developed and implemented in commerce. These publications target specific nations as well as international audiences; others address the requirements of specific trades or industries. Recent research shows that following these existing practices can indeed result in demonstrable improvements in cyber security.

The largest security research project ever done, the "Global Information Security Survey" conducted by PricewatterhouseCoopers for CIO Magazine, found that about one-fifth of its respondents, dubbed the "best practices" group, report that, although they suffered more cyber incidents than the average respondent (presumably because they are more attractive targets), they had less downtime and monetary damage. Indeed, one-third of the group reported that they had zero downtime and zero financial impact, despite being targeted more often by malicious actors.

These findings provide compelling evidence that there is a substantial, though not a majority, number of "good actors" in the corporate information security field. These organizations have, through various mechanisms, identified and implemented effective information security measures. The work of these good actors should be recognized and encouraged. We also need to find a way to get broader adoption of these practices hat have been shown to work.

A third piece of good news is that there is now a robust and growing industry, as well as trade groups such as ISAlliance, focused on internet security. This is a comparatively new phenomenon.

In fact, when ISAlliance was founded 6 years ago our first services were to provide threat, vulnerability and mitigation information to the private sector through the CERT/CC at Carnegie Mellon University. It is sometimes hard to remember but way back then many people actually thought that the internet was safe and secure. The information we provided about vulnerabilities and "exploits in the wild," and advance mitigation strategies were revelations to our members.

All that is now changed. With the creation of DHS the US CERT took over the services we had provided through contracts and non-disclosure agreements to our members. The US CERT information was free to anyone, but not nearly as detailed or useful. As a result the ISA members have found the government service not nearly as useful as we previously provided.

Also since 2001, numerous vendors of threat and vulnerability information have come on the market and this sort of information is now readily available as a commodity. However, as we have moved from vulnerabilities that might have taken months to exploit to the current era of zero day attacks, just getting information is no longer nearly enough.

Our efforts to improve corporate information security have matured with the evolving threat. We now realize that information security is not simply a technical issue, though it has a significant technical component. Treating cyber security just by providing information is like treating a staph infection with a band aid.

Our members now look to us to provide a comprehensive risk management approach that encompasses the full-system approach necessary to address the problem. An example is our Enterprise Integration Program which addresses discrete cyber security issues ranging from preventing and handling breaches of personal information to securing the IT supply chain in the era of globalization.

We address these issues by looking at their technical, business operational, human resource, legal and public policy aspects simultaneously and developing an integrated solution. We would commend this fully integrated model to our government partners to consider.

Moreover, as the world has become aware of the need for security products to address a technology built on inherently insecure protocols, the private sector is responding with ever more sophisticated products and services.

For example, we now know that threats to the net have morphed from broad and often relatively benign, if well publicized, attacks like Love Bug and Blaster, to designer malware constructed to target specific systems where it can reside undetected by traditional methods for an indeterminate period of time while causing serious damage.

As a result, traditional AV software and firewall solutions are becoming inadequate. However, a new generation of security products has been, and continues to be, developed to address the continually evolving threats.

Industry has committed significant resources to increasing levels of security assurance in hardware and software and the development of security enhancing new products and features.

Some of these advances are directly focused on security issues currently creating concern for government and the private sector. Technology that will be released shortly will increase the protection for data at rest through innovative use of encryption. This hardened encryption should help mitigate the risk from security failures such as lost lap tops by making it extremely difficult to retrieve encrypted data off a stolen device. In addition, companies plan to release new technology to protect against threats from malicious software, thus providing information technology departments with better mechanisms for logging onto networks which will help contain malicious software and remediate the impacted systems.

There is Still Much More to Do

Let me be very clear. Notwithstanding the fact that many in the private sector have begun to address this problem seriously, we are not nearly as far along as we need to be.

And, notwithstanding the positive steps being made in some aspects of the industry-government relationship, that relationship is far from being adequately productive.

The point I am making is that, while we know a good deal about how to improve cyber security and are continuing to work as the threat evolves, much more needs to be done.

Getting the amount of buy-in from the government and industrial users, owners and operators necessary to create a sustainable system of immediate, not to mention long-term, cyber security is still a long way off.

Fortunately, we are beginning to see a consensus emerge as to how to formulate an effective government-industry partnership, but we have yet to see much in the way of concrete actions to make that system a reality.

The most effective way to establish an effective and sustainable system of cyber security is to create an economic value proposition for all entities to continually adopt and improve state-of-the art cyber security practices.

The June 2006 GAO Report on the Challenges in Developing a Joint Public Private Partnership again provides us with a road map. That report states: "Private companies currently deal with cyber attacks and physical disruptions on a regular basis.... Infrastructure representatives also noted that in the event of a network disruption, companies that are competitors work together to resolve the disruption. They said that although the companies are competitors that they have a business interest in cooperating because it is common to rely on each other's networks."

It is also a very positive sign that the US government has recognized the fact that there is a compelling national interest in creating this value proposition for the private sector as the most effective and efficient way to improve our collective security. Specifically, the National Infrastructure Protection Plan (NIPP) notes:

> The public private partnership called for in the NIPP provides for the foundation for effective CI/KR protection....The success of the partnership depends on articulating mutual benefits to government and private sector partners. While articulating the value proposition to the government typically is clear, it is often difficult to articulate the direct benefits of participation for the private sector.... In assessing the value proposition for the private sector there is a clear national security and homeland security interest in ensuring the collective protection of the Nation's CI/KR. Government can engage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CI/KR protection through activates such as:
>
> Creating an environment that supports incentives for companies to voluntarily adopt widely accepted sound security practices (NIPP page 9).

Government can provide a vast assist to this effort by fashioning an incentive program for the good actors that will create a business advantage for them over less careful players. In so doing, we hope to harness the power of the market to motivate cyber security on a worldwide basis.

The NIPP and the GAO Report show the way, but we are not yet seeing government start down this road.

The problem is that in order for government to engage industry in the sort of partnership suggested, they must rethink their role in the partnership. This cannot be a parent-child, superior-subordinate relationship. It needs to be more of a partnership wherein both sides achieve their goals.

What is Government's Role—A Top Ten List

As we discussed at the outset, the traditional government role of regulator, while appropriate in narrow instances such as consumer protection, does not fit well for broad infrastructure protection due to the intrinsic characteristics of the internet.

But if government's role is not to regulate, what is its role? Does government, specifically, does the US federal government have a role?

Yes, it does, and many in fact. While fully laying out a modernized set of roles for the US government goes well beyond my expertise and the limits of this testimony, I can offer at least a top ten list of things the US federal government ought to be doing to improve cyber security.

1. Government can lead by example. Treat cyber security within government agencies with a higher priority in recognition of its critical importance, including providing government agencies with the financial and personnel resources necessary and rewarding down to the employee review level adherence to cyber security goals and objectives which create a culture of security within federal agencies.

2. Government can use its market power, instead of its regulatory power, to provide a market incentive for improved cyber security. For example, security ought to be a true decision point in the awarding of federal contracts, along with cost, rather than a comparatively minor item.

3. Government can work with us on developing a series of market incentives to encourage greater adoption of security best practices. The National Strategy to Secure Cyber Space had it right when it noted that the market would need to be the motivator for necessary improvements in cyber defense. But markets do not spring up spontaneously. They need to be developed and nurtured. Government can, and traditionally does, have a role in developing these market incentives to address social goals such as infrastructure security. There is a range of mechanisms at the government's disposal to do this including taxes, procurement, awards programs, as well as more creative programs such as the cap and trade systems enacted to address environmental issues. ISA has developed a series of proposals which it would be delighted to discuss.

4. To mitigate against the effects of a major event, the government needs to address the lack of cyber insurance. The costs of a major cyber event have been estimated to potentially run to the tens of billions of dollars. Should such an event occur, the vast majority of the damages may have little or no insurance coverage at all, meaning thousands of businesses and potentially millions of people would be economically stranded with only the federal government as the payer of last resort. Most traditional insurance policies do not cover cyber losses. In fact one recent study showed more than half of industry CIOs either did not know if they were covered for cyber loss, or thought they were covered when in fact they were not. There are some very logical reasons why the cyber insurance market has been truncated, but not unprecedented ones. Government ought to realize that there is a compelling national interest to manage some of their own cyber risks by transferring a portion of it to the private sector. By enhancing the cyber insurance market government will also assist consumers by lowering prices, providing security and establishing an incentive lever for improved behavior much as health and car insurance are used to motivate improved health and driving behaviors.

5. Government can raise its aim in terms of its awareness efforts. The national security interest is served much more directly by addressing the senior corporate leaders about the need to better secure the information infrastructure, rather than mom and pop awareness efforts.

6. Government can develop a coherent strategy for dealing with private sector. Much like Congress, federal agencies have not coordinated their approach to dealing with the private sector. Even at DHS there appears to be one set of private sector contacts operating through the private sector office, and another through the infrastructure protection/cyber divisions. Many of us on the private sector side are contributing untold hours to meeting and coordinating with government, only to find at times that an entirely different group has been designated as the private sector contact for a particular effort or exercise. The private sector is delighted to work with our government partners, but the system needs to be made more efficient and productive.

7. Government can begin to look at cyber security as a broad international issue, not a narrow US federal government issue. The bifurcated international approach on cyber security is inadequate. It focuses too much on a narrow group of countries and primarily on a government-to-government basis. Given the fact that cyber attacks inherently cross multiple borders, this government-centric approach has limited utility. A more productive approach would be to give greater priority to US-based multinational corporations and to those of allies whose systems transcend national borders to provide a pathway to global system security.

8. Government must clarify the roles and procedures for crisis management and enact any necessary legislation to address pending issues. Now, years past Katrina, there is still unresolved issues such as a lack of assurance that critical infrastructure providers such as those who operate the internet will have access to needed resources and that clear lines of communication have been established between government and industry in the case of a major disruption.

9. Government can support R&D into government-level issues that will not likely be addressed by the private sector. For example, many experts have noted that the TCP/IP protocols upon which the internet is based are inherently insecure. A heavy lift R&D effort by the government to write and implement truly secure protocols, a project that may take some time, is an appropriate role for the government. Use of creative models such as the Sema-Tech model used to attack the 1980s issues with computer chips might be useful models.

10. Government can rethink its approach to information sharing. The traditional model is to withhold information and disclose if necessary. The lack of sharing of information, and government requirements for treating corporate information once disclosed, is one of the major reasons that the necessary trust environment has not been established and the information sharing regime is widely held to be inadequate by all sides.

Mr. CLAY. Thank you so much, Mr. Clinton. The committee will now recess for the duration of these votes on the floor. They tell me it will be about half an hour. I am sorry. The committee stands in recess.

[Recess.]

Mr. CLAY. The committee will come to order. Ms. Allen.

STATEMENT OF CATHERINE T. ALLEN

Ms. ALLEN. Thank you, Chairman Clay and members of the subcommittee and committee for the opportunity to submit testimony before you today on private and public sector efforts to secure our Nation's Internet infrastructure.

The Santa Fe Group does a lot of work for the industry and still for BITS. I am actually going to go directly to the recommendations because of the time.

And what I am suggesting is that the financial services industry has done a great deal to strengthen business continuity, planning and coordinate prior to and during times of crisis. We have business continuity plans which are constantly updated. We refine and test them, and this is a regulatory requirement, and part of our risk management process.

Most financial institutions, in fact, all that are deemed mission critical are required by our regulators to have recovery operations in place and back-up in a very narrow timeframe. And this requires telecommunications, it requires power and it requires dependency upon IT. If any of those are not working, we cannot meet our regulatory requirements.

I would be the first to tell you that we have a long way to go as an industry, but there is much of what we do that we believe could be copied or modeled for other critical infrastructure industries.

We have a very successful FS-ISAC, Financial Services ISAC, and FSSCC, a coordinating council for critical infrastructure protection. We work very closely with our regulators through the FBIIC and with the Department of Treasury in coordinating on everything from Katrina to the power outage after 9/11.

Most recently, we ran a pandemic exercise which included a component that looked at if the Internet was down and we had many people working from home, what would that mean.

And I would say that the two most important things that we have done related to Internet recovery are the work that we did on business critical telecommunications services, where we developed best practices, not only for the financial sector but for the telecom sector, upon which we are extremely dependent, to make sure that they had the diversity and redundancy that we needed.

We also finished a business critical access to power. We did this with the power industry, again to look at best practices for alternative power if there was disruption in any of the IT industry.

Last, we worked in managing third-party service providers. Much of the Internet is dependent upon third parties, many of whom are located in India and China and other places. So, looking at how we manage those. Those are all models for other industries.

The recommendations that I have are, recognize that other industries may need to share the same level of responsibility and li-

ability that we do as an industry, and to look at some of our regulatory requirements might not be a bad idea. Second, we maintain rapid and reliable communications, and that means diverse communications.

I personally had a number of our CIOs from the financial sector in Detroit when we had the power outage, we were all using our Blackberries, which were the only thing that still worked, because the cell phones ran out and there was no power. But that is how we communicated with our regulators, and we were able to make sure that it wasn't a terrorist event, that it was in fact a power outage. But we needed to have alternative channels.

Recognize the critical infrastructures that are dependent upon software and operating systems. The IT industry is the backbone for telecommunications, for power, for the user groups like financial services and chemical, and if they are down or disrupted, we are down.

So, it is critically important to focus on the Internet, the software and operating systems that access the Internet because that is the backbone of both economic and communications-wise for us.

We encourage our regulatory agencies and others to look at the software vendors. Similar to what our regulators look at, third-party service providers, to make sure that they are delivering safe and sound practices and security practices within those vendors.

Encourage collaboration and coordination among critical infrastructures and the government agencies to enhance the diversity and resiliency of the telecommunications infrastructure. The NCC, the NCS, used to be an outstanding organization. We did a lot of our early work with them. They were gutted. They have no budget to be able to do the kind of work that we need for them to do.

Invest in the power grid because of its critical and cascading impact on other industries and other critical infrastructures.

And when I talk about invest, I think there are incentives that Congress can put in place to have these other industries make sure that they maintain a resiliency.

Improve the coordination procedures across all critical infrastructures and with the Federal, State and local governments, I don't believe it is working, and I think there is much that we need to do, when we do have a major event.

And last, encourage law enforcement to prosecute cyber criminals. And in particular, on a global basis, because much of the problems we have are not criminals in the United States, they are criminals in the Ukraine or in Asia or in other countries that are attacking our systems here today.

I thank you, Chairman Clay and Members, for this opportunity to testify ensuring Internet resiliency and security in light of the increased cyber-attacks. It is a daunting task, but it is critically important to do so.

Thank you.

[The prepared statement of Ms. Allen follows:]

100

STATEMENT

OF

CATHERINE A. ALLEN
CHAIRMAN AND CEO, THE SANTA FE GROUP

BEFORE THE

UNITED STATES CONGRESS
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION POLICY,
CENSUS AND NATIONAL ARCHIVES
US HOUSE OF REPRESENTATIVES

HEARING ON
CYBERSECURITY: A REVIEW OF PUBLIC AND PRIVATE SECTOR
EFFORTS TO SECURE OUR NATION'S INTERNET
INFRASTRUCTURE

OCTOBER 23, 2007

TESTIMONY OF CATHERINE A. ALLEN
CHAIRMAN AND CEO, THE SANTA FE GROUP

Introduction

Thank you, Chairman Clay, and Members of the Subcommittee and Committee for the opportunity to submit testimony before you today on private and public sector efforts to secure our nation's Internet infrastructure.

My testimony today will address three points:

- The importance of resiliency and security of the Internet
- Important steps the private sector is taking to prevent and respond to Internet disruptions and security threats
- Recommendations for the public sector on ways to improve resiliency of the Internet and coordinate recovery, if disrupted

I am Catherine Allen, Chairman and CEO of The Santa Fe Group, a strategic consulting firm specializing in risk management, fraud prevention, business continuity, payments risk and information security, based in Santa Fe, New Mexico. Earlier this year I retired as the Founding CEO of BITS, a CEO-driven nonprofit financial services industry consortium of 100 of the largest financial institutions in the U.S. BITS is a division of The Financial Services Roundtable.

BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS members hold about $9 trillion of the nation's total managed financial assets of about $18 trillion. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. BITS works with government organizations including the U.S. Department of Homeland Security, U.S. Department of the Treasury, federal financial regulators, Federal Reserve, technology associations, and major third-party service providers to achieve its mission.

The Santa Fe Group is a strategic partner and preferred provider to BITS. The Santa Fe Group has worked with BITS since I was recruited to lead BITS ten years ago. Many Santa Fe Group staff members are former BITS employees. The Santa Fe Group has managed a number of projects for

BITS related to safety and soundness of financial infrastructures. Today we manage the Financial Institution Shared Assessments Program, an industry-led effort that helps ensure security and efficiency in the third-party service provider security assessment process through rigorous standards and safeguards that are being adopted by financial institutions and their service providers. The Santa Fe Group also created the Santa Fe Group Vendor Council, a service provider-led group that takes a leadership role in the financial services industry to discuss issues of security and reliability. This group works with financial institutions and publishes best practices for ensuring the reliability of the systems upon which financial institutions rely, including the Internet. The Santa Fe Group's core capability is risk management consulting for financial institutions on such issues as fraud reduction, safety and security, and payments systems.

I speak today as a subject matter expert, rather than on behalf of BITS or the financial services industry. But because of my past responsibilities at BITS, I will be mentioning some of the work the industry, through BITS, has accomplished in the business continuity and security areas.

Like you, Chairman Clay, I too am originally from Missouri. I grew up in northeast Missouri in a rural area 100 miles from St. Louis. Access to the Internet has brought a multitude of opportunities to my hometown that weren't there in my childhood. Resiliency of the Internet is as critical to economic growth, banking, communications, education and farming in that town as it is to national security. The Internet offers rural Americans access to global opportunities. I now live in New Mexico, another state that is largely made up of ranches, Indian reservations, small towns and rural areas. It too has benefited from global access the Internet provides, from selling art and Navajo rugs to Europeans online, to supporting our national laboratories at Sandia and Los Alamos, to providing the basis for development of the film, alternative energy and aeronautics industries in our state.

A resilient and secure Internet infrastructure that serves as our economic and communications backbone is critically important to economic growth and competitiveness.

Importance of Resiliency and Security

Our nation's competitiveness, economic vibrancy and physical security relies on the security, reliability, recoverability, continuity and availability of information infrastructures and systems, most importantly, the Internet. The information technology, telecommunications and power industries play the most critical roles because they are the underpinnings of the Internet. If there are security threats caused by malware, hacking or denial of service based on vulnerabilities in software, hardware or other components, there are likely to be disruptions. The telecommunications, power and IT industries are interdependent. A disruption in one means a disruption in another.

In the industry where I have spent most of my career — financial services — continuity of services is not only a regulatory requirement, it is essential in managing our reputational, operational and financial risks. Customer trust in the security and continuity of financial transactions is vital to the stability of the industry and the strength of the nation's economy.

The financial sector is both a target for cyber criminals, as organized crime shifts from drugs to fraud and identity theft to maximize revenues, as well as terrorists, who use the Internet for money laundering, communications, and financing. With 9/11, the industry has also become a symbolic target.

The threats to resiliency and security of the Internet include:

- Exponential growth of purposeful, targeted criminal activity, especially by organized criminals.
- Online crimes like phishing, which targets the financial services industry in 9 of 10 instances, are thriving. At any given time, fraudulent websites mimic hundreds of brands.
- Hundreds of software vulnerabilities are discovered each month in various applications, from browser plug-ins to critical business software.
- Even commonly used firewalls and anti-virus solutions from the worlds largest vendors are affected by severe vulnerabilities.

What is important for the Subcommittee to consider is how pervasive the Internet is today, for all types of businesses, for all types and ages of users and for all geographic regions in the world. Cell phones with Internet access can be found in any developing country or at the base of Canyon

de Chelly. Blackberries are used for Internet access from Bejing to Bowling Green, Missouri. Farmers access the Internet to check commodities futures markets and grandmothers download pictures of their grandbabies across the globe.

Major Internet disruptions would not only undermine global commerce and financial transactions, it would disrupt the way we live our lives every day, across the world.

Private-Sector Efforts

The financial services industry has done a great deal to strengthen business continuity planning and to coordinate prior to and during times of crisis. Financial institutions have business continuity plans which they constantly update, refine and test. This is a regulatory requirement and part of our risk management process. Financial institutions are driven to understand and manage IT-related risks because of several factors:

- Reputational risk if systems fail and customer information and transactions are compromised
- Financial risk if electronic payments and transactions systems are breached and fraud occurs
- Regulatory compliance risks if appropriate policies and procedures are not followed

Most financial institutions — and all that are deemed mission-critical to the U.S. economy — are required by our regulators to have recovery operations in place and back-up in a very narrow timeframe if disruptions occur. All are required to have back-up facilities and to be able to transition systems in near real time. If the Internet is down because of vulnerabilities in IT, telecommunications or power, we cannot meet our regulatory requirements.

I want to highlight some examples of the financial services industry's leadership in mitigating some of the risks it faces, because these examples can be models for all critical infrastructure industries.

Members of the financial services industry are sharing information, analyzing threats, creating best practices, and urging the software and technology industries to do more to provide more secure products and services. The financial services industry has established the Financial

Services Information Sharing and Analysis Center (FS-ISAC) and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) to share information on threats and to coordinate and collaborate with government agencies. The FS-ISAC and the FSSCC continue to work with the U.S. Department of Treasury and DHS to promote information sharing and best practices within the sector and across other critical infrastructure sectors such as telecommunications and energy. Most of BITS' work over the past decade has been shared with and adopted by the FS-ISAC and FSSCC as well as being made public and free to the industry.

For many years BITS and others in the financial services industry have urged major software providers to develop more secure software and to accept greater accountability for the software they market and service. This has been part of a larger effort by members of the user community that rely on technology provided by the information technology industry—private-sector companies, universities, and government agencies—to demand greater *accountability* for the security of information technology products and services.

- The *BITS Consumer Confidence Toolkit: Data Security and Financial Services* provides an overview of industry efforts to address data security challenges. BITS is currently working on projects to address key management challenges with encryption technologies and the security of wireless technologies.
- In 2004, BITS hosted a Software Security CEO Summit to bring leaders from the financial services and information technology communities together. We outlined the impact that software vulnerabilities have on the financial services industry, proposed business requirements for software companies, and offered procurement language for financial institutions to use. Following the Summit, we initiated joint work plans with major software providers and developed a best practices guide for patching and testing software.
- In 1999, BITS created the BITS Product Certification Program (BPCP) which provides product testing by unbiased and professional facilities against baseline security criteria established by the financial services industry. A product certification, the *BITS Tested Mark*, is awarded to those products that meet the defined criteria. An option is available for technology providers to meet the product certification requirements via the internationally recognized Common Criteria certification schema. BITS has urged DHS to support efforts to enhance product certification programs, including the Common

Criteria program run by the National Security Agency (NSA) and National Institutes of Technology and Standards (NIST).

- Financial institutions have extensive expertise in educating customers about securing their computers and avoiding the lure of fraudsters. However, financial institutions also know that this is an ongoing challenge. In 2005, The Roundtable's Board of Directors approved the *Voluntary Guidelines for Consumer Confidence in Online Financial Services* and *Critical Success Factors for Security and Awareness Programs of Financial Institution Employee.*
- BITS has been focusing on making email more secure and reliable. Email is a necessary and important means of communication with customers, business partners, and service providers. In April 2007, BITS released the *BITS Email Security Toolkit: Protocols and Recommendations for Reducing the Risk.* The toolkit recommends email technology protocols for financial services, Internet service providers, and other business partners. BITS would encourage government agencies to adopt these protocols too and work in partnership with financial institutions, Internet Service Providers and others to increase the security of email as a communication channel.
- One critical area of security and reliability is that of managing third-party service providers. The Financial Institution Shared Assessments Program, launched by BITS and managed by The Santa Fe Group, is helping to facilitate risk management of service providers, consolidate various security standards, and provide a rigorous program that introduces efficiencies in the service provider assessment process. The Shared Assessments Program grew out of the efforts of the BITS IT Service Provider Working Group, which has been addressing managing third-party risk since BITS' inception in the mid-90s. The Shared Assessments Program is based on two essential documents: the Standardized Information Gathering Questionnaire (SIG), which gives financial institutions a detailed "snapshot" of the security controls at the service provider's location and the Agreed Upon Procedures (AUPs), whose 45 control points can be used by assessment firms or qualified CPAs to create detailed reports regarding the effectiveness of the controls. To date, more than 50 organizations are involved in the Shared Assessments Program and there is increasing interest in overseas firms that provide services to financial institutions. The Shared Assessments effort is based on previous work of the BITS IT Service Provider Working group which developed the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships* and the *BITS IT Service Provider Expectations Matrix.* Other major documents produced through

the BITS IT Service Provider Working Group include the *BITS Key Considerations for Global Background Screening Practices* and *Key Contractual Considerations for Developing an Exit Strategy.*

- Another example is the work BITS did on telecommunications resiliency and diversity. The *BITS Guide to Business-Critical Telecommunications Services* was completed in 2004 based on extensive work by BITS members, participation by all the major telecommunications companies, and involvement by the National Communications System as well as the President's National Security Telecommunications Advisory Council. The guide is a comprehensive tool that is used by financial institutions to better understand the risks and strategies for working with telecommunications companies to deliver more diverse and secure telecommunication services.
- In 2005, BITS urged the FSSCC to establish a committee to outline research and development priorities based on recommendations in the Administration's National Strategy to Secure Cyberspace and National Strategy for Physical Protection of Critical Infrastructures and Key Assets. The FSSCC's R&D Committee, working in partnership with the Treasury Department, issued a list of research challenges designed to further strengthen the security and resilience across the sector and then published a research agenda. The FSSCC research agenda identifies the most promising opportunities for research and development initiatives in the following areas:
    - Secure Financial Transaction Protocol
    - Resilient Financial Transaction System
    - Enrollment and Identity Credential Management
    - Suggested Practices and Standards
    - Understanding and Avoiding the Insider Threat
    - Financial Information Tracing and Policy Enforcement
    - Testing
    - Standards for measuring ROI of CIP and Security Technology

The FSSCC is working in partnership with the Treasury Department and Federal financial regulators involved in the Financial and Banking Infrastructure Information Committee (FBIIC) to develop the Sector Specific Plan (SSP) for the Banking and Finance Sector and research and development priorities. The Banking and Finance Sector Specific Plan SSP was completed earlier this year and joined with 16 other sector specific plans as part of the National Infrastructure Protection Plan (NIPP). The Banking

and Finance SSP outlines a strategy for working collaboratively with public and private sector partners to identify, prioritize and coordinate the protection of critical infrastructure, including information security. It describes how this public-private partnership has become part of the fabric of our sector over the past four years and identifies areas where work remains to be done.

The financial services industry, through the FSSCC and FBIIC, sponsored by the US Department of the Treasury and the Securities Industry and Financial Markets Association (SIFMA), recently completed a pandemic exercise. More than 2,700 companies participated. One aspect of the exercise looked at systemic risks to the sector, including potential disruptions of the Internet if overloaded by demand from people working at home.

Additional examples of these leadership initiatives include:

- The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and Information Sharing and Analysis Center (FS/ISAC) initiatives to strengthen the industry's infrastructure
- Industry's contributions to the National Strategy for Critical Infrastructure Assurance
- Convening of numerous conferences, meetings and calls to bring together leaders and experts to discuss security and business continuity issues
- Developing industry emergency communication tools
- Conducting worst-case scenario exercises for multiple threats, including cyber threats
- Engaging in partnerships with the telecommunications sector and key software providers on interoperability issues
- Compiling lessons learned from 9/11, the August 2003 blackout and Hurricane Katrina
- Publishing best practices and voluntary guidelines, from telecommunications resiliency to recoverability should there be a power failure affecting financial services
- Creating a model for regional resiliency and disaster-recovery coalitions and helped establish ChicagoFIRST
- Collaboration and pilots with the telecommunications industry and National Communications System for diversity and redundancy of telecommunications circuits and facilities

- Public presentations and Congressional testimony that have raised the public's and policy makers' awareness of the interdependencies among the sectors at the same time demonstrating that the financial services sector is far ahead of other sectors
- Publishing a study of industry security investments for the Council on Competitiveness's Task Force on Competitiveness and Security.
- Contributing to the Business Roundtable's publication of "Essential Steps Toward Strengthening America's Cyber Terrorism Preparedness."
- Publishing the Financial Services Roundtable's Report of the Blue Ribbon Commission on Mega-Catastrophes

Recommendations

The 2006 GAO Report, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan* outlines some of the key challenges to establishing a plan for recovering from an Internet disruption, much of which related to DHS legal and organizational issues. It recommends to Congress that it consider clarifying the legal framework guiding Internet recovery. It also makes recommendations to the Secretary of DHS to strengthen the Department's ability to effectively serve as a focal point for helping to recover from Internet disruptions by establishing clear milestones for completing key plans, coordinating various Internet recovery-related activities, and addressing key challenges to recovery planning. Our industry agrees with this recommendation. But there is much more to be done.

Financial institutions are heavily regulated and supervised. Financial regulators, primarily through interagency efforts of the Federal Financial Institutions Examination Council (FFIEC), have issued numerous regulations and supervisory guidance on information technology covering many aspects including management, information security, outsourcing, business continuity planning, and consumer protection. Regulators constantly examine financial institutions to ensure compliance with these dynamic requirements. In response, financial institutions continue to demonstrate that they have adequate controls in place to mitigate these risks.

Collectively, these efforts by financial institutions and the financial regulators are helping to improve the resiliency of the financial services industry, as well as the Internet. We believe these

same practices and policies should apply to the government and other critical infrastructure industries, especially IT, telecommunications, and power.

Several common steps serve as the foundation for many of our tools that are relevant to government programs:

- **Secure and maintain senior management commitment to ensure that organizations have the appropriate incentives, adequate funding, and training for technicians and users.**
- **Assess risks on an ongoing basis and participate in information sharing and analysis programs.**
- **Implement appropriate controls (e.g., access controls, authentication, physical security, encryption, employee background checks, insurance) based on changing risks.**
- **Manage third party providers effectively and focus on critical interdependencies with other sectors.**
- **Establish meaningful metrics to measure and understand risks, assess gaps, and measure progress.**
- **Educate users through training and awareness programs.**
- **Test regularly to ensure that the technology, people, and processes are working effectively at appropriate levels of assumed residual risk.**
- **Measure progress through meaningful and independent audits.**

These steps and risk-based policies need to be adopted by critical infrastructure industries.

Congress can help critical infrastructure industries meet the challenges of a post-9/11 environment in a number of ways. We ask that the committee consider these recommendations:

1. **Recognize that the financial sector is driven by its "trusted" reputation as well as regulatory requirements.** Other industries do not have the same level of regulatory oversight, liability, or business incentives. However, we rely on other sectors because of our interdependencies. Responsibility and liability need to be shared.
2. **Maintain rapid and reliable communication.** Critical infrastructure industries and the public need to have an early understanding of the scope and cause as early as possible when a major event occurs. During the August 2003 blackout, the announcement that the

problem was not the result of a terrorist event alleviated public concerns and made for orderly execution of business continuity processes. Diverse communication channels such as cell phones, wireless email devices, landline phones, and the Internet are necessary. Both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained.

3. **Recognize the dependence of all critical infrastructures on software operating systems and the Internet.** Given this dependence, Congress should encourage providers of software to critical infrastructure industries to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure. In so doing, Congress should support measures that make producers of software more accountable for the quality of their products and provide incentives such as tax incentives, cyber-insurance, liability/safe harbor/tort reform, and certification programs that encourage implementation of more secure software. Congress also could provide protection from US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase.
4. **Encourage regulatory agencies to review software vendors—similar to what the regulators currently do in examining third-party service providers**—so that software vendors deliver safe and sound products to critical infrastructure industries.
5. **Encourage collaboration and coordination among other critical infrastructure sectors and government agencies to enhance the diversity and resiliency of the telecommunications infrastructure.** For example, the government should ensure that critical telecom circuits are adequately protected and that redundancy and diversity in the telecommunications networks assured.
6. **Invest in the power grid because of its critical and cascading impact on other industries and other critical infrastructures.** The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation.
7. **Establish improved coordination procedures across all critical infrastructures and with federal, state, and local government when events occur.** Coordination in planning and response between the private sector and public emergency management is inadequate and/or inconsistent. For example, a virtual national command center for the private sector that links to the Homeland Security Operations Center would help to provide consistency.
8. **Encourage law enforcement to prosecute cyber criminals and identity thieves, and publicize U.S. government efforts to do so.** These efforts help to reassure the public and

businesses that the Internet is a safe place and electronic commerce is an important part of the Nation's economy.

Several years ago, BITS, on behalf of the financial services industry, outlined seven elements that the Government can pursue to strengthen cybersecurity. We call these seven steps **PREPARE.** The full **PREPARE** statement is included in the Appendix to this testimony, but immediately below are several important elements of these recommendations:

Promote: Government can play an important role in promoting the importance of secure information technology.

Responsibility: Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products.

Educate: Government can help communicate to all users of information technology the importance of safe practices.

Procure: Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the information technology industry to deliver and implement more secure systems.

Analyze: Government should collect information and analyze the costs and impact of information security risks, vulnerabilities, and threats and provide this analysis to policy makers.

Research: Government can play an important role in funding research and development in the areas of secure software development practices, testing, and certification programs.

Enforce: Law enforcement must do more to enforce, investigate, and prosecute cyber crimes here and abroad. Government needs to properly fund enforcement.

During the past two years, the Federal government has taken several important steps to strengthen cybersecurity, many of which the financial services industry supported. Examples include:

- Creation and appointment of an Assistant Secretary for Cyber Security and Communications to the Department of Homeland Security (DHS).
- U.S. Senate ratification of the Council of Europe's Convention on Cybercrime, signed by the United States in November 2001.
- Completion of the Sector Specific Plans for all of the nation's critical infrastructures, including the Banking and Finance Sector Plan, as part of the Administration's National Infrastructure Protection Plan.
- Requirements by U.S. Office of Management and Budget for executive departments and agencies to strengthen information security programs.

These are positive steps but much more needs to be done.

Conclusion

I would like to thank you, Chairman Clay and Subcommittee members, for this opportunity to testify. Insuring Internet resiliency and security in light of increased cyber criminal and potential terrorist attacks is a daunting task. It requires the coordinated and collective efforts of the IT, telecommunications and power industries, the user communities like financial services companies, and the government to create the incentives, policies, best practices and technological innovations needed to prevent disruptions where possible and recover quickly when they happen. I would be happy to answer any questions.

APPENDIX

PREPARE

The federal government can play an important role in protecting the nation's IT assets. The following are seven key elements that the U.S. government should support to secure information technology.

Promote. Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government. Some sectors, such as financial services, are heavily regulated and supervised to ensure that customer information is protected and that financial institutions operate in a safe and sound manner. Examples of actions the government can take include:

- Government should lead by example by ensuring that the issue of cyber security receives adequate attention in the Department of Homeland Security. Today, cyber security is handled at a level far below where most corporations handle these issues. Congress could create a more senior-level policy level position within DHS to address cyber security issues and concerns and ensure that adequate funding is provided.
- Strengthen information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), by ensuring adequate funding is made available to Federal agencies sponsoring such organizations. Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. Information sharing among sectors is equally important as cyber threats sometimes reach some sectors before others.
- Create an emergency communication and reconstitution system in the event of a major cyber attack or disruption of information networks. Such an attack or disruption could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry has developed such a plan for industry-specific events in the BITS/FSR Crisis Communicator. Other organizations have developed similar communication mechanisms. These emergency communications programs should be examined as potential models for a national cyber security emergency communication system.

- Reform of the Common Criteria/National Information Assurance Partnership (NIAP). The current software certification process is costly, inefficient, used on a limited basis by the Federal government, and virtually unknown to the private sector. NIAP should be reformed so that it is more cost effective for vendors to seek certification while ensuring consistent Federal procurement practices and expanded commercial adoption of NIAP-certified products. The BITS Product Certification Program may well be able to serve as a model.

Responsibility. Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products. Examples of actions the government can take include:

- Provide tax or other incentives for achieving higher levels of Common Criteria certification. Incremented incentives would help to compensate companies for the time and cost of certification. This should encourage certification and increase the overall security of hardware and software.
- Provide tax or other incentives for certification of revised or updated versions of previously certified software. Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security
- Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is provided. It is vital that critical infrastructure companies receive immediate notice of serious vulnerabilities.
- Establish requirements that improve the patch-management process to make it more secure and efficient and less costly to organizations.

Educate. Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector. Examples of actions the government can take include:

- Fund joint FTC/DHS consumer cyber security awareness campaign. The FTC should focus its efforts on building consumer awareness, and DHS should coordinate more detailed

technical education regarding specific serious threats. In addition, government employees should be trained in proper cyber safety measures.

- Train government employees on proper cyber security measures.
- Educate corporate executives and officers regarding their duties under Sarbanes-Oxley, GLBA, and HIPAA as they relate to cyber security.

Procure. Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems. Examples of actions the government can take include:

- Require high levels of cyber security in software purchased by the government through procurement procedures. Extend such requirements to software used by government contractors, subcontractors, and suppliers.
- Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement. NIST should include software developers and other stakeholders in the standard-creation process.

Analyze. Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers. Examples of actions the government can take include:

- Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and their impact on the economy. Measuring and making these costs transparent will aid law makers and regulators as they assign resources to cyber security programs.

Research. Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and educational/certification programs. Government can help by facilitating collaboration with the users and suppliers of IT to develop standards for safe practices. Examples of actions the government can take include:

- Enhance DHS, NSF, and DARPA cyber security R&D funding.
- Carefully manage long- and short-term R&D to avoid duplication.
- Establish a mechanism to share educational training and curricula.

Enforce. Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad. Examples of actions the government can take include:

- Ratify the Council of Europe's Convention on Cybercrime.
- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a priority among law enforcement agencies.
- Encourage better coordination among law enforcement agencies in order to detect trends.

Mr. CLAY. Thank you so much, Ms. Allen, for your testimony. Ms. Todt Coon, you may proceed.

STATEMENT OF KIERSTEN TODT COON

Ms. TODT COON. Good afternoon, Chairman Clay, and thank you for the opportunity to testify. As was mentioned in the introductions, I am currently a vice president at Good Harbor, and of particular relevance to this hearing, served on the Senate Committee on Homeland Security and Government Affairs, and worked on the Directorate part of the DHS legislation on Internet Protection and Emergency Preparedness.

In the interests of time, I will move pretty quickly to my recommendations.

As the National Strategy to Secure Cyberspace correctly stated, cyberspace is the nervous system supporting our Nation's critical infrastructure. Yet, despite our recognition of this, little has been done and there are several reasons for this, including authority and ownership issues, both in the public and private sectors.

Our Internet infrastructure is vulnerable for several reasons, and I will tackle two of them regarding infrastructure and looking at response capabilities. Regarding infrastructure in our end systems, there are two classes of end systems. There are home users and enterprise. Access to the servers usually by these enterprise users is critical in a time of crisis. If the end systems are compromised, then key response personnel will not be able to access the information they need to respond to an event.

The current challenge with which we are faced is that all information, both critical and non-critical, is transmitted over our information networks and treated equally. For example, if this Nation is confronted with a pandemic like the avian flu, our information networks as they currently exist will experience disruptions and outages that will paralyze us and prevent us from executing an effective emergency response.

The second area of weakness I will discuss in this brief statement is response capabilities. Our response capability is critical because obviously we are not able to guard successfully against all threats. We don't have a back-up system at this time that can be activated in the event of a widespread Internet failure. And we have not developed scenarios for potential attacks on our Internet infrastructure.

Experts disagree on the magnitude of risks and what needs to be done. And what is important that we routinely use this lack of consensus as an excuse for inaction. Until we reach agreement on these issues, we will not be able to prepare for imminent attacks.

So I offer today the following recommendations. The Internet was designed for the purpose of openly sharing information. The question then with which we are posed is how do we impose the secure exchange of information on top of an open sharing environment.

We should create a three-tiered system that allows our networks to identify and prioritize in the following order. First, critical communications supporting government operations, business and first responders. Second, routine business information, and third, non-critical information. In a time of crisis, we must be able to ensure that critical information is being delivered with priority speed and

that it is not encumbered by non-critical information being sent simultaneously.

We must also develop back-up systems and conduct scenario planning. If we experience a life cycle attack, we would need to have the ability to reboot the Internet. We should have reserve network protocols and we should maintain back-up parallel systems that can replace the active systems and bring up the critical portion of the Internet in the time of crisis.

And we should develop a playbook for scenario planning. And I assert that this is different than exercise. Scenario planning is different than exercises. Scenario planning would push us to identify and conceive possible responses to a serious attack. We need to think through how appropriate players in both the public and private sectors will respond and we need to examine our current authority and ownership issues within both the government and the private sectors.

I now submit to you a final recommendation. One of the first steps we need to take in preparing ourselves for an information infrastructure failure is to set risk standards. However, we can't set risk standards if we don't know what the risk is.

I commend this committee on its work with FSMA because I think FSMA has done a good job with defining cyber security. I also propose a National Cyber Risk Assessment to be conducted by a blue ribbon commission of experts who would be responsible for defining the risks that exist. The only way we can begin to adequately prepare ourselves is to commit to possible scenarios. The assessment would inform the scenarios and enable us to assign ownership and controls. The Office of Management and Budget should provide the resources, the direction and the oversight and leadership for this assessment.

In conclusion, experts and observers postulate that we do not have to be worried about hackers taking down the Internet because hackers would not intentionally bury their playground. But our greatest risk does not come from hackers. It comes, as was mentioned before, from foreign governments that can ably and quietly use the Internet infrastructure for espionage and other nefarious purposes.

The threat is particular strong from governments that have developed their own internal Internets, such as China, and would therefore not be severely affected by a worldwide disruption.

Recent events have demonstrated that these scenarios are not possibilities, but realities. Our national security, the health and well-being of the community, and the daily functioning of our society depend on the security and resiliency of our infrastructure.

We have a responsibility to define the Internet infrastructure risk that exists and to plan for that risk appropriately. And we have a responsibility to act. I assert that we must act now.

Thank you for the opportunity to testify before you today.

[The prepared statement of Ms. Todt Coon follows:]

GOOD HARBOR
CONSULTING, LLC

Prepared Testimony of
Kiersten Todt Coon
Vice President, Good Harbor Consulting

Before the Information Policy,
Census, and National Archives Subcommittee, Oversight and
Government Reform Committee

"Cybersecurity: A Review of Public and Private Sector Efforts to
Secure our Nation's Internet Infrastructure"

Room 2154, Rayburn House Office Building
Tuesday, October 23, 2007
2:00PM

4100 N. Fairfax Drive • 3rd Floor, Suite 301 • Arlington, VA 22203-1629
Tel: 703.812.9199 • www.goodharbor.net

INTRODUCTION

Good afternoon Chairman Clay, Ranking Member Turner and Committee Members. It is a pleasure to testify before you today on this nation's ability to secure its Internet infrastructure. I am currently a Vice President at Good Harbor Consulting and have worked on the issue of infrastructure protection in previous positions at Business Executives for National Security (BENS) and as a Professional Staff Member on the Senate Committee on Governmental Affairs (now Homeland Security and Governmental Affairs). In this capacity, I was one of the drafters of the legislation to create the Department of Homeland Security. Of particular relevance to this hearing, I was responsible for drafting the language to establish an infrastructure protection directorate.

I would first like to commend this Subcommittee for astutely identifying and choosing to examine a significant gap in this nation's ability to protect itself. This country and the world have come to depend on the Internet for all critical functions that keep commerce, the economy and our governments operating. Significant disruption to the Internet will wreak havoc on this nation's ability to function. We have a responsibility to develop and commit to a comprehensive plan to prevent, detect, respond to and recover from a cyber attack on the Internet or a similar systemic failure.

BACKGROUND

As the "National Strategy to Secure Cyberspace" correctly stated, "cyberspace is the nervous system supporting our nation's critical infrastructures." We know that the majority of Internet infrastructure is owned and operated by the private sector. Therefore, any plan developed by the government for protecting this nation's infrastructure must be a result of public/private collaboration.

The government acknowledges this need. In December 2003, the President updated a national directive for federal departments and agencies to identify and prioritize critical infrastructures and key resources. This directive recognized that since most critical infrastructures are owned and operated by the private sector a public/private partnership is crucial for the successful protection of these infrastructures.

However, little progress has been made on this issue. It is not enough to provide guidance on what needs to happen; rather, we must identify the roles and responsibilities within the public and private sector during a disaster.[1] The models for cyber security public/private collaboration that exist outside of the government are reasonable. However, within the Department of Homeland Security (DHS), there is a notable lack of cooperation and information sharing between the public and private sector on these issues. What is lacking in this area is a concrete

[1] For example, the Cyber Annex of the current National Response Plan, which recommends creating a committee, leaves it up to the government to determine who from the private sector should be included, at what point the private sector should be included and at what level the private sector should be included.

understanding of the risks that exist, the points of failure, a clear definition of the parameters of the issue and solutions that address these issues.

CURRENT ENVIRONMENT

The recent exponential increase in our reliance on the Internet puts information infrastructure at the center of fundamental business and government operations, thereby making them more vulnerable. According to a recently released Business Roundtable (BRT) report entitled, "Growing Business Dependence on the Internet, " The World Economic Forum estimates a 10 to 20 percent probability of a breakdown of the critical information infrastructure in the next ten years. Additionally, it estimates a resulting global economic cost of approximately $250 billion. The pervasiveness of the Internet in business and government functions means that a cyber catastrophe would be devastating.

The consequences of Internet failure would significantly affect the economy. According to the BRT report, in a study of 66 security breaches between 1996 and 2001, the Congressional Research Service (CRS) found that there was a 2.1 % decline in stock value for affected firms once they released the information – and a 2.8% reduction in value for those companies highly dependent on the Internet. CRS found that the impact is much greater if an Internet failure lasts longer than a day or two – with a reduction in stock price of 2.7%, relative to the rest of the market on the day of the attack, but a 4.5% drop three days later. For perspective, a 4.5% drop in the DOW Jones today would result in a reduction of approximately 600 points.

Additionally, an Internet failure can compromise our national security – an issue that has been demonstrated by recent events. The vulnerabilities within our information infrastructure must be addressed; previous breaches and disruptions demonstrate the loss that is likely if comprehensive public/private action is not taken quickly. In order to identify how to strengthen our infrastructure, we must first identify critical points of failure.

POINTS OF FAILURE

Infrastructure: Routers and End Systems

Routers

We currently rely upon a small number of key service providers (usually referred to as Tier 1 providers). These providers are the backbone of the Internet and if they were successfully attacked, there would be widespread disruption. Our routing infrastructure is robust enough to handle a single, non-malicious router failure; traffic would flow in an alternate way. However, our routing infrastructure cannot sustain the loss of an entire line (i.e., the loss of all Cisco routers on the network because of a lifecycle attack) of routers.

End Systems

There are two classes of end systems – home-users and enterprise. Home-users are highly vulnerable to attack, the most prevalent on the Internet and consume the majority of Internet

bandwidth. Access to the servers, usually by enterprise users, is critical in a time of crisis; if these systems are vulnerable and compromised, key response personnel will not be able to access the information they need to respond to the event.

The current challenge with which we are faced is that *all* – critical and non-critical – information is transmitted over our information networks and treated equally. Additionally, more information is being transmitted over these networks than ever before. We can expect that in the very near future, most internet users will be streaming data-rich video into their homes, using the web for online games, performing all banking and financial functions, practicing telemedicine and having voice conversations.

As we increase the amount of information running over the Internet without strengthening the systems, we are burdening our information networks; we are burdening this critical infrastructure upon which our country depends for daily functioning and crisis management. As with any infrastructure, we must strengthen it to accommodate the changes and increase in use. We must also adapt its capabilities to manage its most urgent and critical functions.

When this nation is confronted with a pandemic like the avian flu, our information networks, as they currently operate, will experience disruptions and outages that will paralyze us and prevent us from executing an effective emergency response. Additionally, these overburdened networks will prevent key personnel from accessing critical systems remotely. For example, if quarantine measures are instituted in a region(s), will government services be able to continue to operate through remote access by key personnel?

Response Capability Challenges

An efficient response capability is critical and necessary because we will not be able to guard, successfully, against all threats. Currently, we do not have a backup system in place that can be activated in the event of a widespread Internet failure. Additionally, we have not developed scenarios for potential attacks and responses to Internet infrastructure compromises. Although we continue to discuss the realm of risk that exists, we have not defined specific risks or their parameters. Experts disagree on the magnitude of risk and what needs to be done and we routinely use this lack of consensus as an excuse for inaction. Until we reach a reasonable consensus on these issues, we will not be able to prepare thoroughly for imminent attacks.

RECOMMENDATIONS

Infrastructure

Routers

- We must have diversity in the service providers we use; we should develop multiple sources for routing to reduce our risk of losing a router. An individual is advised to diversify his/her stock portfolio to reduce risk of losing one's life savings; we should

employ a similar tactic of router diversification to reduce the risk of losing core components of our Internet infrastructure.

- We need robust architecture within and among routers and service providers. This architecture should be constructed in such a way that if a service provider goes down, we don't lose it – similar to the way a ship is constructed. If water enters a compartment of a ship, the ship has the ability to contain the leak and continue to operate. We must be able to shut down a malfunctioning or contaminated component of the router system without losing the entire router.

End Systems

The Internet was designed from a research and development project within the Department of Defense for the purpose of openly sharing information. The challenge with which we are now confronted is the ability to impose the secure exchange of information on top of an open sharing environment. We must upgrade our networks and develop a system that prioritizes Internet traffic. In a time of crisis, we must be able to ensure that critical information is being delivered with priority speed and that it is not encumbered by non-critical information, which is being sent simultaneously.

We should create a three-tiered system that allows our networks to identify and prioritize in the following order: 1) critical communications supporting government operations, business and first responders; 2) routine business information; and, 3) non-critical information. Such a system will also allow us to categorize the critical traffic for those individuals who need to access it and to stop non-critical traffic in order to make more bandwidth available for the purposes of response and recovery activities.

In its report issued in June 2006, the Government Accounting Office (GAO) similarly recommends establishing a system for prioritizing recovery of Internet service similar to the existing Telecommunications Service Priority Program. The report states that we need to prioritize Internet traffic, but that this idea of prioritization currently faces numerous technical challenges and is not supported by legislation. We need to address these challenges and work with Congress to reach a solution.

Response Capabilities

Backup Systems

Because we cannot protect ourselves against every possible threat, we must develop sufficient response capabilities. Just as an early diagnosis of cancer can save a life, early detection and effective response to a malicious Internet event can prevent significant disruption.

One capability we must develop to ensure a resilient infrastructure is developing a backup system. If we experience a life cycle attack – where a piece of malicious code infects every router – we would need to have the ability to reboot the Internet. We should be maintaining backup parallel systems that can replace the active systems in a time of crisis. We must also

have reserve network protocols and set aside clean backup systems that can bring up the critical portion of the Internet (which could be easily identified with a tiered network system) quickly.

Scenario Planning
We should develop a playbook for scenario planning which pushes us to identify and conceive possible responses to a serious attack – responses geared toward systems administrators all the way up to the President. A significant attack would likely affect the infrastructure of one of the top three critical industries – power/utility, banking or telecommunications. Each of these industries is developing its own solutions for safeguarding the infrastructure upon which its business depends. However, as a nation, we need to think through how appropriate players in *both* the public and private sector will respond. The creation of scenarios will enable us to develop response options before an incident occurs and identify:

- Needed resources
- Additional R&D activities
- Existing engineering options

By not defining or agreeing upon the risk that exists, we prevent ourselves from following through on preparedness activities. It is not enough to establish that a risk exists; we must be able to define roles and responsibilities and assign accountability so that we have ownership of the issue.

NATIONAL RISK ASSESSMENT

One of the first steps we need to take in preparing ourselves for an information infrastructure failure is to set risk standards. However, we can't set risk standards if we don't know, concretely, what the risk is. Moreover, if we don't understand the consequences, we cannot develop solutions, policy, priorities and investment levels. One of the primary challenges that exists within DHS is the Department's lack of ownership on this issue. For example, why isn't the Cyber Warning Information Network[2] the responsibility of the Assistant Secretary for Cyber Security and Communications? When confronted with a disaster of any kind, it is unclear who will take responsibility and ensure an effective response.

Consequently, I propose, as others have in the past, conducting a National Cyber Risk Assessment. A blue ribbon commission of experts, who would be responsible for defining the risks that exist, would conduct this assessment. We, of course, recognize that incidents may occur that do not align perfectly with the proposed assessment, but the only way we can begin to adequately prepare ourselves is to commit to possible scenarios. This assessment will therefore inform the scenarios and inform the right level and type of response. Additionally, a National Risk Assessment will enable us to assign ownership and response roles.

[2] The expansion of the Cyber Warning Information Network (CWIN) was recommended in Priority I of the National Strategy to Secure Cyberspace to play a coordinating role with the US-CERT to provide coordinated crisis management. To date, CWIN has not received appropriate funding or attention.

The Office of Management and Budget (OMB) should provide the funding, resources, direction, oversight and leadership for a National Cyber Risk Assessment and will be responsible for ensuring the recommendations from the commission are executed.

PUBLIC/PRIVATE PARTNERSHIPS

The phrase "public/private partnership" has lost its meaning. We use it so often without any result that it has become a cliché. Effective models for partnering the public and private sector exist, but failure has come from a lack of execution that has prevented the assignment of responsibility or accountability. However, public/private collaboration is necessary in developing efforts to secure our nation's infrastructure because ownership of this infrastructure resides primarily in the private sector.

The challenge that currently exists is that the private sector, as cited in the Business Roundtable Report referenced previously, believes that government has the primary role for restoring business operations following a major Internet disruption. In contrast, government believes industry sectors have recovery plans that will restore service.[3] What is evident is that both have a responsibility, but neither is adequately prepared.

Stafford Act Revision

As we examine public/private partnerships and this country's response to natural and manmade crises, we recognize and know that government or industry cannot and should not respond without support from each other. Multiple post-Katrina reports discuss the roadblocks – literally and figuratively – that prevented altruistic private companies from donating needed supplies. Many of these reports cite the need, in our current environment, for revision to the Stafford Act.

This revision would also apply to our information infrastructure. For example, if there were a sudden attack on the Internet that caused critical hardware and software infrastructure to irrecoverably crash, the backbone of the Internet would collapse. Through Presidential Directive(s), the Department of Homeland Security could force key information technology vendors to prioritize the delivery of goods and services to the recovery effort. We should examine the Stafford Act to identify the benefits from establishing specific government authority to provide for-profit companies – such as those that own or operate critical communications infrastructures – with limited assistance during a crisis.

CONCLUSION

Experts and observers postulate that we do not have to be worried about hackers taking down the Internet because hackers would not intentionally bury their playground. But our greatest risk does not come from hackers. I would like to leave you with the assertion that it comes from

[3] The 17 sector approach to infrastructure protection has thwarted cross-pollination of information sharing and methods across sectors. As industry and government examine effective partnering, it should examine and reconsider this model.

foreign governments that can ably and quietly use the Internet infrastructure for espionage and other nefarious purposes, especially governments, such as China, which have developed their own internal Internet and would therefore not be severely affected by a worldwide Internet disruption. Recent events have demonstrated that these scenarios are not possibilities, but realities.

Our national security, the health and well-being of our community and the daily functioning of our society depends on the security and resiliency of our infrastructure. We have a responsibility to ensure that we have defined the information infrastructure risk that exists; we have a responsibility to plan for that risk appropriately, through dynamic and well-defined public/private partnerships. We have a responsibility to act and to act now.

Thank you for the opportunity to testify before you today. I look forward to answering your questions.

Mr. CLAY. Thank you very much. I will ask the panel several questions, and I would love to hear responses from the entire panel. We will just start at this end of the table with Ms. Todt Coon, and go down the line.

The first issue is, regardless of which sector of the economy we focus on, all of them have significant levels of dependence on the Internet for their operations. It seems, however, that we spend more time focusing on the risk of 17 different sectors, as opposed to the broad risk associated with the disruption of a key critical asset, such as the Internet.

First, should we begin to move away from establishing levels of risk for each specific sector, and move toward establishing risk models according to specific assets or critical functions, such as telecom, Internet or infrastructure resiliency or the security of our power transmission assets?

Ms. Todt Coon, let's begin with you.

Ms. TODT COON. Thank you. That is an excellent question, and it is obviously a question that we are confronted with in looking at how we have organized our sectors.

I think some would assert at this point that the sector model is sophisticated in a way that is almost too sophisticated for us to manage right now, because the reality of how we are handling the sector issue is that it is stalling us and preventing us from making the progress that we could on information infrastructure protection.

I would reference a report that was recently released by the Business Roundtable which talks about public/private partnerships. And it talks about the fact that the private sector incorrectly believes that government is developing response plans and that the Government believes that the industry structures will have their recovery response plans.

We recognize that both the public and the private sector have a role but neither is adequately prepared.

Having said that, I would like to reference, I think, a model within the private sector and its coordination with the public sector that has worked effectively. And that is the FBIIC model, which Ms. Allen has referenced. It is the Financial and Banking Information Infrastructure Committee.

Post 9/11, the financial sector was obviously concerned about the anticipation of what could happen to our banking and financial markets. Through the committee, the Fed reached out to 11 financial institutions—reached out to the banking industry, and said we are going to talk to 11 institutions, we are not going to tell you who they are. Obviously if we talk to you, you will know you are one of them. And if not, you are not.

And they worked with these institutions to create a security and resiliency plan. And Ms. Allen, I am sure, can talk to this in greater detail. But what this collaboration reflected was the clarity of Government purpose, and it also reflected industry working within a Government strategy.

And one of the reasons why I think this was effective, was that the Government was able to leverage its institutional knowledge. The way that we have currently organized with DHS is that we have split the ownership roles across different agencies and enti-

ties, both on the cyber side, but we see it with energy and with other structures.

And what I would propose is that we look at how the Government can institute this integrated approach to industry protection in a more collaborative way that doesn't silo this protection issue.

Mr. CLAY. Thank you for that response.

Ms. Allen.

Ms. ALLEN. I agree with everything you just said, and I would add to it, you can't boil the ocean. And I would pick five infrastructure groups to first coordinate and use that as a model for the others. And that is, the IT, the Internet, the telecom and the power, because they are absolutely interdependent.

Then I would add financial services, because if that is down, then you are going to have a major problem with the economy and the confidence of the people. Last, first responders, so that you are taking care of the first responders.

If you could look at integrated programs across those five groups, with the Government, that would be the starting point. And I think the FBIIC model, that the financial sector developed is the right model.

Mr. CLAY. Should it all be Homeland Security's responsibility? [Laughter.]

Well, maybe Ms. Todt Coon should answer that. You helped design——

Ms. TODT COON. Well, I don't have a lot of confidence. Let's just say that there has been many, many attempts to have this happen under DHS and it has been very difficult for it to be effective. So I think it is really going to take absolute administrative support. I am in support of a blue ribbon commission and then maybe DHS responds back to and does whatever this commission says it needs to do.

But I don't think that it is going to come the way that we have it structured now.

Mr. CLAY. All right. Mr. Clinton.

Mr. CLINTON. Mr. Chairman, I think that is a very thoughtful question. And I have been trying to listen to my colleagues to get a good answer for it, while I have been thinking of it myself.

Here is my off-the-cuff view on it. First of all, we at the Internet Security Alliance have never embraced the sector model. The Internet Security Alliance is built on an entirely different model. We are a cross-sectoral organization. We have the defense sector, IT, banks, Coca-Cola, food service. Only because when you are dealing with the Internet, it is all ones and zeroes.

So we all have the same problem, although, at a sub-structural level, there are individual sector orientations within. So, the sector model, I think, was entirely the wrong way to go, fundamentally. And when I say we ought to rethink things, that is one of the places where I would suggest we begin.

The second question, and this kind of gets to your followup question a little bit, has to do—when you say, what should we be doing. That is a really critical question. Who is the "we" you are talking about, sir? I think it is appropriate for you to be thinking, well, should this be DHS? And my answer is no, it shouldn't be DHS. It can't be DHS. If we try to shove this into DHS, even if we hire

Catherine Allen to run DHS, I am still not sure that they are going to be able to do it. They are a U.S. Federal Government institution trying to deal with an inherently international infrastructure that is owned and operated 95 percent by the private sector.

Trying to get this done through DHS or the Internet Commission on Wonderfulness is not going to work. We have to understand that we are dealing with an entirely different model. We have to find a way to work together with the private sector. The private sector is constantly—the major players, anyway—are constantly doing risk assessments. They are constantly upgrading their systems.

As I said in my testimony, they are not waiting for DHS. And we work cooperatively with DHS. I am not going to bash DHS. But the system is being run by the private sector. That is never going to change. We have to find a way that Government understands its role. And its role is not to manage, to dictate, to be the parent here. Their role is to be a major user who works with all the other major users.

Now, obviously they have a separate role in terms of national defense that we could deal with differently. But my suggestion would be that the way to go about this is to harden the entire system. Not to identify what the one particular risk is because that is a static moment in time.

This past week we had a major conference at ISA where we looked at securing the IT supply chain. Talk about a major problem. There is nothing that is not in the IT system that is not researched, resourced, developed, assembled, whatever, someplace. And some of the places this stuff is made can be a little bit scary.

How do we secure the supply chain? And we looked at all the risks. And we said this is the area where we have the greatest vulnerability. We looked at it for a minute, and we said, well, as soon as we established that as the major risk vector, the guys who are attacking this aren't stupid. Move it over to here.

So the risks don't stay static. We need a full systems solution that is sustainable on a long term basis and that is why we argued for a system of market incentives. We have to make the owners and operators realize that it is in their self-interest to continually upgrade and build-out the system, including the Federal Government's, and that is, we think, the answer to the approach that you are suggesting.

Mr. CLAY. Thank you for that response.

Mr. Silva.

Mr. SILVA. I think that you have brought up a couple of interesting questions here, and I thank you for the opportunity to respond to them.

It is interesting, when you really think about throughout time, we have kind of decided that we would handle this in a sector-specific way and that's just sort of how it worked itself out. In fact, the ISACs themselves were created as sector-specific to a large degree.

And there are problems that are sector-specific. For instance, financial institutions have a more interesting set of threats unrelated to the infrastructure itself, but more around IT security and around the practices of being online for a bank or other financial institutions.

But there are a lot of overlapping infrastructures, and those infrastructures certainly include the Internet itself, which all by itself is very insecure. I mean, the Internet itself doesn't offer any security. It really doesn't. Most of the security is handled either through appliances or through the applications themselves. But the Internet itself was designed to be an open system with really zero security measures to it at all.

So I think that we need to look at the Internet infrastructure and its resilience and whatever security mechanisms we need to put in place to make sure that it continues to stay up, and the international aspect of it needs to be something that is looked at commonly across all of the sectors.

Now you did ask what we should be doing and, as Mr. Clinton pointed out, what we should be doing is dependent upon who "we" is. Since the private sector is responsible for most of the infrastructure on the Internet, it is incumbent upon the private sector to take action.

I think if we beg for too much regulation from the Government, we will get exactly what we asked for, and I don't think that would be a pleasant situation, either.

But as Mr. Clinton pointed out, incentives are probably the best tactical step that could be taken with long term effects that I think would be positive. Unfortunately, when we look at building out the infrastructure, say, for the next generation of the Internet protocol—which by the way that next generation of Internet protocol was developed a decade ago, and still has yet to be implemented literally. IP Version 6 has been pretty much standardized for a number of years and is the best technology yet to come, still.

But there is no incentive for telecommunications providers or Internet service providers to deploy it. There aren't any customers and it is a chicken and egg kind of thing. There is more secure, more robust protocol, and some would argue that it is not necessarily more secure and I might be one of them. But it hasn't been deployed because there are no customers for it. There are no customers for it because it doesn't exist.

The Federal Government is a big enough customer that if they demanded it as part of their infrastructure, and their infrastructure build-out and used their market influence, their buying power, then those kinds of protocols and those kinds of enhancements would be made, if demanded by the Government as part of the procurement process.

Thank you.

Mr. CLAY. Thank you for that response.

Mr. Sabo.

Mr. SABO. Well, summing up after that, or coming to a conclusion, a couple of things I would say with respect to the basic question.

There are risk assessments that can be applied generally to what we see as the infrastructure. And some of that work is happening now. The IT-ISAC and the Sector Coordinating Council, in fact, have work groups of industry experts attempting to look at the key functionality provided by the infrastructure and the sub-functionality, and attempt to build a risk assessment methodology that actually might make some sense.

If you do a static risk assessment, although I respect the idea of bringing in experts and assembling for many months, we have had many of those studies. You can look at the literature and you can see a number of recommendations made by academicians and by industry experts that are sitting on the shelves because the Internet and the infrastructure are very dynamic. And, as Mr. Silva pointed out in his statement, a number of threats to the infrastructure are not on the infrastructure, it is on the applications that ride on the infrastructure and that impact the utility of the infrastructure.

In the financial sector, a number of attacks are based on social engineering. And those attacks open up and expose vulnerabilities, the vector of an attack that can be used much later to go after the infrastructure.

In a way, we have a very organic Internet infrastructure. The components of it, such as software itself or a domain name service resolution or some of the other pieces of it, are all components which lead to the vulnerabilities which actors can use when they decide to make an attack.

So a couple of things. One is, work needs to happen cross-sector and I agree with that, and it is actually starting, but it has not really moved far enough along. Work also has to happen by the users of the infrastructure, and that is, the major sectors and the major corporations and companies in the sector. And to some degree that is addressed by the type of regulatory environment in which financial services operates. It is not addressed in many other environments and yet the work needs to be done.

So I think it really is a combination of both looking at the risks associated with the use of the network infrastructure, for example, by control systems, the use of the infrastructure by the major corporations, but also by the industry that writes the hardware/software and operates resolution services and security services for the infrastructure.

You can't look at it, I think, as one simple solution. You have to recognize how complex the beast is, and you have to let, actually encourage, which was the purpose of my testimony for the ISAC, that where industry is stepping forward to address these issues, Government's best role is to foster and encourage through appropriate incentives. And not all monetary incentives. They could be incentives such as saying we encourage you and we will support some of these activities, to move forward with that.

And I think to conclude, the Roundtable Report is an eye-opener. Because what the Business Roundtable found in its report says that we are increasingly and fundamentally and almost totally becoming dependent on this IT infrastructure which is network based. And in that interdependence, we are losing our capacity to go backward. We are losing our ability to go back to older systems. We are losing our ability to fall back to paper systems. Therefore it is imperative for us as a Nation to take the steps to do what you just said; do an active risk assessment, put in the types of controls we need, do some of the strategic work that is academically based, but have a proactive operational plan to move forward.

If all we are going to do is write more papers, do more commissions, do more studies, we are going to hopelessly fall behind. And

so I think being active, looking at the uniqueness of each sector, what the companies are doing, what the practices are, as well as looking cross-sector at some of the functions, is a combination way to go.

And then from a congressional perspective, avoiding regulation but perhaps looking to measures and to saying to us who are in these sectors, what are some performance measures that you are using to evaluate your effectiveness. What steps are you taking. What outcomes are you offering.

And to me that would be the most effective short-term approach.

Mr. CLAY. Thank you for that response. One more question for the panel. Is the extension of the Federal Terrorism Reinsurance Backstop program an adequate model for Government to provide economic security to the private sector in the event of a major Internet disruption? Do we have effective risk models to determine the cost and potential exposure to the Government for covering this type of incident? We will start with Ms. Todt Coon.

Ms. TODT COON. I would go back to—I appreciate the comments of the panelists, but I continue to assert that we have not defined the risk in a way that allows us to create a model, in response to your question. By not having this accountability and by not defining this risk, we are being stalled with inaction.

And while there has been action in different components, as we cited earlier—I think what the financial sector has done is exemplary and noteworthy—as a whole, we have not made the progress on these issues that we are looking to do.

And I think at the end of the day, in looking at what the public and the private sectors have done, as we cited earlier, looking up multiple post-Katrina reports, we recognize that neither the public nor the private sector can respond individually. They need to work together. And Katrina showed us that the ways in which they work together currently aren't working properly.

And so I would encourage us to look at legislation, like the Stafford Act, to revise to include for-profit companies and also look at the Defense Production Act, which if leveraged correctly by DHS could support the work that they are doing. And I think that legislation exists out there within which we need to work. And that we also need to be assigning the ownership and responsibility in a more clear way that allows those entities responsible for this to act accordingly.

Mr. CLAY. Thank you for that. And, Ms. Allen, the Terrorism Reinsurance Backstop program, is it an adequate model?

Ms. ALLEN. It is not adequate. I think it is a good thing, but it is not adequate. Again, I agree that there is not an appropriate risk model. We don't yet understand the cross-sector impact. I think there are other incentives, including insurance, the ratings agencies, tax incentives, Government procurement, that might be more effective in the short run.

And that is my answer.

Mr. CLAY. Mr. Clinton.

Mr. CLINTON. I think I would agree that it is a useful model, but some important differences have to be realized. First of all, cyber insurance is a very different animal than traditional insurance. The cyber insurance market has not taken off at all. It has been

stagnant for 5 or 6 years, about 20 percent of companies have cyber insurance. And there are things that the Government can do to help in that area.

So, if you are talking about cyber, the model is probably worth looking at, but there are other things that need to be done. And my colleagues are exactly right with regard to you can't assess the risk.

Let me quickly tell you what the core problem is with cyber and then in my written testimony I go into a little bit more depth on insurance. I won't bore you with that now.

But the problem with cyber insurance, it is available. But the problem is, nobody buys it. And the reason nobody buys it is because it costs too much money. And the reason it costs too much money is because since there isn't adequate actuarial tables, the businesses that run the cyber insurance naturally set the risk at maximum and therefore the prices are at maximum.

The Federal Government could do a tremendous service by coming in and working with us so that we get the data appropriate so that we could set actuarial tables which would bring more providers into the market. Currently one company, AIG, has 85 percent of the market. That is not a good thing.

If we got more providers into the market by providing them with the data, which expect the Government does actually have, that would then lower the cost. By lowering the cost, now more providers will get in. That will increasingly lower the cost, which has two major benefits.

First of all, if you have a cyber Katrina right now, there is virtually nobody covered. Which means the insurer of last resort is going to be the Federal Government. The Federal Government is going to be stuck with a billions and billions and billions of dollars bill. It is going to be worse than Katrina because at least there was some insurance down there. There isn't in a cyber Katrina.

Second, once we have insurance available and being purchased broadly throughout the market place, insurance can be, in addition to other incentives, and I would endorse Cathy's comments in that regard, but insurance can be a tremendous incentive.

We use insurance all the time to motivate pro-social behavior. Good driving behavior, good health behavior. My daughter is desperate to get really good grades because it is going to lower the insurance on her car. This can drive better behavior. And what I have argued in my testimony is, the way to have a fully resilient, consistent, consistently up-growing system is to have market incentives. Insurance is a great one. So that people will constantly want to adopt the best practices, get the lower insurance rate and the industry and the Government is therefore covered if we have a major event.

So, it is a good model, but there are a variety of things that we have to do to make it work, particular in the cyber arena.

Mr. CLAY. Thank you for that response.

Mr. Silva.

Mr. SILVA. Thank you. I don't know that level of assistance is necessarily everything that we need. And there has been a lot of discussion about how difficult it is to assess the risk. And I don't know about assessing the risk because I think each individual ele-

ment of this could assess what they believe is a risk and then somehow we could wrap that up. It is difficult to assess now.

What is even harder to assess is what the level of damage is going to be. And it will be more than we can even imagine sitting at this table. We couldn't have imagined the damage that happened during Katrina and when we sat and tried to plan for that ahead of time.

But the damage that would have happened from even shutting down the Internet for a couple of hours in the middle of a trading day or the middle of a business would be catastrophic. It would be huge. And if something so serious occurred that we had to reboot the Internet, so to speak, it would be a significant amount before that recovery would actually take place. There are so many different players.

But one of the things that I worry about, in addition to those attacks that come from a terrorist act, if you will, or some malicious behavior, are those sorts of things that might create a self-inflicted wound. In our zeal to try to improve the Internet, in many cases, we make it more complicated and in fact create new and additional risk that we should think through a lot more carefully before we do it.

One example of that is internationalized domain names. There are proposals to create internationalized domain names in order to let countries create domain names, the name of Web sites, if you will, in Cyrillic or Arabic, etc. The problem is that because of a lack of careful action and careful planning on this, other countries are on their own racing out to create another Internet, if you will, that uses the Internet we are used to, but works in a completely different way.

So the rules and regulations that we would create and the policies that we would create as industry sectors and as governments wouldn't apply to these people. Therefore, we have to take corrective action for whatever the weakest link is going to be, and carefully think through some of these improvements that we think are improvements, and make sure that they are not actually creating more complexity and more confusion for users and more confusion for the people who have to assess threats and damage.

Mr. CLAY. Thank you for that response.

Mr. Sabo.

Mr. SABO. I think an approach to this is to give a chance to the mechanisms that have not been given a chance to work. It is a complex environment. We have never been in a situation where millions of individuals scattered around the whole United States, or for that matter, the world, could literally have an impact on a national economy.

We have never been in a situation where people living—and it has been rare—but if you think of a physical event and the insurance for terrorism, it might be very applicable to that. But we are dealing with a much different animal.

Mr. CLAY. Mr. Sabo, let me interrupt you. Are we too dependent on the Internet as a society? As a world? Mr. Clinton is saying there is no going back. There is no way to go back to the paper or anything else. Does that make us too dependent on the Internet?

Mr. SABO. We are dependent on it. And it is increasingly so. And we can't stop that because the nature of us as human beings, the nature of the capitalist society and the development of many uses of information and new technologies, simply can't be arrested without some dramatic shift back to a society of almost the Stone Age. You can't do it.

Having said that, and knowing the complexity that we do, my suggestion is that we give an opportunity for measures to begin working slowly to address different aspects of this. So one aspect is Internet resilience and some of the things that Ken is talking about.

Another aspect is expectations of companies as noted in the Business Roundtable to take steps, good steps, to deal with business continuity practices. Another example would be looking to industry through the ISACs and so on, to address vulnerabilities.

And by putting this together in combination, you have some opportunity to see progress against a set of measures. But if you just look at it in terms of—particularly with the Internet, as Ken said, a catastrophe so huge that in cyber terms it would be the equivalent of a national state of emergency that might continue for weeks or months.

What is that? How can you insure against it? Insurance might be good to, say, I have a breach issue and I am insured against the risk associated with that. But how do you insure against the loss of a whole infrastructure for the whole economy?

So I would say an approach is let each of the measures that are best suited for this tier of protection be given a chance to operate and be given a chance to demonstrate effectiveness.

Mr. CLAY. Thank you so much for that response. Let me thank the panel for their responses and their expertise in this area. I am certain that this will not be the last hearing.

But as you have heard, the bells have rung, and without objection, this committee is adjourned.

Thank you.

[Whereupon, at 5:50 p.m., the subcommittee was adjourned.]