CYBERSECURITY: PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE, ECONOMY, AND CONSUMERS

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

SEPTEMBER 13, 2006

Serial No. 109-137

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

31-464PDF WASHINGTON : 2006

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

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
Vice Chairman
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *General Counsel*
REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

FRED UPTON, Michigan, *Chairman*

MICHAEL BILIRAKIS, Florida
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
JOHN SULLIVAN, Oklahoma
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas
(EX OFFICIO)

EDWARD J. MARKEY, Massachusetts
Ranking Member
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
MIKE DOYLE, Pennsylvania
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
JOHN D. DINGELL, Michigan
(EX OFFICIO)

CONTENTS

	Page
Testimony of:	
Powner, David A., Director, Information Technology Management Issues, U.S. Government Accountability Office	13
Foresman, Hon. George W., Undersecretary for Preparedness, U.S. Department of Homeland Security	39
Moran, Kenneth P., Director, Office of Homeland Security, Enforcement Bureau, Federal Communications Commission	51
Weafer, Vincent, Senior Director, Symantec Security Response, Symantec Corporation	61
Kurtz, Paul B., Executive Director, Cyber Security Industry Alliance	71
Clinton, Larry, Chief Operating Officer, Internet Security Alliance	79
Additional material submitted for the record:	
Kenney, Jeannine, Senior Policy Analyst, Consumers Union, submission for the record	111
Powner, David A., Director, Information Technology Management Issues, U.S. Government Accountability Office, response for the record	119
Weafer, Vincent, Senior Director, Symantec Security Response, Symantec Corporation, response for the record	122
Kurtz, Paul B., Executive Director, Cyber Security Industry Alliance, response for the record	128
Clinton, Larry, Chief Operating Officer, Internet Security Alliance, response for the record	135
Foresman, Hon. George W., Undersecretary for Preparedness, U.S. Department of Homeland Security, response for the record	138

CYBERSECURITY: PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE, ECONOMY, AND CONSUMERS

WEDNESDAY, SEPTEMBER 13, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in Room 2123 of the Rayburn House Office Building, Hon. Fred Upton (Chairman) presiding.

Members present: Representatives Upton, Stearns, Shimkus, Bass, Walden, Terry, Blackburn, Barton (ex officio), Markey, Gonzalez, Inslee, Eshoo, and Dingell (ex officio).

Staff present: Kelly Cole, Counsel; Howard Waltzman, Chief Counsel for Telecommunications and the Internet; Jaylen Jensen, Senior Legislative Analyst; Anh Nguyen, Legislative Clerk; and Johanna Shelton, Minority Counsel.

MR. UPTON. Good morning. I would like to welcome our witnesses today, as well as welcome back our subcommittee members. Today's hearing is about cybersecurity and what our Government and the private sector are doing to prevent and mitigate attacks on our Internet infrastructure.

I liken cybersecurity and the threat to our Internet infrastructure to what we've seen occur on the Gulf Coast. For years we were worried that the levees in New Orleans were not strong enough to withstand a Category 5 hurricane. When Hurricane Katrina blew through the Gulf Coast, and the eventuality that we all knew was a possibility became a reality: We saw the levees break; we saw the devastation that such a storm could wrought.

Similarly, we know that our Internet infrastructure is subject to attack every day. The unfortunate reality is that there will come a day when this country experiences a debilitating Internet disruption.

The question we face now is: will we be ready? The lesson that we have learned from Hurricane Katrina is that we must be ready. That is why we are here today.

Normally, these types of hearings are held after a major incident, after it, but thankfully, we are in a position to improve our current system, to examine what steps are being taken, and what steps are needed to further fortify the Information Superhighway.

Today's hearing will examine the steps being taken in the public and private sectors to make us ready. We will hear the disappointing report from the GAO that we are not quite prepared for such an attack. I hope that today's hearing will help to improve our readiness and to increase the coordination among government agencies, as well as among government and private sector entities to protect our Internet infrastructure from a major disruption.

I thank the witnesses for appearing today. I look forward to their testimony. I particularly appreciate their ability to send up the testimony last night so that I could see it before I went home.

[The prepared statement of Hon. Fred Upton follows:]

PREPARED STATEMENT OF THE HON. FRED UPTON, CHAIRMAN, SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

Good Morning. I would like to welcome our witnesses today as well as welcome back our subcommittee Members.

Today's hearing is about cybersecurity, and what our government and the private sector are doing to prevent and mitigate attacks on our Internet infrastructure.

I liken cybersecurity and the threat to our Internet infrastructure to what we've seen occur on the Gulf Coast. For years we worried that the levies in New Orleans were not strong enough to withstand a Category 5 hurricane. Then Hurricane Katrina blew through the Gulf Coast, and the eventuality that we all knew was a possibility became a reality: we saw the levies break, and we saw the devastation that such a storm could wrought.

Similarly, we know that our Internet infrastructure is subject to attack every day. The unfortunate reality is that there will come a day when this country experiences a debilitating Internet disruption.

The question we face now is: will we be ready? The lesson we've learned from Hurricane Katrina is that we must be ready.

That is why we are here today. Normally, these types of hearings are held after a major incident. But thankfully, we are in a position to improve our current system, to examine what steps are being taken and what steps are needed to further fortify the information superhighway.

Today's hearing will examine the steps being taken in the public and private sectors to make us ready. We will hear the disappointing report from the GAO that we are not quite prepared for such an attack. I hope that today's hearing will help to improve our readiness and to increase the coordination among government agencies as well as among government and private sector entities to protect our Internet infrastructure from a major disruption.

I thank the witnesses for appearing today and I look forward to their testimony.

MR. UPTON. With that, I will yield to the Ranking Member of the subcommittee, gentleman from Massachusetts, Mr. Markey.

MR. MARKEY. Thank you, Mr. Chairman, very much. I want to commend you for calling this hearing this morning on cybersecurity.

This subcommittee has a long history on cybersecurity. We held a hearing, in this subcommittee, for instance, in 1993 where we demonstrated in this room cyber attacks on the United States Navy Pacific fleet command, on NASA's mission control, and on the Kremlin. We knew in 1993, well before we enacted the Telecommunications Act, that individuals would use the Internet for nefarious purposes. Today, we revisit the issue, knowing that the Internet is even more prevalent than ever, and that more individuals, businesses, and critical infrastructure, public safety, hospitals, and government agencies rely upon it.

Unquestionably, a major disruption of the Internet can invoke dire consequences in an emergency. In addition, successful cyber attacks can cause harm to individuals when security is compromised in a way that leads to identify theft, fraud, or extortion. American consumers pay dearly for such compromises to their privacy and security each year. So-called bot networks where computers are essentially hijacked by Internet-based software implanted in your computer without your consent are used as vehicles for spam and fraud and denial of service attacks. These acts, along with computer virus attacks, have negative financial impacts across the country that are estimated in the billions of dollars.

The Federal Communications Commission plays a vital role in preparing and responding to cyber attacks because of its responsibility over our Nation's telecommunications infrastructure. The Network Reliability and Interoperability Council, for example, was convened by the FCC in response to this subcommittee's inquiry into the massive Bell Atlantic telephone outage in 1991, which was caused by software glitches in digital switching systems. That council is tasked with helping to prevent Internet disruptions from occurring, and has developed a list of best practices for Internet disaster recovery in emergency situations.

The Department of Homeland Security is tasked with the lead responsibility for facilitating response and recovery efforts surrounding major Internet disruptions. The Government Accountability Office report from June of this year concluded that although the Department of Homeland Security has begun several initiatives addressing cybersecurity and Internet security, these efforts are neither complete nor are they comprehensive. As a member of the Homeland Security Committee since its establishment 3 years ago, I remain concerned about the Department's lack of significant progress in the area of cybersecurity.

Obviously, many are concerned about cyber threats from al Qeada. Certainly, cyber terrorism is something that is likely to be in al Qeada's

playbook, and we should be vigilant against such threats. Yet, beyond the daily threats to cybersecurity from hackers and spammers attempting to profit from fraud, the present threat appears to be from China. Numerous published reports highlight how China is actively probing our Internet-based infrastructure. Last year, the *Washington Post*, for example, highlighted how websites in China are being used heavily to target computer networks in the Defense Department and other U.S. agencies.

So based on the GAO's report, we clearly are still without an adequate plan for cybersecurity, and we need to do a better job preparing ourselves, not just for future threats, but for present practices from those who may target Americans for fraud or terrorism.

This is a timely hearing, and again, I want to commend Chairman Upton for holding this hearing, and thank our witnesses for their time and efforts.

MR. UPTON. I now recognize for an opening statement the Chairman of the full committee, Mr. Barton from Texas.

CHAIRMAN BARTON. Thank you, Chairman Upton, for holding this hearing.

Following the anniversary of September 11, 2001, today's hearing takes on added importance. Cybersecurity is both a timely issue to consider, and important issue to consider. Following the events of 9/11, we learned a great deal about our country's vulnerabilities. As a result, there have been ongoing, systemic reviews surrounding our Nation's critical infrastructure, most of which fall within the jurisdiction of this committee. Just as we have taken steps to protect our electricity and drinking water, it is also important to ensure that our information systems, telecommunications networks, and Internet infrastructure are protected from those that wish to do us harm.

In light of the public and private reliance on the Internet for commerce, communications, and education, I have requested the Government Accountability Office to complete a report on our preparedness for a major Internet disruption. Although, thankfully, we have never seen catastrophic Internet disruption, such an event is not out of the realm of possibility. The conclusion of the GAO is that recovering from a major Internet disruption would be very difficult. Roles of responsibility among government agencies are not fully defined, and coordination among the vast numbers of affected entities, both public and private, is not occurring on a satisfactory scale, according to the GAO.

Imagine our country without a functioning Internet, even for a little bit. Most of us have lived to adulthood without the Internet, but it is now a big part of our daily lives. Some people probably think they are

exempt from the impact of the Internet, but you would almost have to live in a cave to be truly unaffected. You benefit if you have a job, see a doctor, drive a car, or eat a meal, and the list goes on and on. Jobs, growth, and opportunity in America without an Internet would not disappear, but they would be dramatically tougher to achieve. Life, business, and the economy would not tumble into a new Dark Age, but it would be a dimmer and poorer life for all of us. That is exactly the outcome envisioned by a man who does live in a cave, Osama bin Laden.

Protecting our Internet is not simply a goal this country should aim to meet. This is an imperative that the United States must achieve. I am anxious to hear from the Department of Homeland Security what steps are being pursued to remedy the problems described by the GAO report. Also, I am interested in hearing from the private industry witnesses about what they see as the most critical issues and how they believe that we can best resolve them.

I want to thank you, Chairman Upton. I would like to point out that Chairman Stearns's subcommittee also has some jurisdiction in this area, but I thank both of you for addressing this very important issue.

With that, I yield back.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you, Chairman Upton, for holding this hearing. Just following the five-year anniversary of September 11th, today's hearing on cybersecurity is both timely and important.

Following the events of September 11th, we learned a great deal about our country's vulnerabilities. As a result, there have been ongoing, systematic reviews surrounding our nation's critical infrastructure, most of which fall within the jurisdiction of this Committee. Just as we have to take steps to protect our electricity and drinking water, it is also vitally important to ensure that our information systems, telecommunications networks, and Internet infrastructure are protected from those who wish to do us harm.

In light of the public and private reliance on the Internet for commerce, communications, and education, I requested the Government Accountability Office to complete a report on our preparedness for a major Internet disruption. Although this country has, thankfully, never seen a catastrophic Internet disruption, such an event is not out of the realm of possibility. The conclusion of the GAO is that recovering from a major Internet disruption would be difficult. Roles of responsibility among government agencies are not fully defined, and coordination among the vast number of affected entities, both public and private, is not occurring on a satisfactory scale.

Imagine America without a functioning Internet, even for a little while. Most of us lived to adulthood without the Internet, but it is now an unnoticed part of our lives. Some people probably think they're exempt from the impact of the Internet, but you'd have to live in a cave to be truly unaffected. You benefit if you have a job, see a doctor, drive a car or eat a meal, and the list goes on and on. Jobs, growth and opportunity in America without an Internet would not disappear, but they'd be dramatically tougher to achieve. Life, business and the economy would not tumble into a new Dark Age, but it would be a

dimmer and poorer one for all of us. That is exactly the outcome envisioned for us by a man who does live in a cave.

Protecting our Internet infrastructure is not simply a goal this country should aim to meet. This is an imperative that the United States must achieve. I am anxious to hear from the Department of Homeland Security what steps are being pursued to remedy the problems described by GAO. Also, I am interested in hearing from our private industry witnesses about what they see as the most critical issues and how they believe we can best resolve them.

Thank you again, Chairman Upton. I look forward to hearing from our witnesses.

MR. UPTON. I recognize the Ranking Member of the full committee, Mr. Dingell from the great State of Michigan.

MR. DINGELL. Mr. Chairman, we are from a great State. Thank you for those kind words.

First of all, Mr. Chairman, thank you for holding this hearing, and I commend you for making cybersecurity a priority for this subcommittee.

Cyber attacks against our Nation's information infrastructure grow in sophistication and in number every day. A failure by the Government to plan for physical and cyber damage to the Internet could be devastating to both our national security and our economic stability.

Cyber criminals are attacking online operations and infrastructure thousands of times a day, with increasingly targeted and malicious attacks. Moving beyond these notorious wide scale attacks of the past, these perpetrators seem bent on more calculated invasions designed to access and misuse corporate, personal, or government information. With a significant and growing level of our Nation's economic activity occurring over networked connections, a major physical or cyber breakdown of the Internet could wreak havoc on our economy. But a loss of the public's trust in the digital economy would likewise ripple across every industry and severely damage the Nation's overall economic health.

Given the range of threats and vulnerabilities, this hearing provides an excellent opportunity to understand on a broad level what is being done to secure cyberspace. How well prepared are the Government and the private sector to respond to and to recover from a major Internet disruption and from other cyber threats, and what is it that we should do about these problems?

The public sector is a holder of great responsibilities, but the private sector is at the forefront in the defense against cyber attacks, and it is vital that corporate management appropriately invests in cybersecurity. Do corporations, large and small, have the necessary commitment, information, and tools to protect against cyber intrusions and restore systems that have been compromised? The information technology sector is deploying tools to help businesses and consumers manage cyber risks, but they need a lot of help, and this is one of the places the

Government comes in. The Federal government must take a leading role in working with the private sector to secure cyberspace.

What steps has the Government, particularly the Department of Homeland Security, DHS, taken in regard to protecting against and recovering from a major cyber incident, whether from cyber warfare or from a natural disaster? Is cybersecurity receiving the proper level of attention within the Department, or is there more that can and should be done?

The Government Accountability Office reports that the role of the Government in planning for Internet recovery remains unclear. According to GAO, years after its formation, DHS is falling short on its efforts to secure cyberspace. GAO's recent report on Internet recovery provides a list of items upon which the Department must focus its attention. Curiously, more than a year after announcing, with more than a little fanfare, the creation of an Assistant Secretary for Cybersecurity and Telecommunications, that DHS position, along with others, remains vacant. This is a noticeable and a lengthy absence of cybersecurity leadership, and it conveys a clear lack of appreciation for our Nation's real and mounting cyber threats.

The American people should not have to wait for a massive cyber disaster to bring the necessary level of government attention to cyber risks. Companies on the front lines are clamoring for more leadership from the Government in securing cyberspace. Perhaps this is because the private sector knows full well that the costs of inaction in preparing for and recovering from a cyber disaster could be catastrophic to our national and economic security.

Mr. Chairman, this hearing is a very important one. Let us hope that it helps us get some answers, but let us also hope that it enables us to jog the Government into a more vigorous effort at addressing these problems, and perhaps filling an empty appointment or two at DHS.

Thank you.

MR. UPTON. Mr. Terry.

MR. TERRY. Thank you, Mr. Chairman, for holding this hearing. I would just like to associate myself to all of the remarks that have been made from this kiosk, and I yield back.

MR. UPTON. Especially the remarks about the great State of Michigan, we are glad to have--

MR. TERRY. With that exception.

MR. UPTON. Mr. Stearns.

MR. STEARNS. Thank you, Mr. Chairman. Obviously, all of us are glad that you are holding this hearing. As Mr. Barton pointed out, my Subcommittee on Commerce, Consumer Protection, and Trade, we have

had seven hearings on privacy and we have dealt a lot with data security, and we are also concerned with cybersecurity.

As the Government and private sector become more reliant on widespread interconnectivity, protecting both the public and private computer systems and the critical operations and infrastructure they support is more critical than ever before.

Although the Bush Administration, the Department of Homeland Security, DHS, have begun a variety of initiatives to protect the Internet infrastructure, obviously, much work needs to be done. According to a recently released GAO report, the efforts by DHS to fulfill its responsibilities for developing an integrated public, private plan for Internet recovery are neither complete nor comprehensive. DHS has developed a high level plan for infrastructure protection and incident response, but the components of these plans addressing Internet infrastructure are not yet complete.

DHS has started initiatives to improve response, such as working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events, but GAO notes progress on these initiatives have been limited and they often lack timeframe for completion.

My colleagues, much of the United States' critical infrastructure is potentially vulnerable to cyber attacks. Industrial control computer systems involved in this infrastructure are specific points of vulnerability, as cybersecurity for these systems has not been previously perceived as a very high priority. Many international terrorist groups now actively use computers and the Internet to communicate, and several may develop or acquire the necessary technical skills to eventually direct a coordinated attack against computers in the United States. A cyber attack intended to harm the U.S. economy would likely target computers that operate the civilian critical infrastructure and our government agency.

While there is no published evidence that terrorist organizations are currently planning a coordinated attack against computers, computer system vulnerabilities persist worldwide and initiators of the random cyber attacks that plague computers on the Internet remain largely unknown today. Reports from security organizations show that random attacks are now increasingly implemented through the use of automated tools called bots that direct large numbers of these compromised computers to launch attacks through the Internet as swarms. The growing trend towards the use of more automated attack tools has also overwhelmed some of the current methodologies used for tracking Internet cyber attacks.

The potential consequences of this are critical, and range from temporary loss of service to catastrophic infrastructure failure affecting multiple States for an extended duration. The consequences of attack could vary widely. In addition, DOD has also observed that the number of attempted intrusions into military networks has gradually increased.

Mr. Chairman, this uncertainty highlights the necessity of this hearing and I thank you for holding it. I look forward to hearing from our witnesses.

MR. UPTON. Mr. Shimkus.

MR. SHIMKUS. Thank you, Mr. Chairman.

I will just brief and say thank you for coming to the panelists. I thank the Chairman for asking for the report in 2005.

In July, we suffered some pretty horrific storms in the St. Louis metropolitan area. Over three-quarters of a million people were without power for many days. My home was without power for 5 days. I think that allowed the public to understand how connected we are through the computer, through Internet, through electricity, and the like. The public really needs to think what we can do collectively. And I think what these storms showed the public in the St. Louis metropolitan area is what they had to do themselves to prepare. That is really the same message that we talked about in Katrina and other major disasters. What are the individual citizens doing to help protect themselves in the case of attacks? This is cybersecurity, but we do rely more and more on technology, and the public needs to be prepared to--how to do their own work, and that is what I will be asking about later on.

Thank you, Mr. Chairman. I yield back.

MR. UPTON. Thank you. That concludes the opening statements by the members of the subcommittee.

[Additional statement submitted for the record follows:]

PREPARED STATEMENT OF THE HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you Mr. Chairman, and thanks to the witnesses for joining us today.

As a member of the House Intelligence Committee, I take very seriously the range of threats to our country from terrorists and other enemies, including threats to our basic infrastructure including our telecommunications networks and the Internet.

In the 21st Century, no part of our national infrastructure is more important than our technological infrastructure and communications networks.

Former Cybersecurity Czar Richard Clarke once described the potential for a telecom disaster as an "electronic Pearl Harbor." CRS has estimated a cyber attack could produce an economic blow exceeding $200 billion.

This is undoubtedly a shared responsibility of government, the telecommunications industry, businesses, and consumers, and critical gaps in security remain unaddressed at every level.

I'm increasingly concerned that cybersecurity is not receiving the attention it requires from the federal government.

In the wake of 9/11 the Administration has slowly diminished responsibility for and visibility of cybersecurity matters at the federal level. Instead, they have focused almost exclusively on threats to air safety and border security. These are critical threats to our national security but they are not the only ones. We must attend to all critical sectors, including cybersecurity.

The position of cyber security czar once resided at the White House and reported directly to the President, but after Richard Clarke's resignation in 2003, the position was relegated to a mid-level position in the Department of Homeland Security.

In July 2005, after significant pressure from Congress and the private sector, DHS Secretary Chertoff announced the creation of an Assistant Secretary for Cyber Security and Telecommunications. The Assistant Secretary would have the authority to set policy and develop public-private partnerships with industry to improve national cybersecurity.

But in the year since the position was announced, the Administration has yet to even nominate someone to fill it.

Clearly, we cannot expect national leadership in cybersecurity without an individual to lead the effort. I hope the President will act soon to appoint someone to assume this vital function.

I also believe much of the responsibility for America's cybersecurity lies with the private sector and individual citizens.

Many of the most potent viruses and worms that afflict our computer networks are able to do so only because the vast majority of personal computers are not secure, thus becoming the unwitting distribution network for destructive programs.

Businesses and individuals must be vigilant in maintaining appropriate security on their networks and personal computers, and utilize sound security practices.

The federal government should play a leadership role in promoting effective security standards and practices and assisting private and public institutions in reaching out to individual users to protect themselves from cyber attacks.

Data security legislation unanimously endorsed by this Committee would provide significant government leadership in endorsing and promoting robust security systems and standards, and I hope the House will consider our bill before Congress adjourns.

We have to do better than react to an "electronic Pearl Harbor." I look forward to working with my colleagues to make sure that we do everything we can to protect our nation's vital computer and communications networks.

MR. UPTON. At this point, we will hear the testimony by our distinguished panel. We are joined by Mr. David Powner, the Director of Information Technology Management Issues from the United States Government Accountability Office; Mr. George Foresman, Under Secretary for Preparedness of the United States Department of Homeland Security; Mr. Ken Moran, Director of the Office of Homeland Security of the Enforcement Bureau of the FCC; Mr. Vincent Weafer, Senior Director of Symantec Corporation from California; Mr. Paul Kurtz, Executive Director of Cybersecurity Industry Alliance; and Mr. Larry Clinton, CEO of Internet Security Alliance.

Gentlemen, your testimony is made part of the record in its entirety. We would like you to take not more than 5 minutes to summarize it, at which point we will have questions from members of panel.

Mr. Powner, we will start with you. Welcome.

STATEMENTS OF DAVID A. POWNER, DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, U. S. GOVERNMENT ACCOUNTABILITY OFFICE; HON. GEORGE W. FORESMAN, UNDER SECRETARY FOR PREPAREDNESS, U. S. DEPARTMENT OF HOMELAND SECURITY; KENNETH P. MORAN, DIRECTOR, OFFICE OF HOMELAND SECURITY, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION; VINCENT WEAFER, SENIOR DIRECTOR, SYMANTEC SECURITY RESPONSE, SYMANTEC CORPORATION; PAUL B. KURTZ, EXECUTIVE DIRECTOR, CYBERSECURITY INDUSTRY ALLIANCE; AND LARRY CLINTON, CHIEF OPERATING OFFICER, INTERNET SECURITY ALLIANCE

MR. POWNER. Chairman Upton, Ranking Member Markey, Chairman Barton, and members of the subcommittee, we appreciate the opportunity to testify on our Internet Reconstitution Report that we recently completed at your request.

Federal law and policy calls for critical infrastructure protection activities and establishes DHS as our Nation's focal point. Among its many responsibilities is to work with the private sector to develop an integrated public private Internet recovery plan. To date, no such plan exists. Today, at your request, I will briefly discuss the growing threats to the Internet, where our Nation is in its efforts to develop this plan, and recommendations to both DHS and the Congress to facilitate public and private efforts to recover the Internet when major disruptions occur.

First, threats. Criminal groups, foreign intelligence services, hackers, and terrorists are threats to our Nation's computers and networks. A recent intelligence report on global trends forecasts that terrorists may develop capabilities to conduct both cyber and physical attacks against infrastructure modes, including the Internet. In fact, the Internet has been targeted and attacked, and private sector companies who own the majority of the Internet infrastructure deal with cyber and physical disruptions on a regular basis. For example, viruses and worms are often used to launch denial of service attacks that result in traffic being slowed or stopped. Several recent cyber attacks highlight the importance of having robust Internet recovery plans, including a 2002 coordinated denial of service attack that targeted all 13 Internet route servers.

For most of these attacks, the Government did not have a role in recovering the Internet; however, recent physical attacks like 9/11 and Katrina highlight the need for public/private coordination associated with Internet recovery.

DHS has begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan, but these efforts are not yet complete or comprehensive. Specifically, DHS has developed high level plans for infrastructure protection and national disaster response, but components of these plans that are to address Internet recovery are incomplete and inadequate. In addition, the National Response Plan cyber annex does not reflect the National Cyber Response coordination group's current operating procedures. DHS has started a variety of initiatives to tackle this problem, including working groups to facilitate response, and exercises to practice recovery efforts; however, these efforts are immature and the relationships among groups like the Internet disruption working group and others are not evident.

Regarding the challenges that have impeded progress, first, it is unclear what government entity is in charge, what the Government's role should be, and when it should get involved. Expanding on each of these: DHS's National Cybersecurity Division and the National Communications System have overlapping responsibilities. In addition, there is lack of consensus about the role that DHS should play. The Government is pursuing large scale plans with the NIPP and the National Response Plan, while the private sector wants more of an assist or tactical role from the Government that our report lays out in detail. Finally, triggers that clarify when the Federal government should get involved are unclear.

Second, our Nation is working in a legal framework that doesn't specifically address the Government's role and responsibilities in the event of an Internet disruption. In addition, the Katrina recovery efforts showed that the Stafford Act can create a roadblock when for-profit companies that own and operate critical infrastructure need Federal assistance during national emergencies.

Third, the private sector is reluctant to share information with DHS because it does not see value in sharing, does not necessarily trust the Government, and views DHS as an organization lacking effective leadership.

To address these inadequacies, my statement includes nine specific recommendations to DHS, including determining who should be in charge, given the convergence of voice and data communications, developing a plan that is consistent with what the private sector infrastructure owners need during a time of crisis, and incorporating lessons learned from incidents and exercises.

In summary, Chairman Upton, exercises to date in a recently issued report by the Business Roundtable found that both the Government and the private sector are poorly prepared to effectively respond to cyber events. Although DHS has various initiatives underway, these need to be

better coordinated and driven to closure. Until this happens, the credibility of the Department will not be where it needs to be to build effective public/private relationships needed to effectively respond to major Internet disruptions.

This concludes my statement. I would be pleased to respond to any questions.

[The prepared statement of David A. Powner follows:]

PREPARED STATEMENT OF DAVID A. POWNER, DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

United States Government Accountability Office

GAO

Testimony before the Subcommittee on Telecommunications and the Internet, House Committee on Energy and Commerce

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, September 13, 2006

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan

Statement of David A. Powner
Director, Information Technology Management Issues

Keith A. Rhodes
Chief Technologist
Director, Center for Technology and Engineering

GAO
Accountability * Integrity * Reliability

GAO-06-1100T

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

September 2006

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-1100T, a testimony before the Subcommittee on Telecommunications and the Internet, Committee on Energy and Commerce, U.S. House of Representatives

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—*Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006). This 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 suggests that Congress consider clarifying the legal framework guiding Internet recovery and makes recommendations to DHS to strengthen its ability to help recover from Internet disruptions. In written comments, DHS agreed with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-1100T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner at (202) 512-9286 or pownerd@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.

DHS has begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery, but these efforts are not complete or comprehensive. Specifically, DHS has developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure are not complete. In addition, the department has 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 to date on these initiatives has been limited, and other initiatives lack time frames for completion. Also, the relationships among these initiatives are not evident. As a result, the government is not yet 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 summarize our previously issued report on public/private recovery plans for Internet infrastructure. Since the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. Our country 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 government's and our nation's computer systems 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 cyberspace—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] Last year, we testified before the Senate on DHS's responsibilities for cybersecurity-related critical infrastructure protection.[3] In that testimony, we discussed the status of DHS's efforts and challenges faced by DHS in fulfilling its responsibilities. We reported that DHS had much work ahead of it. In a related report, we recommended that DHS prioritize cybersecurity-related responsibilities—including establishing recovery plans for key Internet functions.[4]

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

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

[3]GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, D.C.: July 19, 2005).

[4]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

In June 2006, we issued a report 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.[5] 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. That report contains a detailed overview of our scope and methodology. As we stated in our report, all supporting work was 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 both 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 as a whole 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

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

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.

DHS has begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts are not yet comprehensive or complete. Specifically, DHS has developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure are not complete. In addition, DHS has 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 to date on these initiatives has been limited, and other initiatives lack timeframes for completion. Also, the relationships among these initiatives are not evident. As a result, the risk remains that the government is not yet 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.[6] 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. In written comments, DHS agreed with our recommendations and provided information on initial activities it was taking to implement them.

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, do 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

[6]GAO-06-672.

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 increasing in frequency and complexity. These attacks can come from a variety of actors, 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.[7] 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 the vast majority 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

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

restore services. In addition, government initiatives could facilitate response to major Internet disruptions.

Federal policies and plans[8] assign DHS lead responsibility for facilitating a public/private response to and recovery from major Internet disruptions. Within DHS, responsibilities reside in two divisions within the Preparedness Directorate: 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 cybersecurity responsibilities have highlighted issues and challenges facing the department. In May 2005, we issued a report on DHS's efforts to fulfill its cybersecurity responsibilities.[9] We noted that while DHS had initiated multiple efforts to fulfill its responsibilities, it had not fully addressed any of the 13 key cybersecurity 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 cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with stakeholders, and demonstrating the

[8]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.

[9]GAO-05-434.

value that DHS can provide. In this report, we also made recommendations to improve DHS's ability to fulfill its mission as an effective focal point for cybersecurity, including recovery plans for key Internet functions. DHS agreed that strengthening cybersecurity is central to protecting the nation's critical infrastructures and that much remained to be done, but it has not yet addressed our recommendations.

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 the above. Disruptions to Internet service can be caused by cyber and physical incidents—both intentional and unintentional. Recent 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, a coordinated denial-of-service attack was launched against all of the root servers in the Domain Name System. At least nine of

the thirteen root servers experienced degradation of service. However, average end users hardly noticed the attack. The attack became visible only as a result of various Internet health-monitoring projects. The response to the attacks was handled by the server operators and their service providers. The 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. If a massive disruptive attack on the domain name server system were successful, it could take several days to recover from. According to experts familiar with the attack, the government did not have a role in recovering from it.

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 addition, Hurricane Katrina caused substantial destruction of the communications infrastructure 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 over 3 million telephone customers, 38 emergency 9-1-1 call centers, hundreds of thousands of cable customers, and over 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[10] and Homeland Security Presidential Directive 7[11] establish critical infrastructure

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

protection as a national goal and describe a strategy for cooperative 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, this law and regulation do not specifically address roles and responsibilities in the event of an Internet disruption.

Regarding federal disaster response, the Defense Production Act[12] and the Stafford Act[13] 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[14] and the NCS authorities,[15] 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

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

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

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

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

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

powers regarding telecommunications, including the authority to require any carrier subject to the Communications Act of 1934 to grant preference or priority to essential communications.[16] 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 been seldom 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 Relationship Between Initiatives Is Not Evident

DHS has begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts are not complete or comprehensive. Specifically, DHS has developed high-level plans for infrastructure protection and national disaster response, but the components of these plans that address the Internet infrastructure are not complete. In addition, DHS has 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. While these activities are promising, some initiatives are not complete, others lack time lines and priorities, and still others lack effective mechanisms for incorporating lessons learned. In addition, the

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

relationship between these initiatives is not evident. As a result, the nation is not prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

High-Level Response and Protection Plans

DHS has two key documents that guide its infrastructure protection and recovery efforts, but components of these plans dealing with Internet recovery are not complete. The *National Response Plan* is DHS's overarching framework for responding to domestic incidents. It contains two components that address issues related to telecommunications and the Internet, Emergency Support Function 2 and the Cyber Incident Annex. These components, however, are not complete; Emergency Support Function 2 does not directly address Internet recovery, and the annex does not reflect the National Cyber Response Coordination Group's current operating procedures. The other key document, the *National Infrastructure Protection Plan*, consists of both a base plan and sector-specific plans. The base plan, which was recently released, describes the importance of cybersecurity and networks such as the Internet to critical infrastructure protection and includes an appendix that provides information on cybersecurity responsibilities. The appendix restates DHS's responsibility to develop plans to recover Internet functions. However, the base plan is at a high level and the sector-specific plans that would address the Internet in more detail are not scheduled for release until December 2006.

Several representatives of private-sector firms supporting the Internet infrastructure expressed concerns about both plans, noting that they would be difficult to execute in times of crisis. Other representatives were uneasy about the government developing recovery plans, because they were not confident of the government's ability to successfully execute the plans. DHS officials acknowledged that it will be important to obtain input from private-sector organizations as they refine these plans and initiate more detailed public/private planning.

Both the *National Response Plan* and *National Infrastructure Protection Plan* are designed to be supplemented by more specific plans and activities. DHS has numerous initiatives under way to

better define its ability to assist in responding to major Internet disruptions. While these activities are promising, some initiatives are incomplete, others lack time lines and priorities, and still others lack an effective mechanism for incorporating lessons learned.

National Communications System Reorganization

DHS plans to revise the role and mission of the National Communications System (NCS) to reflect the convergence of voice and data communications, but this effort is not yet complete. A presidential advisory committee on telecommunications[17] established two task forces that recommended changes to NCS's role, mission, and functions to reflect this convergence, but DHS has not yet developed plans to address these recommendations.

National Cyber Response Coordination Group

As a primary entity responsible for coordinating governmentwide responses to cyber incidents—such as major Internet disruptions—DHS's National Cyber Response Coordination Group is working to define its roles and responsibilities, but much remains to be done. DHS officials acknowledge that the trigger to activate this group is imprecise and will need to be clarified. Because key activities to define roles, responsibilities, capabilities, and the appropriate triggers for government involvement are still under way, the group is at risk of not being able to act quickly and definitively during a major Internet disruption.

Internet Disruption Working Group

Since most of the Internet is owned and operated by the private sector, NCSD and NCS established the Internet Disruption Working Group to work with the private sector to establish priorities and develop action plans to prevent major disruptions of the Internet and to identify recovery measures in the event of a major disruption. According to DHS officials who organized the group, it held its first forum, in November 2005, to begin to identify real versus perceived threats to the Internet, refine the definition of an Internet disruption,

[17]The National Security Telecommunications Advisory Committee advises the President on issues and problems related to implementing national security and emergency preparedness telecommunications policy.

determine the scope of a planned analysis of disruptions, and identify near-term protective measures. DHS officials stated that they had identified a number of potential future plans; however, agency officials have not yet finalized plans, resources, or milestones for these efforts.

North American Incident Response Group

US-CERT officials formed the North American Incident Response Group, which includes both public and private-sector network operators that would be the first to recognize and respond to cyber disruptions. In September 2005, US-CERT officials conducted regional workshops with group members to share information on structure, programs, and incident response and to seek ways for the government and industry to work together operationally. While the outreach efforts of the North American Incident Response Group are promising, DHS has only just begun developing plans and activities to address the concerns of private-sector stakeholders.

Exercises

Over the last few years, DHS has conducted several broad inter-governmental exercises to test regional responses to significant incidents that could affect the critical infrastructure. More recently, in February 2006, DHS conducted an exercise called Cyber Storm, which was focused primarily on testing responses to a cyber-related incident of national significance. Exercises that include Internet disruptions can help to identify issues and interdependencies that need to be addressed. However, DHS has not yet identified planned activities, milestones, or which group should be responsible for incorporating lessons learned from the regional and Cyber Storm exercises into its plans and initiatives.

While DHS has various initiatives under way, the relationships and interdependencies between these various efforts are not evident. For example, the National Cyber Response Coordination Group, the Internet Disruption Working Group, and the North American Incident Response Group are all meeting to discuss ways to address Internet recovery, but the interdependencies between the groups have not been clearly established. Without a thorough

understanding of the interrelationships between its various initiatives, DHS risks pursuing redundant efforts and missing opportunities to build on related efforts.

After our report was issued, a private-sector organization released a report that examined the nation's preparedness for a major Internet disruption.[18] The report stated that our nation is unprepared to reconstitute the Internet after a massive disruption. The report supported our findings that significant gaps exist in government response plans and that the responsibilities of the multiple organizations that would play a role in recovery are unclear. The report also made recommendations to complete and revise response plans such as the Cyber Incident Annex of the *National Response Plan*; better define recovery roles and responsibilities; and establish more effective oversight and strategic direction for Internet reconstitution.

Multiple Challenges Exist to Planning for Recovery from Internet Disruptions

Although DHS has various initiatives under way to improve Internet recovery planning, it faces 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 it addresses these challenges, DHS will have difficulty achieving results in its role as focal point for recovering the Internet from a major disruption.

[18]Business Roundtable, *Essential Steps to Strengthen America's Cyber Terrorism Preparedness* (Washington D.C.: June 2006).

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.

The trigger for the *National Response Plan*, which is DHS's overall framework for incident response, is poorly defined and has been found by both us and the White House to need revision.[19] Since private-sector participation in DHS planning activities for Internet disruption is voluntary, agreement on the appropriate trigger for government involvement and the role of government in resolving an Internet disruption is essential to any plan's success.

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 did not have a direct recovery role, while others identified a variety of potential roles, including

[19]See GAO, *Hurricane Katrina: GAO's Preliminary Observations Regarding Preparedness, Response, and Recovery*, GAO-06-442T (Washington, D.C.: Mar. 8, 2006), and the White House, *The Federal Response to Hurricane Katrina: Lessons Learned* (Washington, D.C., February 2006).

- 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[20] 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 addition, the organizations with roles in Internet recovery (NCS and NCSD) have overlapping responsibilities and may be reorganized once DHS selects permanent leadership. As a result, it is difficult for DHS to develop a clear set of organizational priorities and to coordinate between the various activities necessary for Internet recovery planning. In May 2005, we reported that multiple senior DHS cybersecurity officials had recently left the department.[21] 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. Additionally, DHS officials acknowledge that the current

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

[21]GAO-05-434.

organizational structure has overlapping responsibilities for planning for and recovering from a major Internet disruption.

In a July 2005 departmental reorganization, NCS and NCSD were placed in the Preparedness Directorate. NCS's and NCSD's responsibilities were to be placed under a new Assistant Secretary of Cyber Security and Telecommunications—in part to raise the visibility of cybersecurity issues in the department. However, almost a year later, this position remains vacant. While DHS stated that the lack of a permanent assistant secretary has not hampered its efforts in protecting critical infrastructure, several private-sector representatives stated that DHS's lack of leadership in this area has limited progress. Specifically, these representatives stated that filling key leadership positions would enhance DHS's visibility to the Internet industry and potentially improve its reputation.

Implementation of GAO Recommendations Should Improve DHS Internet Recovery Planning Efforts

Given the importance of the Internet infrastructure to our nation's communication and commerce, in our accompanying report we suggested matters for congressional consideration and made recommendations to DHS regarding improving efforts in planning for Internet recovery.[22] 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 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

[22] GAO-06-672.

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 the following nine actions:

- Establish dates for revising the *National Response Plan*—including efforts to update key components that are relevant to the Internet.
- 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.
- Review the NCS and NCSD organizational structures and roles in light of the convergence of voice and data communications.
- 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.
- Establish time lines and priorities for key efforts identified by the Internet Disruption Working Group.
- Identify ways to incorporate lessons learned from actual incidents and during cyber exercises into recovery plans and procedures.
- 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 written comments, DHS agreed with our recommendations and stated that it recognizes the importance of the Internet for information infrastructures. DHS also provided information about initial actions it is taking to implement our recommendations.

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, pertinent Internet components of these plans are not complete. While DHS has also undertaken several initiatives to improve Internet recovery planning, much remains to be done. Specifically, some initiatives lack clear timelines, lessons learned are not consistently being incorporated in recovery plans, and the relationships between the various initiatives are not clear.

DHS faces numerous challenges in developing integrated public/private recovery plans—not the least of which is the fact 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, our report 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. Effectively implementing these recommendations 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 us at (202) 512-9286 and at (202) 512-6412 or by e-mail at pownerd@gao.gov and rhodesk@gao.gov. Other key contributors to this testimony include Don R. Adams, Naba Barkakati, Scott Borre, Neil Doherty, Vijay D'Souza, Joshua A. Hammerstein, Bert Japikse, Joanne Landesman, Frank Maguire, Teresa M. Neven, and Colleen M. Phillips.

(310829)

Page 22

MR. UPTON. Thank you.

Mr. Foresman.

MR. FORESMAN. Mr. Chairman, Ranking Member Markey, and members of the subcommittee, thank you for the opportunity to appear today to discuss cyber and telecommunication security. You have my written statement and I offer it for the record.

I would like to briefly highlight several points.

First, there has been much discussion about the Department's ability to find and hire a qualified individual to serve as the Assistant Secretary

for Cyber and Telecommunications Security. I want to be very clear. This has been and remains a top priority for the Department. We are in the final stages of a security process review for a candidate that we feel is very well qualified. We look forward to announcing the candidate with Congress very soon. I am confident this individual will continue to build on the progress that is being made every day in our cyber and telecommunications security efforts.

Second, today, the Department is releasing its After Action report from our recent government private sector national and international cybersecurity exercise, Cyber Storm. This report will measurably advance refinements to operational protocols. Its lessons will not simply be documented, they will be implemented.

Third, telecommunication networks and information technology activities are both mutually dependent and interdependent, and they have converged. By the end of this year, we will complete our efforts to collocate together the U.S. Computer Emergency Readiness Team and the National Coordination Center for Telecommunications to improve operational coordination. This means better coordination among all levels of government, better and stronger relationships between government, and the private sector during threats and actual events.

Secretary Chertoff said last week in his speech that reflected on five years since 9/11 the way to protect the critical infrastructure is "in partnership with Federal, State, and local officials, and with the private sector folks who actually own the things that we are trying to protect." This collaboration is key to our approach to protecting telecommunications and the Nation's cyber infrastructures.

Last month, our cybersecurity experts worked quietly with their counterparts at Microsoft to address a critical software vulnerability. Microsoft was competent in their partnership with DHS and quickly brought the vulnerability to our attention. While Microsoft worked over several weeks to develop a patch, our U.S. cert was quietly and effectively monitoring Internet activity to ensure the vulnerabilities were not being exploited. At the same time, the Department was working domestically and internationally and with our private sector partners to mitigate terrorist threats associated with the British airline plot. These concurrent actions are two of many examples of the day-to-day public/private sector activity taking place in the Department's preparedness efforts.

Maintaining these types of collaborations remains, as you know, a multi-dimensional challenge. From personal computers in homes, to vast networks, to control systems, to the Internet, cyber and telecommunications security presents enormous challenges. These challenges are obvious: prioritizing our work, partnering for effective

collaboration, balancing security and economic considerations, and most notably, increasing the understanding.

The other witnesses today will add clarity to these points from varying perspectives, but I think it is safe to say there is no one before you today that does not share the belief that protecting America's cyber and telecommunications systems is as critical to national security as it is to citizens' security. I want to be clear. Progress is being made every day, and there is more to be done. Mr. Chairman and members of the committee, as you well know, the security of America's cyber and telecommunications systems do not lend themselves to surrounding one building with heavily armed police officers or simply mandating an action and we will be safe. Simply put, there is no magic bullet.

The success of our national cyber and telecommunications security efforts depends on unity of purpose and continuing public/private sector collaboration. This is serious business and we at the Department are serious about the business. We look forward to continuing discussions with this committee, with the Congress on the wide range of policy issues that we must confront together if we are going to measurably advance our efforts to secure the Nation's cyber assets and its telecommunications assets.

Thank you, and I look forward to your questions.

[The prepared statement of Hon. George W. Foresman follows:]

PREPARED STATEMENT OF THE HON. GEORGE W. FORESMAN, UNDER SECRETARY OF PREPAREDNESS, U.S. DEPARTMENT OF HOMELAND SECURITY

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about cyber security and the recovery and reconstitution of critical networks.

Our Nation's communications and information infrastructure will support profound improvements in the security of our homeland in the next 20 years. States, communities, and our private sector partners are already finding innovative ways to prevent terrorism and protect critical infrastructure by leveraging information technology. As I outline further below, the Federal government is similarly deploying innovative programs that significantly raise the level of preparedness in this critical area.

Our vision and philosophy for the future build upon accomplishments of the past several years – critical infrastructure businesses, home users, and government at all levels have a greater understanding of the threat posed by malicious software. The communications and information technology sectors have deployed new tools to help these constituents manage cyber risks.

However, at the core of our vision and philosophy is a strong belief that the Department of Homeland Security (DHS) must increasingly guard against more virulent attacks and cyber disruptions – whether caused by a terrorist attack or natural disaster. We must prevent cyber incidents of national significance.

In this testimony, I will outline three strategic goals to execute this vision, and examples of current and future programs that will move us forward to these objectives.

Assistant Secretary for Cyber Security and Telecommunications

As a preliminary matter, allow me to outline the steps the Department is currently taking while working with the White House to actively pursue qualified candidates for the post of Assistant Secretary for Cyber Security and Telecommunications. I am personally engaged in the process of selecting the new Assistant Secretary and, in the interim, am providing program direction pending the post being filled permanently. Because of the importance of this mission, all parties want to ensure that the individual appointed to this position possesses the right combination of skills, experience, and leadership necessary to succeed.

To supplement my own personal involvement in strategy, the Assistant Secretary for Infrastructure Protection has been serving as the Acting Assistant Secretary for Cyber Security and Telecommunications. As such, he has been actively engaged in overseeing operational programs, program reviews, governance structure, and has participated in government/industry forums to further the advancement of this important new office as well as the strategic goals that I will outline shortly.

Regardless of when this position is filled, the mission of the Department of Homeland Security (DHS), the National Cyber Security Division (NCSD), and the National Communications System (NCS) remain clear. The absence of a permanent Assistant Secretary for Cyber Security and Telecommunication has not had an impact on NCSD's or NCS's critically important work.

Strategic Vision and Philosophy

Our vision and philosophy for cyber security and recovery reflects the expanding importance of our communications and information infrastructure in all walks of life. As you know, a failure to consider and deploy effective strategies could adversely affect homeland and national security, public health and welfare, and our economic security. Policies that advance a safe and secure communications infrastructure promote public trust and confidence, project stability to those who wish us harm, and foster valuable relationships between the public and private sectors.

We fully recognize the challenges inherent in our preparedness responsibilities. We are faced with difficult choices and options. We must think about risks to the communications and information infrastructure in new and creative ways. We must prioritize resources, and make hard decisions where resources are limited.

We must also continue to partner strategically with the communications and information technology sectors as well as other experts outside of the Federal government. As we focus on the potential for catastrophic cyber disasters, our partnerships are becoming more diverse and sophisticated, reflecting the different technology, business, and policy decisions that must be made. These partnerships also entail strengthening cooperation across the government and, at a minimum, finding ways to cultivate support outside of the Department where expertise clearly exists. Whether public or private, the partnerships must deliver real and measurable value in light of the catastrophic damages that can occur in the absence of smart collaboration.

Finally, we must reinforce a culture of preparedness and increasingly shift from a reactive to a proactive stance. In sum, we must prepare by promoting effective security strategies that evolve as the threat evolves.

Three Strategic Goals

In responding to these challenges, the Preparedness Directorate is executing three strategic priorities. (1) We are preparing for cyber incident of national significance; (2) we are working to forge more effective partnerships; and (3) we are working to foster a culture of preparedness to prevent cyber incidents and mitigate damage when disruptions occur.

- **First, we must prepare for a large scale cyber disaster.**

Our primary strategic goal is to prepare for high-consequence incidents. These would include, for example, a widespread disruption involving the Internet or critical communications infrastructure, whether from an attack or natural disaster.

Now, as the Department matures we are preparing for large scale cyber disasters. Our strategic intentions are ambitious and will require resolution of multiple impediments, such as:

- Identifying incidents and providing early warning;
- Deploying Federal assets and services more efficiently to mitigate damages where disruptions occur;
- Responding to the speed of attacks and disruptions, which will require new technologies and skill sets in our workforce; and
- Maximizing the use of tools that promote and integrate privacy protections as well as real-time security needs.

The Preparedness Directorate has several important programs already underway to prepare for a cyber incident of national significance. The Office of Cyber Security and Telecommunications has established an Internet Disruption Working Group (IDWG) to address the resiliency and recovery of Internet functions in the event of a major cyber incident. The IDWG is not examining all risks, but is focusing on and identifying measures that government and its stakeholders can take to protect against nationally significant Internet disruptions.

These proposed measures may yield heightened expectations, roles, and responsibilities for the United States Computer Emergency Readiness Team (US-CERT).

- **Second, we must continue to forge more effective partnership arrangements.**

Our second strategic goal is to improve the Department's partnership programs and practices. Homeland Security Presidential Directive 7, the Administration's policy on critical infrastructure protection, explicitly recognizes the importance of partnerships, which are essential for many sound reasons. In the cyber security arena, the Department is working to nurture existing partnerships and establish new relationships with three key stakeholder communities: (1) the private sector; (2) Federal departments and agencies and State, local, and tribal governments; and (3) academia.

Private Sector Partnerships. Industry owns, operates, and controls the bulk of the communications and information infrastructure, so collaborating with industry to prepare for and respond to catastrophic cyber disasters is a strategic priority.

In "The Federal Response to Hurricane Katrina: Lessons Learned," the White House pinpointed specific problems experienced by infrastructure owners in restoring communications services. The report additionally described interdependencies between the critical infrastructure sectors, such as energy and transportation, that impact restoration of communications services. Our vision for the future, and emphasis on close collaboration with the private sector, follows directly from these lessons learned.

In our partnerships, the government must deliver real value to our private sector partners, who are clearly committed to a collaborative approach. Smart, effective partnerships demand that we:

- Understand how the private sector will prepare for and respond to cyber disasters – and where the government can complement industry practices;
- Leverage state of the art technologies to improve preparedness and response and sustain privacy protections;
- Promote pools of knowledge and subject matter expertise for reconstituting communications and information infrastructure; and
- Ensure close coordination of Preparedness Directorate functions, such as those provided by NCSD and NCS,

Government Partnerships. The Department is similarly committed to enhancing partnership arrangements across the Federal government and with State, local, and tribal governments. We will continue to explore innovative ways to leverage skill sets outside of the Department as part of our strategy for cyber-preparedness and response. We currently partner with Multi-State Information Sharing and Analysis Center (MS-ISAC), as well a key operational information technology and communications officials in the states, and we are strengthening those partnerships for recovery and reconstitution efforts.

Partnerships with Academia. The Department is serious about partnering aggressively with experts in academia. To date, the Department has included academia in partnership discussions; however, in order to lay a foundation for more effective cyber response capability, we must seek guidance from academia on a range of more complex problems. As an example, we expect to learn more from academia on such matters as challenges with insurance and risk transfer for the critical infrastructure sectors as well as business case arguments for catastrophic preparedness. These areas promote public and private sector collaboration.

Third, we must create a culture of preparedness – both to prevent a cyber disaster and to mitigate damages if widespread disruptions occur.

Our third and final strategic goal seeks to influence how we prepare for security challenges in the coming decade. As with our other strategic priorities, this goal demands a focused and disciplined approach in several areas. At a minimum, we are structuring programs to:

- **Clearly outline preparedness organizations, relationships, and expectations:** One of the Preparedness Directorate's strategic priorities is to clearly set forth all aspects of "doctrine" in accordance with legislative and Presidential direction. To create a long-term culture of preparedness, we are developing clear organizational doctrine, which memorializes strategic policies, clarifies roles and responsibilities, and defines measures of accountability.
- **Promote a shared way of life that measurably improves preparedness for a catastrophic cyber disaster:** Finally, we are focusing our energies on cyber-preparedness. Our programs in the coming years will seek to inculcate to change behavior as we continue to leverage our government partners to help continue efforts in these other areas. Awareness and education in the past decade have focused on large segments of the population, including home users and students in K-12. We hope to develop additional awareness programs that look more carefully at catastrophic cyber risk and continue to leverage our government partners to help advance our efforts in these other areas.

Organizational Framework

The three strategic goals outlined above will require clear organizational directions and programs.

HSPD-7 directs the Department to establish an organization dedicated to cyber security. The Preparedness Directorate's National Cyber Security Division (NCSD) has been that organization since it was created in June 2003. Since its inception, the NCSD has taken on the broad mandate of HSPD-7 and those provided in the President's National Strategy to Secure Cyberspace, in its mission to work collaboratively with private, public and international entities to secure cyberspace and America's cyber assets.

The NCSD is just one of the valuable preparedness resources within the Department. As part of the Preparedness Directorate, the NCSD works closely with the Office of the Manager of the National Communications System (NCS), which addresses national security and emergency preparedness (NS/EP) telecommunications. These two entities comprise what is now the Office of Cyber Security and Telecommunications. The Office of Cyber Security and Telecommunications works closely with the Office of

Infrastructure Protection to ensure that the ever increasing interconnected nature of physical and cyber security is integrated throughout our overall preparedness efforts.

The National Communications System consists of 23 Federal departments and agencies with assets, resources, requirements and/or regulatory authority regarding national security and emergency preparedness (NS/EP) communications. Established pursuant to Executive Order 12472, the community is administered by DHS as Executive Agent and Manager and it supports the Executive Office of the President (the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget) in the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.

Executive Order 12472 also mandates inclusion of an industry component, the National Coordinating Center (NCC) for Telecommunications, or NCC Watch, a joint industry/Government body operating a 24 hour, 7-day a week watch center to coordinate NS/EP communications activities. The NCC Watch has a unique relationship with members of the private telecommunications sector in the Communications Information Sharing and Analysis Center (ISAC). The Communications ISAC provides an opportunity for private sector industry to partner with government to exchange information and coordinate restoration of communications assets and services during emergencies. In this role, the NCC Watch communicates daily and shares a web-portal with NCSD (US-CERT) on cyber related issues.

To meet its mission, the NCSD is focused on leading a cyber risk management program, and building and enhancing the National Cyberspace Response System. To address these priorities, the NCSD is engaged in a public-private partnership which is incorporated into all of NCSD's programs. This is especially critical since the vast majority of our national assets and critical infrastructure are owned and operated by the private sector.

National Cyber Risk Management Program

The National Cyber Risk Management Program reflects the Department's overall strategic approach that is focused on risk management, as outlined in the National Infrastructure Protection Plan (NIPP). The NIPP incorporates the Department's overall risk management framework to assess and reduce our cyber risk, and improve our planning for response, recovery, and reconstitution of our critical networks.

- The Department released the NIPP on June 30 of this year after consultation with industry. The NIPP formalizes the collaboration between government and industry through the Sector Partnership Model with Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC) working together to address risk by analyzing consequences, vulnerabilities, and threats.
- The NIPP provides a unifying structure for protection of the Nation's 17 critical infrastructure and key resources (CI/KR) sectors designated in HSPD-7, including the Information Technology Sector and the Internet. The NIPP calls upon each sector to develop a Sector Specific Plan based on the risk management framework. DHS is the Sector Specific Agency (SSA) responsible for both the Information Technology Sector and the Communications Sector, and assists other sectors with the cyber elements of their infrastructure. The NCSD works closely with the IT Sector Coordinating Council, which was formally launched in January of this year. The IT-SCC and IT-GCC are working together on the IT Sector Specific Plan, which will be completed at the end of the year.
- In order to accomplish the risk management objectives of the NIPP, we have been working closely with the private sector to build the framework required.

> To facilitate the development of this partnership, the Department has established the Critical Infrastructure Partnership Advisory Council (CIPAC). The CIPAC comprises representatives from each of the critical infrastructure and key resources (CI/KR), sectors, SCCs, and GCCs, and provides a mechanism for the information exchange and collaboration between industry and government that is so crucial to understanding the risk we face. The Council also prioritizes the protective measures that need to be taken to reduce that risk.

As we develop the IT Sector Specific Plan and deepen our collective understanding of the cyber risks in other sectors, we are building the foundation for the development of a national cyber risk assessment. Working with our government and private sector partners, we are taking steps, such as developing attack scenarios and conducting red cell workshops and exercises, to identify what we are most concerned about in cyberspace, and then using that information to build our response and mitigation plans. As part of our risk management efforts, we have three priority mitigation programs.

First, as discussed above, the Office of Cyber Security and Telecommunications has established an IDWG to address the resiliency and recovery of Internet functions in the event of a major cyber incident. The IDWG is working with government, private sector, academic and international security experts to examine risks, improve preparedness and situational awareness, and identify measures that we can take to protect against nationally significant Internet disruptions. The IDWG conducted a tabletop exercise in June to examine the kinds of scenarios that would have significant impact on the Internet, understand when information exchange between the public and private sector is mutually beneficial, and to determine what roles and responsibilities industry and government should assume in responding to and recovering from such disruptions.

Second, the NCSD is collaborating with the national laboratories for its Control Systems Security Program to bring together government, industry, and academia to address the threats and vulnerabilities of the process control systems that remotely operate and control access to many of our critical infrastructure assets and systems. To support the Program, NCSD has established a US-CERT Control Systems Security Center, which is an assessment and incident response facility located at Idaho National Laboratory. The department also partners with the industry sectors that utilize process control systems in their operations through the Process Control Systems Forum, or "PCSF". The PCSF met recently in San Diego and furthered its work to accelerate the security of control systems, provide a venue for sharing perspectives on cross-sector security issues, and facilitate solution-driven collaborative workshops.

Through the Process Control Systems Forum (PCSF), the Department also partners with the industry sectors that utilize process control systems in their operations. The PCSF met recently in San Diego and furthered its work to accelerate the security of control systems, provide a venue for sharing perspectives on cross-sector security issues, and facilitate solution-driven collaborative workshops.

The third risk mitigation effort is NCSD's Software Assurance Program that seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products and tools to analyze systems for hidden vulnerabilities. In collaboration with industry, academia, and government partners, the Department's approach to addressing software assurance identifies the following as keys to success:

- People – education and training for developers and users
- Processes – practical guidelines and best practices for the development of secure software
- Technology – tools for evaluating software vulnerabilities and quality
- Acquisition – specifications and guidelines for acquisition and outsourcing

To further its efforts, the Software Assurance Program holds semi-annual Software Assurance Forums with other Federal agencies, industry, academia, and international entities to facilitate ongoing collaboration and progress. As part of the program, NCSD has launched "Build Security In" to raise awareness and foster collaborative efforts.

The Office of Management and Budget (OMB) has recently designated NCSD as the Managing Agency for the Information Systems Security Line of Business. As part of NCSD's work with the Federal government, NCSD is currently working to establish a Program Management Office for this government-wide initiative which has an overarching goal of improving the effectiveness and consistency of systems security across the Federal enterprise. This effort will reduce costs through consolidation and standardization of resources. DHS will be working closely with partner agencies in overseeing the implementation of information systems security products and services.

In order to reduce our collective cyber risk we need to raise awareness of cyber security vulnerabilities and understand what we must do as individuals to create a collective, shared secure cyber infrastructure.

NCSD's awareness program leverages partnerships with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the National Cyber Security Alliance (NCSA), as well as our own National Cyber Alert System to reach state and local governments, small businesses, home users, and K-12 and higher education audiences. October is National Cyber Security Awareness Month. In October 2005, together with our state government and industry partners, we reached millions of Americans with a public service announcement, a satellite media tour on how to avoid identity theft in cyberspace, a national cyber awareness webcast for fourth and fifth graders, and many other activities. We look forward to making this year's campaign even more successful.

Cyber space is borderless, and as such, managing cyber risk needs to take into account international activities. NCSD has an international affairs program that seeks to address cyber security globally through cooperation and collaborative action toward building and leveraging the relationships needed to prevent, protect against, respond to and recover from cyber incidents and reduce overall cyber risk.

National Cyberspace Security Response System

There are three elements to the National Cyberspace Security Response System: the U.S. Computer Emergency Readiness Team Operations, or "US-CERT Ops"; the National Cyber Response Coordination Group, or "NCRCG"; and our regional preparedness and recovery efforts.

The first key element, US-CERT, was established in 2003 as a partnership between the Department and the public and private sectors to protect the nation's critical infrastructure and coordinate defense against and responses to cyber attacks. The US-CERT public website, http://www.us-cert.gov, the secure portal for stakeholders, and the National Cyber Security Alert System, provide timely, actionable information to technical and non-technical users. We encourage each of you to sign up for the US-CERT cyber alerts by going to http://www.us-cert.gov.

NCSD/US-CERT has an Operations component, which manages many aspects of the Cyberspace Security Response System, including situational awareness, incident handling and response, malicious code analysis, and strategic operations. Under Federal Information Security Management Act guidelines, OMB requires all Federal civilian agencies to notify US-CERT of any data breaches, unauthorized access, or suspicious activity, including the loss of personally identifiable information within one hour of discovery.

US-CERT maintains a 24x7 secure Watch center; acts as a trusted third party to assist in the responsible disclosure of vulnerabilities; develops and participates in regional, national, and international level exercises; supports forensic investigations with recursive analysis on artifacts; provides malware (software that is designed to infiltrate or

damage a computer system, without the owner knowing) analytic and recovery support for government agencies; coordinates Federal programs of computer emergency response teams and Chief Information Security Officer peer groups for sharing cyber incident information, best practices, and other cyber security information; and, collaborates with national and international computer security incident response teams both in the US and abroad. US-CERT's efforts in these and additional areas build our cyber situational awareness capabilities that allow us to prepare for and defend against cyber attacks, while also enhancing our ability to respond to the attacks.

US-CERT has established the Government Forum of Incident First Response Teams (GFIRST), a community of Federal agency incident response teams, which comprises the government's critical group of cyber first responders. GFIRST meets regularly, and we have hosted two GFIRST conferences to enhance information sharing and collaborative efforts to secure government cyberspace. US-CERT provides an Internet Health Service tool to GFIRST members through the US-CERT secure portal. IHS is a web-based application that provides members with access to several commercially available Internet and security products for use in building their situational awareness capabilities through the monitoring of their respective networks and the overall health of the Internet. In addition, as part of our Situational Awareness Program, US-CERT also leverages information technology for the automated sharing of critical information across the Federal government and analysis of traffic patterns and behavior.

US-CERT has developed a set of informational resources that it provides to our public and private sector stakeholders, including alerts, vulnerability notices, current activity reports, Federal Information Notices provided to the GFIRST community and Critical Infrastructure Information Notices provided to the private sector Information Sharing and Analysis Centers. In addition, US-CERT runs the National Cyber Alert System and the public website reference above, which provide cyber security tips, guidance, and other resource materials to technical and non-technical audiences.

The second key element of the National Cyberspace Security Response System is the National Cyber Response Coordination Group, or "NCRCG". NCSD co-chairs the NCRCG with its counterparts in the Department of Justice and the Department of Defense. The NCRCG includes 13 agencies with responsibility for and capabilities in cyber security matters and works to coordinate national response activities to incidents of national significance. The NCRCG meets monthly to prepare for cyber issues through tabletop exercises and working groups.

In addition to the IDWG's efforts and US-CERT Operations incident handling and analysis functions, the NRP's Emergency Support Function 2 (ESF-2) for Communications, led by NCS, is a critical component of advanced planning and ensuring coordinated recovery efforts. When ESF- 2 is activated, the Manager of the NCS ensures appropriate NS/EP communications support to operations conducted under the NRP. As part of ESF-2, NCSD works closely with NCS on preparing for recovery and reconstitution of critical communications networks and services. In preparation for this year's hurricane season, we have held ESF-2 training and exercise sessions with participation by many Federal agencies and organizations. We have created and published an ESF-2 Operational Plan and a Standard Operating Plan for ESF- 2 supporting agencies to enhance understanding across the spectrum of public and private sector entities that participate in recovery and reconstitution efforts. We have hired two Regional Communications Coordinators for Federal Regions IV and VI communications pre planning with state emergency planners. The NCS has also created more analytical tools for predictive and post-impact analysis.

One of the critical parts of ESF-2 is a management function to coordinate and facilitate the handling of private sector donations for recovery and reconstitution efforts in the immediate aftermath of a disaster such as Hurricane Katrina. We are working with our private sector stakeholders and state and local government partners to establish a set

of requirements for such donations in order to match those needs with the products and services available.

The third key element of the National Cyberspace Security Response System is our regional preparedness and recovery efforts. Our regional efforts have greatly improved DHS's ability to incorporate the work of our government and private sector stakeholders at both the state and local levels. The Pacific Northwest Economic Region and the Gulf Coast Region are increasingly coordinating their efforts as a result of exercises held in the respective regions, and we are working with them to continue their preparedness planning for both cyber security events, and manmade or natural disasters that have a cyber impact. In addition, we are working with our industry stakeholders in the IT-SCC and IT Information Sharing and Analysis Center) to develop plans for industry assistance in the event of an incident that requires surge support to recover and reconstitute critical IT systems. These efforts depend greatly on our partnerships with the full spectrum of affected industries, state and local government stakeholders, and the emergency response community.

Recent Success Stories

I would like to take this opportunity to highlight two recent success stories in our comprehensive cyber security efforts. First, we conducted the first National Cyber Exercise organized and sponsored by the Federal government. Conducted in February 2006, "Cyber Storm" was the largest multinational, cross-sector cyber exercise to date and assessed policies and procedures associated with a cyber-related incident of national significance, as outlined in the National Response Plan's Cyber Annex. The exercise tested, for the first time, the full range of cyber-related response policy, procedures, and communications methods required in a real world crisis.

Cyber Storm exercised the responses of over 100 public and private agencies, associations, and corporations in over 60 locations and five countries. It achieved collaboration in crisis response at operational, policy, and public affairs levels, including participation of more than 30 private sector corporations and associations in the planning, executing, and after action analysis of a federally funded and congressionally mandated emergency response exercise. As mentioned earlier, Cyber Storm exercised the NCRCG as the principal Federal mechanism for coordinating the national response to a cyber incident of national significance. Cyber Storm demonstrated the close cooperation and information sharing needs across Federal agencies, across boundaries, and between the public and private sectors.

First, the exercise reinforced the importance of defining roles and responsibilities, processes and procedures and having strong communications and coordination among the cyber community. In addition, it highlighted the importance of coordinating and integrating incident communications and public affairs outreach. Unlike a physical, self-announcing incident, a set of cyber attacks such as those imagined in the Cyber Storm scenario are not immediately apparent, either in occurrence or attribution. The correlation of multiple incidents proved challenging for our players, and only further demonstrated the importance of public-private relationships and the need to provide on-going training activities, discussions, and exercises to further build those relationships to strengthen our collective response to a cyber incident.

A second accomplishment falls in the international arena. At the end of June, we successfully hosted here in Washington the second multilateral conference on the development of an International Watch and Warning Network, or "IWWN", among 15 countries in the Americas, Europe, and Asia Pacific. The country participants included representatives from their government critical information infrastructure protection organizations, their computer security incident response teams, and their law enforcement agencies with responsibility for cyber crime. The IWWN was established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities.

The June conference established a clear path forward for the IWWN community to enhance global cyber situational awareness and incident response capabilities and marked the launch of a secure Internet portal to facilitate ongoing international information sharing as well as coordination during cyber incidents.

The Road Ahead

As we further develop our programs and leverage our recent successes, there are some efforts we need to undertake in the near term with our industry and agency partners to better prepare ourselves to respond to, and recover from, cyber incidents. These efforts include, but are not limited to:

- Further integration of the cyber security and telecommunications efforts in the Department and with industry to reflect increasing convergence in the sectors;
- Clearer articulation of roles and responsibilities in the public-private partnership for information sharing and incident response through coordinated concept of operations and standard operating procedures;
- Development of the IT Sector Specific Plan in the NIPP risk management framework;
- Development of a national cyber risk assessment based upon the cross sector cyber component of the NIPP risk management framework;
- Share aggregated situational awareness across the civilian agencies, the military, the international community, and the private sector; and
- Further collaboration between US-CERT Operations and the Department of Defense's Joint Task Force-Global Network Operations to leverage our respective expertise and capabilities toward common cyber security objectives.

These action plans have defined benchmarks and milestones to drive and track our progress in each of these areas.

Conclusion

The National Cyber Security Division has established its mission and priority objectives, developed a strategic plan, and undertaken significant steps to implement its strategic plan across the programs outlined here. In this ever-evolving environment, we know that the target will shift to accommodate new threats, new vulnerabilities, and new technologies. We need to be flexible enough to adjust our efforts to meet these new challenges.

Our progress to date is tangible: we have a construct for public-private partnership; we have a track record of success in our cyber operations; we have established relationships at various levels to manage cyber incidents; we have built international communities of interest to address a global problem; and we have tested ourselves at a critical development stage and will continue to examine our internal policies, procedures, and communications paths in future exercises. We are building on each of these achievements to take further steps to increase our cyber preparedness and improve our response and recovery capabilities.

I would like to thank the Subcommittee for its time today and I appreciate this opportunity to bring further transparency to these important cyber security priorities.

MR. UPTON. Mr. Moran.

MR. MORAN. Thank you. Good morning, Chairman Upton, Mr. Markey, and distinguished members of the subcommittee. My name is Ken Moran. I serve as the Director of the Federal Communications Commission's Office of Homeland Security. In that role, I am

responsible for coordinating the Commission's policies and activities with respect to homeland security and emergency preparedness.

The importance of effective communications cannot be overstated, especially during emergencies. The attacks of September 11 and the unprecedented devastation caused by Hurricane Katrina remind us to be prepared for both natural and manmade disasters. Effective response to a disaster, regardless of its cause or lack of advanced notice, is tied to the ability of first responders and commanding control authorities and the public to communicate. Immediate, secure, and reliable communications are needed across all platforms.

Today, I am testifying about the Network Reliability and Interoperability Council, known as the NRIC, a Federal advisory committee chartered by the Commission. I will also share some of the lessons the Commission learned from its experiences in dealing with Hurricanes Katrina, Rita, and Wilma.

This subcommittee's attention to cybersecurity issues comes at an important time in the development of broadband and IP-based networks. Communications traffic is increasingly migrating to these high speed packet based technologies. With the rollout of these technologies, we are seeing a network security environment very different from that of public switch telephone network, or PSTN. Unlike the PSTN, Internet based communications systems are decentralized and far more open. As a result, they present new and difficult challenges in order to deliver the expected high level of reliability and security.

The Network Reliability and Interoperability Council examines ways to improve and strengthen the Nation's critical communications networks. NRIC members agree on best practices through a process of consensus and adopts solutions that are field tested. In recent years, NRIC subject matter experts contributed thousands of hours in study and dialog that resulted the identification of best practices that address business continuity, physical security, and public safety communications. In fact, over 200 best practices address cybersecurity issues. The Commission is actively promoting both the awareness and the implementation of these best practices.

Last fall, Hurricane Katrina caused an enormous amount of damage to the communications infrastructure. The Commission chartered an independent committee called the Katrina Panel to analyze the impact that Katrina had on critical infrastructure to examine the overall recovery effort and to recommend ways for improvement. In June of this year, the Katrina Panel completed its work and produced a report with a number of important recommendations. The Commission subsequently released a notice seeking comment on these recommendations. Here are a few.

The Federal Government should encourage and work with each communications sector to develop and publicize readiness checklists. State and local authorities should keep a reserve supply of communications equipment, including IP gateways, for quick restoration in communications functionality. The FCC should serve as the single point of contact within the Federal Government for communications data collection. The FCC should work with the Department of Homeland Security and the Congress to improve the credentialing processes and have critical infrastructure providers treated as emergency responders under the Stafford Act.

In large measure, the functioning of the Internet is dependent on communications networks that carry packet-based information through both wired and wireless systems. These communication networks support e-commerce measured in billions of dollars per year. They enable many new communications applications, including the use of voice over the Internet, and they help first responders use IP solutions for interoperability.

The Commission is actively engaged in promoting the development of new technologies to ensure that robust, reliable, and readily restorable communications networks exist to lead our Nation into the future.

I would be pleased to answer your questions. Thank you.

[The prepared statement of Kenneth P. Moran follows:]

PREPARED STATEMENT OF KENNETH P. MORAN, DIRECTOR, OFFICE OF HOMELAND SECURITY, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Good morning, Mr. Chairman and distinguished members of the Subcommittee. My name is Ken Moran and I serve as the Director of the Federal Communications Commission's Office of Homeland Security. In that role, I am primarily responsible for coordinating the Commission's emergency preparedness and critical infrastructure protection efforts. Specifically, my role is to help the Commission: (1) strengthen measures for protecting the Nation's critical communications infrastructure; (2) facilitate its rapid restoration during disasters; and (3) ensure the Nation's emergency responders have access to effective communications services at all times.

In my testimony today, I will describe advisory councils, such as the Network Reliability and Interoperability Council (NRIC) and the Media Security and Reliability Council (MSRC) that the Commission uses to promote highly reliable and rapidly restorable communications systems for the Nation, including the Internet. Then, I will describe some of NRIC's cyber-security best practices. Finally, I will review the lessons the Commission has learned during last year's catastrophic storms.

The Importance of Communications in Times of Disaster

The September 11, 2001, terrorist acts and last year's devastating hurricanes starkly illustrate the need for reliable communications during emergencies. During 9/11, for example, first responders and medical personnel were alerted of the tragic events by a range of telecommunications platforms, including pagers, cellular telephones, wireline telephones, and the Internet. Long distance communications, including satellite telecommunications, were used to initiate the movement of equipment and personnel into the affected areas for restoration purposes. All levels of government coordinated their restoration and homeland defense efforts through wireless and wireline phones, Internet networks, and pagers. After Hurricane Katrina and Rita, when communications infrastructures had been destroyed or impaired, the absence of

familiar methods of communication severely hampered the relief and recovery effort. Clearly, the need for immediate, secure, and reliable communications services is no more obvious than during a large-scale disaster.

As more and more traffic on the public telecommunications network migrates to Internet-based technologies, the importance of these technologies and the services they can bring to the public safety and homeland security community grows in proportion. As this migration proceeds, the well-understood and secure environment of the existing switched telephone network will be overtaken by the vastly more complex environment of Internet-based communications. Today's public networks, while complex, have the benefit of being nearly closed systems to which only a few trusted individuals have access. This makes security relatively easy to manage. On the other hand, Internet-based communications systems are de-centralized and use open systems; as a result, there are substantial challenges to prevent cyber attacks and to ensure their overall reliability.

The Network Reliability and Interoperability Council

In 1992, the Commission established the Network Reliability and Interoperability Council (NRIC) in accordance with the provisions of the Federal Advisory Committee Act. The Nation had experienced a series of major service outages in various local exchange and inter-exchange telephone networks, and the Commission established the NRIC to study the causes of service outages and to develop recommendations to reduce their number and their effects on consumers.

The first NRIC consisted of CEO-level representatives from carriers, equipment manufacturers, state regulators, and large and small consumers. Under its initial charter, NRIC commissioned studies in the areas in which the Council believed reliability concerns to be

greatest – network signaling, cable cuts, switching system failures, power failures, fires, 911 outages, and digital cross-connect systems. The Council's analysis led to the development of nearly 300 Best Practices and other recommendations, most of which, though formally presented to the Commission, were intended to guide communications industry participant operations and network investments.

Best Practice development is not unique to the communications industry. However, the specific topic areas covered in the NRIC Best Practices are. For example, communications industry Best Practices would be the "best in class" methods and procedures for carrying out operational functions like network engineering, service provisioning, network monitoring, and network maintenance. Best Practices are agreed upon through a consensus process and are not product-specific. They address classes of issues with practical solutions that are already in use by at least some members of the industry before they are considered by NRIC.

Over the years, the membership of NRIC has expanded to include CEO-level representatives of wireless, Internet Service Provider (ISP), Cable television (CATV) and satellite firms. As NRIC's representation has grown, the body of Best Practices has kept pace by addressing important reliability issues connected with these emerging communications platforms.

In the months after the September 11 attacks, NRIC VI was asked to take a close look at communications security. Focus Groups were formed to address business continuity, physical security, public safety communications, and cybersecurity. Thousands of staff-hours were contributed by subject-matter experts, who produced hundreds of new Best Practices, all of which are available at the NRIC web site – www.nric.org.

To conduct its work in the area of security NRIC assessed vulnerabilities in Internet networks and public telecommunications networks and determined how best to address those

vulnerabilities to prevent disruptions that would otherwise result from terrorist activities, natural disasters, or similar types of occurrences. Likewise, NRIC reported on existing disaster recovery mechanisms, techniques, and practices and developed additional Best Practices to more effectively restore Internet and telecommunications network disruptions arising from attacks and natural disasters. The work on cybersecurity has led to over 200 Best Practices to help service providers engineer, operate and maintain secure networks.

NRIC Cybersecurity Best Practices

The NRIC cybersecurity Best Practices can be categorized into several areas, including: (1) updating software; (2) secure equipment management; (3) intrusion prevention and detection; and (4) intrusion analysis and response.

Updating Software. New vulnerabilities regularly arise after network operators have placed new software in operation in their networks, so keeping system software up to date is vital to continued security of the network. For example, NRIC has a Best Practice entitled "Expedited Security Patching" to address this issue. This Best Practice specifies that service providers should have special processes and tools in place to quickly patch critical infrastructure systems when important security patches are made available.

Secure Equipment Management. Communications networks often manage network equipment remotely and automatically. These capabilities can provide significant operational benefits; however, this remote management capability can also expose networks to significant risks of unauthorized access. Many NRIC Best Practices cover remotely managed equipment and ensure, as fully as possible given current technologies, against damage or unauthorized access to network equipment.

Intrusion Prevention and Detection. Despite the best equipment management and patching practices, communications networks, by their very nature, can be susceptible to intrusion. Therefore, a necessary component of any security regime will be procedures to ensure timely and appropriate intrusion detection and response. These procedures should be calibrated to most quickly detect and respond to those network intrusions that, by virtue of their location, pose the greatest threat to the continued reliable and secure operation of the affected network. Leaving unused network services running can enable hackers to plant code for the initial phase of an attempt to incapacitate a network target by inundating it with traffic, also know as a "Distributed Denial of Service" attack. NRIC includes a Best Practices that gives service providers detailed advice on how to erect defenses against intruders and how to use systems that have been compromised.

Intrusion Analysis and Response. Physical damage or disruption of network components, whether the product of natural or man-made events, poses another significant threat to our communications networks. Accordingly, proper network-security practices dictate that network operators be prepared to quickly respond in the event that network components sustain physical damage or experience degraded operating efficiency. This would include having appropriate redundancies built into the network and having adequate repair and replacement plans for network components likely to sustain physical damage.

Outreach

While many of the largest telecommunications industry participants are members of NRIC, there are many others that have not been intimately involved in the process. The Commission has turned its attention to outreach and education to expand the range of awareness and encourage implementation of NRIC Best Practices, including those aimed at improving

cybersecurity. Venues for these educational seminars include state and national telecommunications associations, with a primary emphasis on reaching small independent service providers.

Hurricane Katrina

The massive damage and loss of life caused by last year's hurricane season is well known. As I am sure you are also aware, most of the communications industry sustained tremendous damage to their facilities in the affected area, and the damage had a significant impact. The damage to the communications infrastructure hampered the rescue operations of emergency responders. Relief efforts and survivors struggled with the effects of the hurricane. Survivors lacked information about relief efforts. People displaced from their homes did not have the means to contact their loved ones to let them know they were safe. And of course, survivors remaining in the affected area lacked a reliable means of contacting the authorities and getting help in life-threatening situations.

In the months after Hurricane Katrina, the Commission established the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks (Katrina Panel). The Panel was charged with (1) reviewing the impact of Hurricane Katrina on telecommunications and media infrastructures; (2) reviewing the effectiveness of the recovery effort; and (3) recommending to the Commission ways to improve disaster preparedness, network reliability, and communication among first responders. The Katrina Panel produced a report and recommendations in June of this year. Shortly thereafter, the Commission released a Notice of Proposed Rulemaking (NPRM) seeking comment on the Katrina Panel's report and recommendations.

A number of the recommendations will likely lead to more reliable Internet services. For example, the Katrina Panel recommended that the Commission work with and encourage each industry sector, including IT, to develop and publicize sector-specific readiness checklists. These checklists would be based on relevant best practices developed by the NRIC and MSRC, and would include business continuity plans, exercises, development of communications plans and routine archival of critical system backups and providing for their storage in "secure off-site" facilities. The Panel suggested that the Commission coordinate with other federal and state agencies to identify a single repository/point of contact for communications outage information in the wake of an emergency. In this regard, the Panel recommended that the FCC serve as the single point of contact and that it work with affected industry members and their trade associations to establish consolidated data sets and geographic areas for data collection. The Panel also suggested that the Commission work with Congress and other appropriate federal departments and agencies to improve the credentialing process and to provide emergency responder status under the Stafford Act for critical infrastructure providers. The Report also encouraged state and local jurisdictions to retain and maintain a cache of equipment components, including IP gateways that would be needed to immediately restore existing public safety communications within hours of a disaster. The Commission is currently reviewing the more than 100 comments and reply comments filed in response to this NPRM.

Conclusion

Internet-based telecommunications systems are becoming increasingly important to the Nation. Legacy telephone service is now supplemented by various forms of Internet telephone service. Internet-based applications have entered the mainstream and broadband access connections continue to make their way into our homes and businesses. With this change comes

increased opportunity, as well as increased risk. The opportunities stem from the Internet's ability to transport and deliver multimedia services over an integrated broadband network. At the same time, high performance computing platforms that were once largely isolated from the network are now interconnected and open to compromise if unprotected. The Commission, through the policies and actions described today, is working to protect the integrity and reliability of the critical communications infrastructure.

I would be happy to respond to your questions.

MR. UPTON. Mr. Weafer.

MR. WEAFER. Mr. Chairman, Ranking Member Markey, distinguished members of the subcommittee, thank you for inviting me here today to testify about protecting our Nation's critical infrastructure

from cyber attacks. My name is Vince Weafer and I'm the Senior Director of Symantec Corporation.

I commend the committee for bringing attention to this critical issue of the threat of potential cyber attacks against our Nation's information infrastructure. I would like to provide you with the current assessment of the vulnerabilities of our Nation's critical infrastructure and share with you some insights of how cyber crime is undermining consumer trust and confidence in using the Internet for commerce.

Before I turn to the substance of my testimony, I would like to provide some background on Symantec. We are a local leader in information security. Symantec provides solutions that assure security, availability, and integrity to our customer's information. Headquartered in Cupertino, California, Symantec employs over 15,000 professionals and has operations in over 40 countries.

I am responsible for Symantec's Security Response global research teams, whose research provides rapid response to the latest Internet security attacks. Our global intelligence network consists of over 40,000 sensors monitoring the computer activity in over 180 countries. We operate four security operation centers worldwide, in the United States, here in Alexandria, England, Germany, and Australia. Each provides preemptive managed protection to potential cyber threats 24/7. In short, if there is a class of threat on the Internet, Symantec knows about it.

The important message regarding our Nation's cybersecurity landscape is that threats in our critical infrastructure are absolutely real, and without a doubt growing in intensity and volume. The question is not if or when, but when will we be attacked; how severe will that attack be?

Today's cyber threat landscape has changed. Internet attacks these days are not the large scale fast-moving virus or worm pandemics that we saw with frequency just a couple of years ago. Consider this: from 2002 to 2004, there was almost 100 medium to high severity attacks. Last year, there were only six, and this year, there have been none.

What happened?

Well, we have certainly made significant headway in containing these sort of threats, but the very nature of the risk we face has also changed. Cyber crime is now the dominating security threat we are seeing today. In the past, cyber attacks were largely designed to destroy data and gain notoriety, but today's attacks are increasingly designed to silently steal information for profit or advantage. Fraud, intelligence gathering, and gaining access to vulnerable systems are the motivation behind today's attacks.

How do many of these threats arrive in the consumer's computer? A lot do so through botnets, programs that provide attackers unauthorized

and secret control of the computer. Botnets are the engines that drive most of the criminal activity we see today, as their use distributes spam, phishing, malicious code, as well as storage for illegal material. Many of these botnets are created on systems owned by home users, small businesses, and even some large corporations.

Symantec releases a biannual Internet security threat report, or ISTR, which includes a worldwide analysis of Internet attacks, which review known threats, vulnerabilities, and security risks. The findings consistently reveal that a strong growth in cyber crime software built for the purpose of committing online scams, stealing information, bots, keystroke loggers, spyware, adware, and Trojan horses.

Attackers are not focusing just on GAN systems, but the exploitable web browsers and also on the weaknesses of Web servers and Web applications themselves. Bots are contributing to the rise in cyber crime threats in the United States, having the highest percentage of bot commander control servers in the world. There has been an increase in modular malicious code, which initially possesses limited functionality, but is designed to update itself with new, more damaging capabilities.

With all of these threats and vulnerabilities that exist on today's Internet, it is difficult to quantify the economic impact of cyber crime, but according to the cyber crime costs about $47 billion to U.S. businesses last year. A report by the Congressional Research Service also found that cyber attack targeted firms suffer stock price decrease of about 1 to 5 percent in the days after attack, which translates into shareholder loss of between $50 and $200 million.

Over the past year, more than 53 million records of Americans' private, personal information, an average of over 142,000 times per day, have been hacked into, lost, stolen, or otherwise compromised from digital databases. The cost of these breaches is astounding. According to the Federal Trade Commission, identity thefts cost businesses annually $48 billion, and last year, consumers lost $680 million. But more damaging than loss of money is a lost of trust and confidence by consumers in the Internet. That is why we can't risk losing the public's trust in online commerce, but we are. According to a survey conducted by the Conference Board, 41 percent are purchasing less online because of security concerns, and a survey by the Cybersecurity Alliance found that 32 percent of respondents strongly believe their financial information gets stolen.

Congress can help fight cyber crime and cyber terrorism by investing in cyber safety education, awareness, increase funding for cyber R&D, passing strong national data breach law, extending international cyber crime law enforcement efforts, and requiring an Internet reconstitution plan for the U.S. government.

I would be happy to elaborate on these points and any questions the committee may have. Thank you.

[The prepared statement of Vincent Weafer follows:]

PREPARED STATEMENT OF VINCENT WEAFER, SENIOR DIRECTOR, SYMANTEC SECURITY RESPONSE, SYMANTEC CORPORATION

Summary of Points for Vincent Weafer Testimony

- It's vitally important that we pay attention to the threats to our nation's security including the clear and present danger of potential cyber attacks against our nation's information infrastructure.
- An attack against the U.S. that combines both cyber and physical elements could be particularly devastating. The threats to our critical infrastructure are absolutely real and, without a doubt, growing.
- Cybercrime is the dominant security threat we're seeing today and there's been a marked increase in the use of "crimeware," or software used to conduct cybercrime.
- Cybercrime is undermining consumer trust which in turn is eroding the publics' confidence in performing commerce over the Internet. There are economic consequences that cyber attacks are having on the U.S. economy.
- The cyber threat landscape has changed. In the past, cyber attacks were largely designed to destroy data or gain notoriety, but today's attacks are increasingly designed to silently steal data for profit or advantage, without leaving behind the system damage that would be noticeable.
- Symantec's most recent Internet Security Threat Report (ISTR) found that the last 6 months have seen growth in attack trends, bot infections denial of service attacks, malicious code such as Trojans and phishing attacks.
- Symantec's ISTR found that attackers are moving away from large, multiple purpose attacks against traditional security devices such as firewalls and routers. Instead, they are focusing their efforts on smaller regional businesses using combination of employee and end user desktops and Web applications to steal corporate, personal, financial, or confidential information.
- Programs that provide attackers with unauthorized control of a computer, known as bots, also contribute to the rise in cybercrime threats. Symantec identified an average daily total of 57,717 active bot network computers per day or a total of 4,696,903 distinct active bot network computers over the six month period. In the first six months of 2006, the United States had the highest percentage of bot command-and-control servers with 42% of the worldwide total. As a result of this fifty-eight percent of all spam detected worldwide originated in the United States
- If we fail to create a trusted digital environment, we won't just slow the growth of e-business, but of all business. And this is the real hidden threat today – not some massive cyber attack, but the loss of consumer confidence in the digital world.
- It is difficult to quantify the economic impact of cyber crime but according to the FBI's 2005 Cyber Crime Survey cyber crime costs about $67 billion to U.S. firms over the last year.
- The cost of these breaches, in terms of time and money, is astounding. According to the Federal Trade Commission identity theft costs businesses $48 billion annually, and last year cost consumers $680 million in losses. On top of that, identity theft victims collectively spent almost 300 million hours trying to repair damage.
- In this country, we need one, national data-breach law. The business community must join together with Congress to push for comprehensive privacy legislation.

Overview

Chairman Upton, Ranking Member Markey, distinguished members of the Subcommittee: Thank you for inviting me here today to testify about protecting our nation's critical infrastructure and the opportunity to provide you with an overview of the current cyber threat landscape. My name is Vincent Weafer and I am the Senior Director of Security Response for Symantec Corporation.

I'd like to begin by commending the Subcommittee for bringing attention to this critical issue. It's vitally important that we pay attention to the threats to our nation's security including the clear and present danger of potential cyber attacks against our nation's information infrastructure.

Our society's increasing dependence on computers means that the disruption of our networks whether due to nation-states, terrorists, criminals, or simply pranksters could seriously impair public safety, national security, economic prosperity and, more generally, our way of life. An attack against the information technology backbone of one of our nation's so-called critical infrastructures such as communications services, energy, financial services, manufacturing, water, transportation, health care, and emergency services could disrupt Americans physical and economic well-being and have a worldwide impact. An attack against the U.S. that combines both cyber and physical elements could be particularly devastating, such as a physical attack against a building combined with disruption of the telecommunications infrastructure needed to provide emergency services to the physically affected area.

Accordingly, I would like to devote my testimony today to two issues. I would first like to provide this Subcommittee with Symantec's updated assessment of our nation's cyber security landscape and discuss the vulnerabilities of the U.S. information infrastructure to cyber attacks.

Second, I'd like to discuss the considerable negative impact that cybercrime is having on undermining consumer trust which in turn is eroding the publics' confidence in performing commerce over the Internet. Finally, I will discuss the economic consequences that cyber attacks are having on the U.S. economy.

Background on Symantec

Before I turn to the main substance of my testimony, I would like to provide you background on Symantec Corporation. Symantec is the global leader in information security. We provide solutions to help individuals and enterprises assure the security, availability and integrity of their information. Symantec's Norton brand of products is the worldwide leader in consumer security and problem solving solutions. Headquartered in Cupertino, California, Symantec employs over 15,000 professionals and has operations in more than 40 countries.

I am responsible for the Symantec Security Response global research teams. My mission is to advance the research into the new Internet security threats and to provide the most trusted and rapid response to today's complex threats, security risks and cyber attacks. Symantec Security Response protects a variety of businesses, consumers and government agencies from the latest security threats. Symantec Security Response consists of dedicated intrusion experts, security engineers, virus hunters, and global technical support teams that provide our customers with comprehensive, global, 24x7 Internet security expertise to guard against today's complex Internet threats.

Symantec gathers our research from our "Global Intelligence Network" which consists of more than 40,000 sensors monitoring activity on computers in more than 180 countries. We gather data from over 120 million computer systems that use Symantec's anti-virus products and probe over 2 million decoy email accounts. Symantec also operates 4 cyber Security Operations Centers spread across the globe –including Alexandria, Virginia; London, England; Munich, Germany; and Sydney, Australia – each dedicated to relentlessly searching the Internet for potential cyber threats 24 hours a day,

365 days a year to provide managed, pre-emptive protection for our customers. If there is a class of threat on the Internet Symantec knows about it.

State of the Nation's Cyber Security Landscape

As the company representative of the security technology industry on this morning's panel, I want to stress an important message about our nation's cyber security landscape: First, the threats to our critical infrastructure are absolutely real and, without a doubt, growing. The question is not if or even when we'll be attacked but how severe will the attack be.

Today, I stand before you to say that the threat has changed.

The main risks to information these days are not the large-scale, fast-moving virus or worm pandemic type attacks that we saw with frequency just a couple years ago. Consider this: from 2002 to 2004, there were almost 100 medium-to-high risk attacks. Last year, there were only six and so far in 2006, there have been none.

What happened?

We've made significant headway in containing and repelling these sorts of threats. And an equally big part is that the very nature of the risks we face has changed. In the past, cyber attacks were largely designed to destroy data or gain notoriety, but today's attacks are increasingly designed to silently steal data for profit or advantage, without leaving behind the system damage that would be noticeable to a user.

Fraud, intelligence gathering and gaining access to vulnerable systems are the motivation behind many of today's attacks. The attackers are not interested in notoriety. They're interested in flying below the radar, using lower profile, more targeted attacks, attacks that propagate at a slower rate in order to avoid detection and thereby increase the likelihood of successful compromise. Instead of exploiting vulnerabilities in servers, as traditional attacks often did, these threats tend to exploit vulnerabilities in client-side applications that require a degree of user interaction, such as word processing and spreadsheet programs. A number of these have been zero-day vulnerabilities. These types of threats also attempt to escape detection in order to remain on host systems for longer periods so that they can steal information or provide remote access. They're increasingly interested and capable of perpetrating silent, highly-targeted attacks to steal sensitive personal, financial, and operational information using data mining techniques to identify the victims and improve the effectiveness of the attack.

Cybercrime is the dominating security threat we're seeing today and there's been a marked increase in the use of "crimeware". Crimeware is software built with the purpose of committing online scams and stealing information; it includes (but is not limited to) bots, keystroke loggers, spyware, backdoors, and Trojan horses or software used to conduct cybercrime.

Symantec just compiled the latest cyber threat data for our tenth Internet Security Threat Report, or ISTR, which is widely acknowledged to be the most comprehensive analysis of security activity for today's information economy. The Report includes an analysis of network based attacks on the Internet with a review of known threats, vulnerabilities, and highlights of malicious code and additional security risks. Symantec has provided this Report semi annually since 2002.

The ISTR also offers security best practices for consumers and businesses to help them protect against current and emerging cyber crime threats. Symantec's ISTR found that the last 6 months have seen growth in attack trends, bot infections denial of service attacks, malicious code such as Trojans and phishing attacks.

Symantec's ISTR found that attackers are moving away from large, multiple purpose attacks against traditional security devices such as firewalls and routers. Instead, they are focusing their efforts on regional targets, desktops and Web applications that may allow an attacker to steal corporate, personal, financial, or confidential information; this information could then be used for additional criminal activity. Attackers are

focusing not just on the end users systems via exploitable browser vulnerabilities, but also on weaknesses in the web servers and web applications. They can use that weakness to drop malicious code such as a keyboard logger onto a users system, when the unwitting and unprotected user browses or 'drives-by' the compromised Web site. This attack impacts both the end user privacy, as well as the brand name of the company whose Web presence has been compromised.

Programs that provide attackers with unauthorized control of a computer, known as bots, also contribute to the rise in cybercrime threats. Symantec's March 2006 Internet Security Threat Report identified an average of 9,163 infected computers each day—bot networks are being increasingly used for criminal activities such as DoS-based extortion attempts. We believe we will see a continuing growth trend in the area of botnet infected computers. During that period, the United States had a very high percentage of the bot command-and-control servers worldwide. Symantec expects this trend to continue.

Botnets are the engine that drives most of the criminal activity, as they get used by to distribute Spam, Phishing messages, malicious code as well as storage for illegal material. Many of these botnets are created on systems owned by home users, small businesses and even some large corporations.

Symantec estimates that the measurement above is only capturing a portion of global activity and that the actual infection numbers are likely to be much higher. In our March 2006 Internet Security Threat Report Symantec identified an average of 1,402 DoS attacks per day—a 51 percent increase over the previous reporting period. Our Reports consistently show that the United States was the target of the most DoS attacks, accounting for over half of the worldwide total.

We believe that this growth trend will continue as attackers leverage an increasing number of Web-based application and browser vulnerabilities.

In Symantec's March 2006 ISTR, we saw, attacks directed at Web application technologies increase—69 percent of the vulnerabilities reported to Symantec affected Web application technologies, a 15 percent increase over the previous reporting period. The new report does see a significant amount of attacks targeted. We found that Web application technologies, which rely on a browser for their user interface, present an easier target for attackers due to their availability over commonly allowed protocols such as HTTP.

Symantec has also consistently seen an increase in modular malicious code, which initially possesses limited functionality but is designed to update itself with new, more damaging capabilities. Modular malicious threats often expose confidential information that can then be used in identity theft, credit card fraud, or other criminal financial activities. According to our March 2006 ISTR, malicious code that could reveal confidential information rose from 74 percent of the top 50 malicious code samples last reporting period to 80 percent this period—an increase of 6 percentage points. Symantec expects this growth to continue to increase in future reporting periods.

These criminals are targeting all sorts of organizations. By leveraging the vast number of new vulnerabilities, the potential introduction of entirely new and more destructive forms of malicious code and cyber attacks tools represents a substantial future risk. Our law enforcement, military and national security agencies face an even more sophisticated threat with all of these new vulnerabilities, zero day attacks and highly targeted attacks.

Right now, more than 20 nations possess dedicated computer attack programs – and that number doesn't include terrorist organizations.[1] Cyber warfare is a part of their war plans.

---

[1] "Information Battleground," *Air Force Magazine*, http://www.afa.org/magazine/Dec2005/1205info.asp.

Indeed, in the first half of 2004, DoD experienced more than 150 hostile intrusion attempts per day. In the first half of 2005, that number was up to more than 500 a day.[2]

More specifically, cybercriminals could attack our computer systems in a variety of ways, causing serious consequences including: (1) compromising the integrity of data, such as deleting records of financial institutions; (2) breaching the confidentiality of data, such as obtaining information from power and energy plants which can then be used to plan a physical attack; and (3) acting as weapons of mass disruption to take-down key Internet nodes whose failure would then lead to a cascading effect, meaning wide-ranging disruption of other parts of our critical infrastructures, or more likely impacting our ability to respond to a physical event.

The Economic Impact of Cyber Attacks and the Undermining of U.S. Consumer Confidence in Using the Internet for Commerce

Unless a trusted relationship exists between businesses and consumers the risks associated with online transactions will become unacceptable. So, the expectations are high. And, the stakes are enormous.

Across industries, companies have built into their business models the efficiencies of these new digital technologies – such as real-time tracking of packages and online commerce. The continued expansion of the digital lifestyle is already built into almost every company's assumptions for growth – and underpins the assumptions for the global economy.

Think about what would happen if banks were forced to stop all online banking and go back to the days of long lines at teller windows. The costs would be enormous. Today, it costs a bank $10 when a consumer originates a loan online. That cost jumps to more thank $200 when the loan is originated through a branch office.

We can't go back to the old way of doing business – and, that's why creating confidence in the digital world is everybody's job. For the individual company, failure to protect their customers' information will result in customers simply taking their business someplace else, to someone they can trust. And they won't necessarily turn to the company around the corner. In the global economy, security can be a competitive advantage – or disadvantage. If consumers can't trust businesses from our country, they'll look all over the world for the one's they believe they can trust. In such a world, security guarantees are very likely to trump the comfort of the local brand.

If we fail to create a trusted digital environment, we won't just slow the growth of e-business, but of all business. We won't just hurt the digital economy, but the economy as a whole. And this is the real hidden threat today – not some massive cyber attack, but the loss of consumer confidence in the digital world.

The IT industry has made huge strides these past few years, and from the evidence at hand we've made significant headway in controlling large-scale, fast moving viruses and worms. The broad adoption of best security practices and defense in-depth strategies, deployment of firewall, antivirus, and intrusion detection software and the progress operating system vendors have made in improving the security of their operating system platforms have made this possible. Mitigating the large scale virus and worm challenge is a major accomplishment but those are yesterday's problems.

Today we face a bigger challenge. As vendors and enterprises have adapted to the changing threat environment this has resulted in more targeted malicious code and targeted attacks aimed at client-side applications, such as Web browsers, email clients, and other applications. These applications are used to communicate over networks and interact with Web-based services and applications and Web sites. Today's threats are silent and highly targeted. They take advantage of the naiveté and inexperience of many

---

[2] "Information Battleground," *Air Force Magazine*, http://www.afa.org/magazine/Dec2005/1205info.asp.

online users. For example, attackers set up fake Web sites with relative ease and dupe people into offering up financial information or making a donation to a bogus charity. And of course, there are the large scale data breaches – some innocent, some inside jobs, and some the work of skilled criminals – that have made identity theft a growing threat to the digital lifestyle.

For six consecutive years, identity theft has topped the annual list of consumer complaints collected by the Federal Trade Commission. Over the past year more than 52 million records of Americans' private personal information – an average of 142,000 per day – have been hacked into, lost, stolen or otherwise compromised from digital databases.

The cost of these breaches, in terms of time and money, is astounding. According to the Federal Trade Commission identity theft costs businesses $48 billion annually, and last year cost consumers $680 million in losses. On top of that, identity theft victims collectively spent almost 300 million hours trying to repair damage.

It is difficult to quantify the economic impact of cyber crime but according to the FBI's 2005 Cyber Crime Survey cyber crime costs about $67 billion to U.S. firms over the last year. A Report by the Congressional Research Service found that investigations into the stock price impact of cyber-attacks show the identified target firms suffer losses of 1%-5% in the days after an attack. For the average New York Stock Exchange corporation, price drops of these magnitudes translate into shareholder losses of between $50 million and $200 million.

But more damaging than the loss of money is the loss of trust and confidence by consumers in the Internet economy which so many of our nation's businesses depend upon. We can't risk losing the public's confidence in online e-commerce but consumers are beginning to rethink doing business on the Internet.

In the first six months of 2006, the home user sector was the most highly targeted sector, accounting for 86% of all targeted attacks. According to a survey of more than 10,000 households conducted by the Conference Board, 41 percent are purchasing less online because of security concerns. And according to a survey by the Cyber Security Industry Alliance, 32 percent of respondents strongly believe that their financial information may get stolen online.

We can't allow this trust to continue to erode. We can't continue to lose the public's confidence and expect to continue the robust digital lifestyle that we've come to enjoy. Trust ultimately, is the foundation of the online world.

But we have a long way to go in educating consumers. For example, a study by Small Business Technology Institute (SBTI) entitled, "Small Business Information Security Readiness," reveals a real lack of appreciation of the true economic impact of information security incidents and a lack of knowledge of cyber threats. Additionally, they find a lack of forward planning and matching investment required to maintain the security necessary to protect small businesses. Shockingly this study found that over 74 percent of small businesses perform no information security planning whatsoever. Such a lack of knowledge and awareness is inhibiting the wide adoption of adequate information security protection.

Recommendations

Let me now discuss some actions that we believe Congress can improve our cyber security.

I. Awareness and Education

Educating our consumers, our small businesses, the operators of the critical infrastructure and all levels of government on the importance of protecting our systems is essential. We need a broad awareness campaign that reaches out to all users of the Internet.

The growing use of always-on broadband connections by home users and small businesses represents a significant amount of computing power, which left unprotected can be taken over and used as zombie machines to damage our networks and the hinder the commerce and services that flow through them.

At the least, these home users should deploy a minimum protection of firewall and anti-virus technology. The remote or wireless-connected worker is also becoming more prevalent and can unknowingly open up a corporate network to potential vulnerabilities and attack through unprotected connections.

Enterprises and government agencies should engage their employees in security awareness programs to ensure better protection of their systems. Whether it's reminding them not to post their passwords on a yellow sticky pad on their computer, or enacting corporate best practices to change those passwords on a regular basis making them difficult to break.

In an effort to better educate consumers, Symantec will participate in the October National Cyber Security Awareness Month initiative organized by the National Cyber Security Alliance (NCSA). As a founding sponsor of the NCSA, Symantec will also support the NCSA's national public service announcement campaign to promote online security among individuals, small businesses and schools.

The NCSA is a non-profit, public-private partnership consisting of businesses, consumer groups, government agencies and educational institutions dedicated to raising the awareness of cyber security issues and best practices. The NCSA provides tools and resources to empower home users, small business, and schools to stay safe online. More information about the organization and the October National Cyber Security Awareness Month can be found at www.staysafeonline.info.

At the enterprise and organizational level, the issue of IT security has for too long been an administrator or a CIO issue. This needs to change. Cyber security needs the attention of the CEO and the boardroom. Only then can we institute the necessary cultural change and focus enough attention and resources to truly address this issue. We urge the Committee to provide much needed resources to the agencies under its jurisdiction such as the Federal Trade Commission, the Department of Commerce and the Federal Communications Commission to promote cyber education to help better inform consumes of cyber threats.

II. Cyber Crime

We need to realize that protecting the Internet is really a global issue, one that requires better international cooperation. First, we need better resources for law enforcement to work on computer forensics, and we need cooperation from industry to assist prosecutors in building cases. Second, the ratification of the Council of Europe's cyber crime treaty is a good starting point but now that this framework is in place we need additional resources for international cybercrime enforcement, training funds and a single point of contact in the U.S. to coordinate such efforts. Third, industry should reach across borders when appropriate, to share information on best practices, threats and vulnerabilities, in order to gain a measure of early warning of potential attacks. Finally there should be a single point of contact in government so that those leaders can communicate at a peer level in times of major cyber attack.

III. Research and Development

Today, industry and government tends to look at the more immediate threats to our cyber infrastructure, rather than a holistic view of encompassing threats of today and tomorrow. It is a view that needs to change. As mentioned earlier, flash threats may be on us in the near future and we must be more proactive in our cyber security practices focusing on behavior blocking and better patch management, including the use of fast, safe and non-disruptive patching. Given the shrinking time from discovery to exploit, we

should engage in projects like real-time vulnerability scanning, management and patching and we must do it together in partnership; industry government and academia alike. The Federal Government must focus on funding cybersecurity R&D to meet the constantly evolving threats that face our nation's critical infrastructure. And the Government must also lead by example, securing its own systems through the use of reasonable security practices.

IV. Clearly Defined Internet Response and Reconstitution Policy

The federal government needs a clearly defined Internet response and reconstitution policy for all agencies and departments. 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. Also, existing organizations and institutions charged with Internet recovery should have sufficient resources and support. For example, little of the National Cyber Security Division (NCSD)'s funding is targeted for support of cyber recovery.

V. Secure Digital Control Systems for Physical Infrastructure

Our nation relies on a digitally controlled utility and commercial infrastructure such as the electrical transmission grid, oil and natural gas, water, waste water, chemicals, telecommunications, transportation, banking and finance – and many critical manufacturing processes. Remote control of distributed critical infrastructure occurs with Supervisory Control and Data Acquisition (SCADA) systems. These systems are designed to be open and interoperable; but their increasing use of the Internet for communications makes them vulnerable to cyber attack. Such attacks could have devastating consequences such as endangering public health and safety, according to the Government Accounting Office. We urge Congress to pass legislation to form a task force of key government agencies, appropriate regulators, experts in the cyber security field, and representatives from utilities and suppliers to meet and recommend concrete actions to improve the security of control systems supporting critical infrastructure.

VI. Direct a Federal Agency to Track Costs Associated with Cyber Attacks

No one in the field is satisfied with our present ability to measure the costs and probabilities of cyber attacks. There are no standard methodologies for the cost measurement, and study of the frequency of attacks is hindered by the reluctance of organizations to make public their experiences with security breaches. The lack of a methodology or measurement program also prohibits knowing how much national efforts to improve cyber security are working. We urge Congress to pass legislation directing the federal government to work with private industry on a methodology to measure the true cost of cyber attacks, and to track those associated costs as part of ongoing national economic assessment.

VII. Pass a National Data Breach Law and Consider Comprehensive Privacy Reform

The business community must join together with Congress to push for comprehensive privacy legislation. Some governments have already stepped to the plate. However, up until now, the U.S. government has been reactive – dealing with important parts of the issue on a piecemeal basis. Currently, U.S. privacy regulations focus on sensitive areas such as financial and health information and protecting children online. It's an approach that, ultimately, will result in a number of different confusing regulations. In light of the growth of identity theft and the rise of invasive threats like spyware, we need a comprehensive response that ensures that information is protected at every step along the way.

In this country, we need one, national data-breach law. Instead of the quilt of state laws, we need one federal law that protects all consumers from data breaches and requires businesses to put in place some type of reasonable security measures. We urge Congress to pass a national data breach law this year that would require notification of affected consumers and would provide tough enforcement policies.

Conclusions

In closing, let me issue this challenge to industry, government and the individual users: We must take cyber security more seriously and we must do it together.

The increasing prevalence of blended threats and the potential for even more fast-spreading and damaging exploits is a serious threat to our nation's information infrastructure and the economic benefits that we derive from it. We need strong leadership from industry and government to promote awareness and education on cyber security, more resources for law enforcement to investigate and prosecute cyber criminals, strong research and development partnerships to tackle the challenges of future threats to the Internet, and more vigilance from business and governments by putting resources and support behind a proactive IT security program.

But most importantly we all as individual users of the Internet need to do our part, to protect cyber space. Experience shows that effective implementations of security solutions cost in the range of 6-8% of overall IT budgets. Few corporations outside of the finance sector, or government departments, have allocated such levels of funding to this critical need. It is time that we put our resources to work to minimize the risk of a serious disruption of our national cyber infrastructure.

Thank you and I look forward to your questions.

MR. UPTON. Mr. Kurtz.

MR. KURTZ. Thank you, Mr. Chairman and other members of the committee. It is a pleasure to be here this morning.

You have asked me to comment on a very broad topic: to look at the importance of cybersecurity, not just as it relates to our critical infrastructures, but across America's economy and for all consumers.

Cyber systems are our newest and most pervasive infrastructure. They drive and organize every facet of our collective and individual lives, from national and economic security to personal health and well-being. And yet, we do not have a strategic national capability to assess how well most critical systems are protected and what the consequences are if they fail. There is little strategic direction or leadership from the Federal government in the area of information security. Insuring the resiliency and integrity of our information infrastructure and protecting the privacy of our citizens should be a higher priority for the Government. We must move beyond philosophy and statements of aspiration to defining priorities in programs.

CSI believes that the Government has a responsibility to lead, set priorities, coordinate, and facilitate protection response. Let me be clear. This is not a call for regulation and intervention. This is a call for leadership. It is myopic to assume that DHS has exclusive government responsibility for the entire continuum of security across the information infrastructure and for all threats.

When we think about the potential impact of cyber threats and attacks on our overall economy, for consumers as a whole we must acknowledge that we have a strategic national interest in cybersecurity and that a much broader review of cybersecurity is required and extended beyond DHS.

We face various forms of cyber attacks every day, and within businesses. Every day, thousands of citizens have their sensitive personal information compromised through data breaches, phishing campaigns, Internet fraud, and other cyber crimes. As a result, consumers do not have confidence that they should in the Internet. A major cyber disruption could prevent companies from operating critical systems, possibly for sustained periods of time. This means the planes may not fly, goods and services may not be distributed, power and gas may not be available, and all this would potentially have a devastating impact on our economy and national security.

In preparing for how to respond to a significant cyber event, the critical unanswered question is what is a suitable role for the Government, including DHS, DOD, and FCC, in facilitating, recovering, and reconstitution from an incident of national significance? The Federal government must engage in a serious inquiry of the following questions. What is an incident of national significance and what is the process for determining such an event? What are its ramifications? What obligations do the private sector entities have to obey a DHS directive or another entity's directive? Who would resolve conflicting demands for scarce cyber resources, such as bandwidth? What authorities should DHS, DOD, and FCC have to help the Nation recover from cyber attacks? We must take a holistic view. United States needs a strategic national information assurance policy.

We have a chart over to your right that you might take a look at. What I have tried to do here is identify a cycle, if you will, for responding, preparing to cyber attacks or cyber difficulties. It is an overly simplistic chart. I will say that right up front, you know. You could add Department of Energy and Treasury, but the point here is that several agencies have a role and responsibility in this process, and it would be helpful if the White House would assert a greater level of coordination and support for these activities as well. This problem clearly extends beyond DHS. DHS has significant issues that it is trying to resolve, and it would help if the White House would step in and ensure greater level of coordination.

DHS, working with other agents, needs to articulate a chain of command for recovery and reconstitution. In addition, DHS needs to articulate an emergency communications system that works, even when standard communications interconnectivity is disrupted. Emergency

communications entail more than simply establishing a resilient mechanism for allowing people to talk; it requires advance identification for the right people being able to use the right language to talk, and I will note that Under Secretary Foresman's report that was released today talks about some of these issues.

A summary of our recommendations: consider the need for a government-wide strategic national information assurance policy; increase attention to cybersecurity; appoint a leader. Everybody has talked about the need for an Assistant Secretary for Cyber and Telecommunications. I don't need to dwell on that more. Plan to prevent or minimize a cyber attack of major significance. Plan to work with the private sector to recover from a major disaster. And I have to urge the Congress to take the step and pass a national bill to secure sensitive, personal information.

Thank you.

[The prepared statement of Paul B. Kurtz follows:]

PREPARED STATEMENT OF PAUL B. KURTZ, EXECUTIVE DIRECTOR, CYBER SECURITY INDUSTRY ALLIANCE

Introduction:

Chairman Upton, Congressman Markey and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Paul Kurtz and I am Executive Director of the Cyber Security Industry Alliance (CSIA).

CSIA is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. The organization is led by CEOs from the world's top security providers who offer the technical expertise, depth and focus needed to encourage a better understanding of security issues. It is our belief that a comprehensive approach to ensuring the security and resilience of information systems is fundamental to global protection, national security and economic stability.

Before joining CSIA, I served at the White House on the National Security Council and Homeland Security Council. On the NSC, I served as Director of Counterterrorism and Senior Director of the Office of Cyberspace Security. On the HSC, I was Special Assistant to the President and Senior Director for Critical Infrastructure Protection.

You have asked me to comment on a very broad topic – to look at the importance of cyber security not just as it relates to our critical infrastructures, but across America's economy and for all consumers. Later today I will testify before the House Homeland Security Committee on a narrow but important piece of your much broader inquiry – cyber security and recovery of our critical infrastructure – so I particularly appreciate the chance to begin that dialogue at the 50,000 foot level you posit.

Right now no one in government is really looking at the macro-level. The fact is that cyber systems are our newest and most pervasive infrastructure. They drive and organize every facet of our collective and individual lives from national and economic security to personal health and well-being – and yet we do not have a strategic national capability to assess how well the most critical systems are protected, and what the consequences are if they fail. Currently, there is little strategic direction or leadership from the federal government in the area of information security. Ensuring the resiliency and integrity of our information infrastructure and protecting the privacy of our citizens

should be higher on the priority list for our government. CSIA believes the government has a responsibility to lead, set priorities, and coordinate and facilitate protection and response.

DHS has a central role in protecting critical cyber infrastructure from massive attack, but government must consider economic consequences and impact to our citizens in a more comprehensive and systematic way.

Clearly DHS has a vital and central role – HSPD 7 designates the Department of Homeland Security as a focal point for infrastructure protection, including cyber security. [We'll get to how well, or poorly, they are doing in just a moment.] But it is myopic to assume DHS has exclusive government responsibility for the entire continuum of security across all information infrastructures, and for all threats. DHS should, indeed ***must*** be accountable for coordinating the protection of our most critical infrastructures from serious attack or devastation. But when we think about the potential impacts of cyber threats and attacks on our overall economy, or for consumers as a whole, we must acknowledge that we have a strategic national interest in cyber security that is much broader than the mandate of DHS or the immediate challenges it faces. We face various forms of cyber attacks and efforts to exploit faulty software code every day. Businesses routinely fight against unauthorized intrusions, whether for sport, industrial espionage, or more nefarious reasons. Companies incur significant costs to keep up with ever-more sophisticated efforts to compromise their systems, ultimately we all bear these costs. And every day, thousands of citizens have their sensitive personal information compromised through data breaches, phishing campaigns, Internet fraud and other cyber crimes. As a result, consumers do not have trust and confidence in online services and e-commerce, with significant economic results for many industries.

The truth is that a major cyber disruption could prevent companies from operating critical systems, possibly for sustained periods of time. This means that planes may not fly, goods and services may not be distributed, power and gas may not be available, and all of this would have a potentially devastating impact on our economy and our citizens.

Most importantly, DHS must consider and articulate how it will work with the private sector to respond to and recover from a massive failure of information technology systems – whether from a cyber attack or a natural disaster. In preparing for how to respond to a significant cyber event, the unanswered question affecting all is: What is a suitable role for DHS as well as other key federal agencies, including DoD and the FCC, in facilitating recovery and reconstitution from a cyber "incident of national significance"? The Federal government must engage in a serious inquiry of the following questions:

- What is an "incident of national significance" and what is the process for determining such an event and its legal significance?
- What obligations do private sector entities have to obey directives from DHS, or other agencies?
- Who would resolve conflicting demands for scarce cyber resources?
- What enforcement power does DHS, DOD, and the FCC have to help the nation recover from a cyber disaster?

These are tough questions, and raise complex policy issues which extend beyond DHS.

We must take a holistic view – the United States needs a Strategic National Information Assurance Policy

The bottom line is that protecting our cyber infrastructure is not just DHS's problem. In large measure, because our cyber infrastructure is almost exclusively owned and operated by the private sector, the front line defense is the investment made by

infrastructure providers on behalf of their customers. But, in addition to DHS, many key departments and agencies have key roles in protecting our cyber infrastructure:

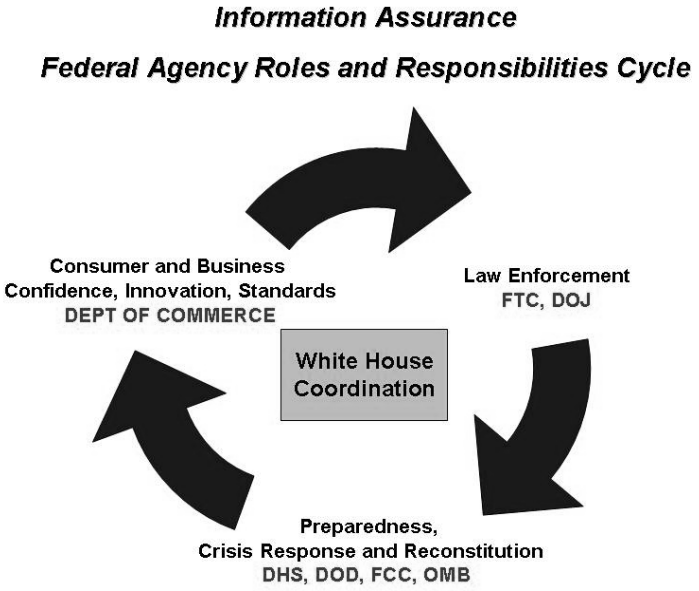
- **The Department of Commerce has a key role.** The Department of Commerce advocates for technological innovation and has responsibility to develop and promote measurements, standards, and technology to enhance productivity, trade, and the quality of life. This includes conducting research to advance the U.S. technology infrastructure and supporting the development of technologies for broad national benefit.[1] The Under Secretary for Technology Administration has the lead in developing and promoting information security standards and in leading research and development efforts to enhance privacy and security. There is much more Commerce could do. For example, Commerce currently does not measure consumer or business confidence in the information infrastructure or the costs of attacks or disruptions. Commerce, in partnership with DHS, could support increased adoption of insurance. Currently, many insurance companies are reluctant to enter this market because of a lack of actuarial data.
- **The Federal Trade Commission has a key role.** The FTC's Enforcement Division conducts a wide variety of law enforcement activities to protect consumers online, including: (1) ensuring compliance with administrative and federal court orders entered in consumer protection cases; (2) conducting investigations and prosecuting civil actions to stop fraudulent, unfair or deceptive marketing and advertising practices; and (3) enforcing consumer protection laws, rules, and guidelines.[2]
- **The U.S. Department of Justice has a key role.** The Computer Crime and Intellectual Property Section (CCIPS) within DOJ's Criminal Division is responsible for combating computer and intellectual property crimes worldwide. CCIPS' Computer Crime Initiative is a comprehensive program designed to combat electronic penetrations, data thefts, and cyber attacks on critical information systems. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.[3]
- **The Federal Communications Commission has a key role.** Charged with regulating interstate and international communications, the FCC has established the following objectives:
    - To evaluate and strengthen measures for protecting the Nation's communications infrastructure.
    - To facilitate rapid restoration of the U.S. communications infrastructure and facilities after disruption by a threat or attack.
    - To develop policies that promote access to effective communications services by public safety, public health, and other emergency and defense personnel in emergency situations. [4]
- **The Department of Defense has a key role.** DoD gives highest priority to securing its national security systems. The Defense Information Systems Agency (DISA) provides a seamless, secure and reliable web of communications networks, computers, software, databases, applications, and other capabilities to meet the information processing and transport needs of DoD. DISA also ensures the integration and interoperability of command and control, communications, computers and intelligence systems.[5]

---

[1] http://www.technology.gov/Index.html
[2] http://www.ftc.gov/bcp/bcpenf.htm
[3] http://www.justice.gov/criminal/cybercrime/ccips.html
[4] www.fcc.gov/homeland
[5] http://www.disa.mil/main/about/missman.html

- **The Office of Management and Budget has a key role.** The government has a critical need to ensure critical Federal IT systems are resilient; after all, our citizens rely on our government not to let them down. Under the Federal Information Security Management Act (FISMA), OMB is responsible for developing and overseeing the implementation of government-wide policies, principles, and standards, as well as providing guidance for the federal government's information technology security program.[6]
- **White House Coordination.** The President's staff must ensure seamless coordination across Federal agencies and ensure sufficient attention and fiscal resources are allocated to the issue.
- **Congress has a key role.** Congress must exercise its traditional role. This Committee, for example, has worked hard to enact effective legislation to protect sensitive personal information; Congress should act before the end of the session to pass data security legislation.

A graphical depiction of this discussion is noted below:



Clearly, as a nation we have a strategic national interest in making sure that we understand the risks across all our cyber infrastructures and who is accountable for their resilience to attack. We urge policy makers to consider the need for a strategic national information assurance policy, developed in consultation with industry, operating across all of government. The policy would address many of the questions I have posed.

[6] http://www.whitehouse.gov/omb/egov/

DHS needs to specify steps to prevent and/or minimize a massive cyber attack or telecommunications disaster

My remaining testimony will reflect on DHS's effectiveness to-date, because the bottom line is that cyber security is receiving inadequate attention from DHS. Of particular urgency is the need for DHS to specify how it and the private sector would coordinate actions if a massive cyber attack were to occur.

Last week in his updated national strategy for counterterrorism, President Bush declared that "America is safer but we are not yet safe." The reality of physical terror occurring in the United States has riveted our attention since the attacks on September 11, 2001. Prevention of any physical incident of horror has since been priority one.

The President's reminder for vigilance clearly applies to threats against our physical well-being, but his admonition should also apply to cyber security. Since 9/11, responsibility for coordinating federal efforts on national safety shifted to the Department of Homeland Security. DHS has predictably reacted to a myriad of security challenges by focusing first on immediate physical threats and natural disasters. This focus is understandable, but it has also impeded progress toward stronger national cyber security. As a result, the United States remains unprepared to defend itself against a massive cyber disruption or to systematically recover and reconstitute information systems after such an event. However, by realistically refining the Department's role in national cyber security, DHS can escalate cyber security efforts along with efforts to prevent physical terror in America.

National coordination of cyber security is the purview of the Department of Homeland Security, and its related leadership position is Assistant Secretary for Cyber Security and Telecommunications. This new position was established in July 2005 by Secretary Chertoff specifically to elevate the importance of cyber security in relation to DHS's main focus on physical security. Unfortunately, fourteen months later, the Assistant Secretary position is unfilled, which reflects the low priority DHS still has toward cyber security. No one is in charge to lead efforts to protect information infrastructure against cyber attacks or to lead response and recovery.

For example, currently members of the IT sector are working with DHS on a sector specific plan as required under HSPD-7 and the National Infrastructure Protection Plan. While we have made progress, there has been little to no senior-level attention to the plan at DHS, as well as several other agencies. The plan seeks to hammer out many of the questions I posited earlier.

DHS has not specified how it will work with the private sector to a cyber incident of national significance

The Cyber Incident Annex of the National Response Plan, published January 6, 2005, states that the federal government plays a significant role in managing intergovernmental (federal state, local and tribal), and, where appropriate, public and private coordination in response to cyber incidents of national significance. DHS is well aware that the private sector "runs the show," which may account for its encouragement of public-private partnerships. However, the Government Accounting Office recently reported that progress on those initiatives is limited, some lack time frames for completion, and relationships between these initiatives are unclear.[7]

Consequently, DHS needs to articulate a chain-of-command for each step of recovery and reconstitution. For example, the DHS's U.S. Computer Emergency Readiness Team (US-CERT) may be aware of a network attack, but the North American Network Operators Group (NANOG) is the operational forum for backbone/enterprise networking.

---

[7] "Challenges in Developing a Public/Private Recovery Plan," GAO-06-863T (July 28, 2006).

In addition to chain-of-command, DHS needs to articulate an emergency communications system that works even when standard telecommunications and Internet connectivity are disrupted. Emergency communications entail more than simply establishing a resilient mechanism allowing people to talk. It also requires advance identification of the right people from appropriate organizations who speak the "same language" for establishing rapid recovery and reconstitution of national systems.

These are but a few of the details that must be articulated and agreed upon in advance if the nation is to truly prepare for recovery and reconstitution from a cyber disaster. Ostensibly, DHS would have a leading role in planning.

These issues should be answered in the DHS's 400-plus page *National Response Plan*. Unfortunately, the plan does not articulate clear answers on how federal agencies work with each other, with other government entities, or with the private sector in responding to a national disaster. Instead of one coordinator, there are at least six: Homeland Security Operations Center, National Response Coordination Center, Regional Response Coordination Center, Interagency Incident Management Group, Joint Field Office, and Principal Federal Official. The *National Response Plan*'s discussion of cyber security is contained in the "Cyber Incident Annex." The Annex mentions many other federal departments and agencies with "coordinating" responsibility for cyber incident response, including Defense, Homeland Security, Justice, State, the Intelligence Community, Office of Science and Technology Policy, Office of Management and Budget, and State, Local, and Tribal Governments. The agency tasked with maintaining the *National Response Plan* is FEMA.

As I draw toward the end of my testimony, I wish to comment on one other topic that also requires close coordination of the government and private sector – namely, the need for a cyber early warning system that provides the nation with situational awareness of attacks. DHS has sponsored some mechanisms toward this end, such as US-CERT, and Information Sharing and Analysis Centers (ISACs) that share some cyber alert data from the private sector with the federal government. As noted by the Business Roundtable, however, the nation lacks formal "trip wires" that provide rapid, clear indication that an attack is under way.[8] This mechanism would be akin to NOAA's National Hurricane Center, which usually can provide a day or so of advance notice before a dangerous storm lands ashore. Cyber attacks provide far less notice to prepare and react. DHS should lead the establishment of an efficient national cyber warning system because the private sector is most likely to first detect an attack, and data correlation and follow through coordination closely involves the government.

Summary of Recommendations

In summary, CSIA offers the following recommendations for the Subcommittee's consideration:

Consider the need for a government-wide strategic national information assurance policy. Cyber security is too important to be left to piecemeal and bifurcated approaches. There needs to be more active engagement by the White House to lead in developing a coherent national information assurance policy across all agencies.

Urge Congress to enact comprehensive data security legislation this year. Sensitive personal information should be protected whether it is being held by a commercial enterprise, non profit organization or government entity. Millions of Americans are looking to the government for help in safeguarding their personal information.

---

[8] Business Roundtable, "Essential Steps to Strengthen America's Cyber Terrorism Preparedness" (June 2006); see also Section 15 of Homeland Security Presidential Directive 5, "Management of Domestic Incidents" (Feb. 28, 2003), and the *National Strategy to Secure Cyberspace* (Feb. 2003).

Increase Attention to Cyber Security. DHS has inadvertently exposed the nation to another vector of attack by providing inadequate attention to cyber security. The Department should reassess its priorities and shift some attention from an almost exclusive focus on physical security.

Appoint a Leader. There is no leadership at DHS in terms of a person who is solely responsible for cyber security. DHS should swiftly fill the open position of Assistant Secretary for Cyber Security and Telecommunications to close the leadership vacuum.

Plan to Prevent or Minimize a Major Cyber Disaster. DHS should shift this energy to articulating a smaller set of priorities focused on preventing and/or minimizing the likelihood or severity of a massive cyber attack or telecommunications disaster.

Plan to Work with the Private Sector to Recover from a Major Disaster. The existing DHS "plan" for recovery cites more than a dozen federal departments and agencies with "coordinating" responsibility – not including state, local and tribal governments. DHS needs to clearly articulate a chain-of-command between government and the private sector for recovery from a major cyber disaster.

With that, I appreciate the opportunity to testify today and am pleased to answer your questions.

MR. UPTON. Mr. Clinton.

MR. CLINTON. Thank you, Mr. Chairman.

The Internet Security Alliance represents about 500 companies operating worldwide from almost every sector. We basically represent the major industrial users of the Internet.

My remarks today will focus on three messages.

First, the threat to this Nation's and the world's economic infrastructure from cyber attack is real and growing. Second, not enough is being done either by government or by industry to secure cyberspace. We can't manage the 21st Century technology solely based on regulatory models designed 2 centuries ago. While regulation has its place, new more creative models built on market incentives must be built. Third, there are concrete steps that can be taken both by industry and by government to create this new model.

Let me start with some core facts. Today, there are more than one billion Internet users. That is a 300 percent increase since 2000. The gross in applications has increased nearly 2,000 percent in that time. Twenty-five percent of America's economic value, $3 trillion a day, moves over the connections on the Internet. The main protocols to protect that data are 30 years old and contain multiple well-known security flaws. The Congressional Research Services estimated the economic impact of cyber attacks to business is about $226 billion. In the first half of '06, banks financial losses from cyber attacks were up 450 percent since 2005. In addition, international terrorists are also becoming increasingly sophisticated in their use of the Net. A terrorist can sit at a computer and create havoc worldwide. They don't need a bomb or explosives to cripple a sector or shut down a power grid.

To address these issues, we have to broaden our thinking about Internet security governance. The Internet is international, interactive, constantly changing, and constantly under attack. The national strategy to secure cyberspace, published in 2002, stated correctly that regulation in this space would be effective and possibly counterproductive. Even if Congress enacted a lightened statute, it would only have reach to our national borders. Even if some agency wrote a brilliant regulation, it is likely to be outdated before it gets through the process and could stunt innovation. But we can't sit idly by and do nothing, either. The best mechanism to ensure sustainable defense is to interject market incentives to motivate the corporations who own and operate the vast majority of the Internet to adopt best practices.

One of the untold stories of Internet security is that we already know a good deal about how to address these issues. Studies show that approximately 25 percent of companies who do currently follow best practices are still intact, but the resulting financial loss, down time, disruption, et cetera is greatly minimized. While many have suggested, hopefully, that a positive return on investment would stimulate enough voluntary action, this has not been the case. Recent research indicates that most companies still do not see security as a core value driver. Various private sector entities are already doing a great deal to address these problems, some of which are detailed in my written statement. We are doing research, creating best practices, providing incentives, coordinating with standard-setting bodies, reaching out to educate the corporate investment communities.

But the reason you asked us here today was to discuss what the Government's role would be, and more specifically, how we can work together. Acting through a range of coalition activities known as the Corporate Information Security working group, the National Cybersecurity Partnership, the WYE II Coalition, et cetera, we have developed an outline of a market-based incentive program to breach the gap between a pure voluntary and regulatory approach. Six weeks ago the National Infrastructure Protection Plan officially embraced the idea of developing a market incentive program by stating, and I quote, "The success of a public/private partnership depends on articulating the benefits of participating to the private sector." There is a clear national security and homeland security interest in ensuring collective protection of our Nation's critical infrastructure. Government can engage industry to go beyond the efforts already justified by their corporate business needs by creating an environment that supports incentives for companies to voluntarily adopt widely accepted security practices.

Now, we move to the hard question: Exactly how do we do this? Fortunately, there exist a number of paths, most with Congressional

precedent, that may provide incentives that are in the national interest. Among these paths are Congress can tie incentives such as civil liability safe harbors, such as those provided in the Safety Act, or provide procurement credits for companies who demonstrate compliance with generated best practices. Congress can stimulate the stunted cyber insurance market by temporarily insuring the risk of a massive cyber hurricane until the market is sufficiently large to take the risk themselves. Congress can create industry, government, and university consortia, similarly to the Symantec model we developed in the 1980's to address our computer chip problem. Congress can use tax incentives to motivate corporations, particularly small ones, to adopt best practices. Congress can create awards programs, such as the Baldrige Program, to make security a market differentiator, just as we did quality a while ago.

My written testimony provides numerous other examples of private sector programs already underway, many without any Federal buy-in.

The bottom line is this, Mr. Chairman. We have a major security problem revolving around the Internet. If we attempt to use the traditional regulatory method to address it, we will be unsuccessful. The Federal government, in cooperation with the private sector, can create an effective and sustainable security system with market incentives.

Thank you, Mr. Chairman.

[The prepared statement of Larry Clinton follows:]

PREPARED STATEMENT OF LARRY CLINTON, CHIEF OPERATING OFFICER, INTERNET SECURITY ALLIANCE

Good Morning, I am Larry Clinton, Chief Operating Officer of the Internet Security Alliance. I also sit on the Board of the National Cyber Security Partnership, and both the IT and Telecommunications Sector Coordinating Councils. In addition, I chair the NCSP Committee on Incentives for Improved Corporate Security. I want to thank Chairman Upton for having this hearing and inviting me to participate on behalf of the Internet Security Alliance.

The ISAlliance represents about 500 companies operating on 4 continents who are primarily major corporate *users* of Internet services. Our diverse membership includes companies from a wide variety of economic sectors including financial services, IT and Telecommunications, entertainment, manufacturing, food services, defense, business consulting and security services. Companies such as American International Group, Mellon Financial Corporation, Northrop Grumman, Visa, Verizon, Verisign, NAM, Sony, Tata Consulting, Raytheon, Nortel and Ceridian, among many others. Companies join ISAlliance because we believe we must work across corporate and national boarders, and engage both security providers and users in order to improve cyber security in a comprehensive fashion. Our goal is to improve cyber security across the nation and the globe through education, training and the creation of market based incentives for action.

My remarks today will focus on three main messages I would like to leave with the Committee today.

First, the threat to this nation's and the world's economic infrastructure from the risk of cyber-attack is real. It is not science fiction. It is not theoretical. It is happening today and in all likelihood will get worse.

Second, regrettably not enough is being done, either by government or industry, to secure cyber space. We continue down this path at great peril. If we are to address the threats we face in the Internet security space, we must broaden our thinking considerably. We cannot manage what is, essentially, the first 21st century technology solely using regulatory models designed two centuries ago. A new, more creative, model built on market incentives and creative solutions must be developed and added to the mix.

Third, fortunately, there are concrete steps that can be taken to both by industry and government to create this new model. Some of these steps have already begun, but we need to pick up the pace of activity considerably.

CYBER THREATS ARE SIGNIFICANT AND GROWING

It was not that long ago that popular myth held that cyber attacks were largely propagated by some Matthew Broderick type High School student playing "war games" with the pentagon computer system to prove how smart he was. If that ever was the case it is no longer. Now the most likely perpetrator is more likely to be agents of foreign countries, organized criminal syndicates or highly educated and trained cyber-terrorists.

Here are some core facts:

- The dot-com bust gave the illusion that Internet growth slowed down, but in fact it has grown at remarkable rates. At the height of the dot-com boom in 2000, for example, roughly 250 million people used the Internet. Today, according to Internet World Stats, more than 1 billion users worldwide rely on the Internet, a 300 percent increase since 2000.

  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 far surpassing the increase in users. While users have increased 300 percent since 2000, the volume of traffic on .com and .net has increased 1,900 percent in that same period.

- This very growth of Internet users, broadband capacity and number of Internet-enabled devices has created an opportunity for hackers, organized criminals and even more serious terrorists to attack our networks. Some do so for technical trophies, some for political objectives, but today, most bad behavior on the Internet is done for financial gain.

  In fact, the very devices and increased bandwidth that make the Internet more robust and user friendly are being deployed to compromise the Internet. Now that computers are always-on, they are easily accessible to hackers and other abusers to hijack. And the increased bandwidth and computing power available literally gives hackers more ammunition to utilize against the infrastructure.

- In October 2002, the Internet community got a wake-up call when the 13 DNS root servers, which serve as the heart of the Internet addressing system, came under heavy denial of service (DoS) attack. In these attacks, the hackers send countless bogus inquiries to domain-name servers, which are computers that direct Internet traffic. By sending phony website requests to these servers, they overload and disable them, making websites unavailable.

  The most alarming of attacks occurred in early January 2006, when a hacker systematically disabled over 1,500 websites using hijacked PCs. In these attacks, the hacker didn't directly attack the domain-name servers. Instead, they sent their traffic to a legitimate server with a DNS query and a forged source

address.

- Twenty-five percent of America's economic value ---up to 3 trillion dollars a day--- moves over network connections each day. The main protocol used to protect this data is over 30 years old and has multiple well-know security flaws. There are now more electronic financial transactions each day than there are paper checks written.

If the Internet were to go down for a just few hours, we would lose hundreds of millions of dollars of economic activity. If it went down for several days, U.S. economic activity would be severely curtailed; payrolls would not be met, securities transactions not cleared; invoices not paid.

- In 2004 the Congressional Research Service estimated that the economic impact of cyber attacks on business grew to $226 billion. In truth, we don't know the precise amount of the economic losses because there is a tremendous disincentive to disclose this information. But we do know it's huge and growing.

- In August 2006 the SANS Institute claimed that bank's financial losses caused by cyber attacks were up 450% from the first half of 2005.

- August 2006 was the worst month in history for data breach notifications according to SANS. Consumers Union tells us that although about 98% of bank robbers get caught, only 1 in a thousand identity thefts are prosecuted. One of the main reasons is again the internet infrastructure itself makes tracing these thieves very difficult.

- There has been a massive increase in cyber crime from organized groups in Eastern Europe and Asia.

This is the on-going chronic cyber security problem we face day in and day out.

However, the threat is not just from criminals. International terrorists are becoming increasingly sophisticated in their use of the global net creating a threat potentially more dangerous than physical explosives. Of course, for some time now, terrorists have used the net for fund raising, communication and recruitment activities. However, there is growing testimony from the intelligence community that they are pursuing methods to inflict a deadly combination of electronic breakdown and serious physical injury either using cyber means alone or in combination with physical explosives.

Former CIA Director George Tenent has said the Internet represents the "Achilles heel" of our financial stability and physical security. Former CIA Director Gates has warned that cyber-terrorism could be the most devastating weapon of mass destruction yet.

In April of 2002, then Homeland Security Director Tom Ridge probably said it best: "Terrorists can sit at one computer connected to one network and can create worldwide havoc. [They] don't necessarily need a bomb or explosives to cripple a sector of the economy, or shut down a power grid."

A recent Google search on the term "cyber-terrorism" found over 900,000 entries.

Accordingly to the Insurance Information Institute, 2005 was the most costly on record for the insurance industry, with insured losses from Hurricane Katrina alone at $40.6 billion and total catastrophe losses for the year from 24 disasters totaling $61.2 billion. We have but to watch the news to see vividly the misery and destruction caused to New Orleans and the surrounding areas.

Now, imagine a hurricane with intelligence. One that learns and grows more destructive with each year. Imagine a hurricane that methodically, intentionally with malice born of a lifetime of anger plans and executes a destructive force to precisely hit the very fabric of our economy and daily life. That is a cyber-terrorism attack.

However, those of us who operate major information systems know that we must worry not just about that cyber-hurricane of the future but of the smaller attacks we are under every day---thousands of times a day.

Thus, it is our job in industry to work with you in government to address not just the large scale, massive, attack scenarios but also to address the chronic cyber security problems we face.

To do this, we must broaden our approach.

WE NEED TO BROADEN OUR THINKING ABOUT INTERNET SECURITY GOVERNANCE

When I say we need to broaden our thinking about the Internet, I mean that we need to do at least three things.

First, we need to realize that the Internet is unlike anything we have dealt with before.

- 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's critical to our national defense, but it is not a military installation.
- It's all these things and much much more.

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

Consequently, it will require a security system unlike anything we have designed before.

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

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 and the FTC. And that system has worked arguably well in most instances.

But that system, whatever its advantages, will not work with Internet security. Even if Congress were to enact an enlightened statute, it would not reach beyond our national boarders and hence would not be comprehensive enough. Even if some agency wrote a brilliant regulation, it is likely to be out-dated before it went 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 compromise, simplify and "dumb-down" the eventual regulations so that we end up with a standard which offends no one, where everyone can attest that they met the new federal regulations, but everyone knows the system is not really working.

That is not to say that regulation doesn't have its place, especially with traditionally regulated industries. It is to say that regulation, standing alone, will not be sufficient.

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.

We, the Internet Security alliance, contend that the best mechanism to assure an adequate and sustainable defense system is to inject the market with a combination of motivations.

We need to have corporations, who own and operate the vast majority of the Internet, to perceive that it is their own self interest to continually improve not only their own security, but that of everyone else with whom they interact.

Sadly, this is not the case now.

A range of studies have demonstrated that corporations, for various reasons, tend to regard security and resilience, including cyber security, as a cost center to be minimized.

Moreover, the enlightened companies will do what they perceive is appropriate to assure the cyber defense within their corporate borders, however, the Internet is a shared infrastructure.

We need to develop a system that assures comprehensive security---and nothing motivates the private sector like market incentives.

Psychologists tell us that punishment as the sole means of behavioral modification doesn't effectively work past the age of two. Rather, the best course of action is the use of the carrot, sometimes alone and sometimes in combination, with an already in place and existing stick.

THE ROLE OF INSURANCE

Numerous private and governmental documents have encouraged the use of cyber-insurance and the creation of a robust cyber-insurance market. There is little wonder about this. Insurance can:

(1) motivate best practices by modifying the availability and affordability of insurance based on the degree of implementation of such best practices,
(2) spread the financial costs of a cyber-attack, especially a massive cyber-attack, among society creating an efficient funding mechanism in the event of "digital Pearl Harbor", and
(3) be a primary distribution channel for risk management information on preventing and mitigating cyber-risks given the history view of the insurance industry as the "risk management experts".

Given that a robust insurance market is necessary to achieve these essential public goods, the question is how best to achieve such a market. While the primary burden is on the insurance sector itself to make this happen, left purely on its own, the industry will move "too little, too late". One main reason for this is that the lack of historical loss information makes the creation of standard actuarial tables impossible leaving carriers to "guesstimate" correct rates, something most carriers do not want to do. Thus, the market is currently estimated to be less than $200 million in premium with only a handful of carriers willing to issue policies.

Fortunately, there are concrete steps, some easy and some hard, that can be taken by the insurance industry and government to achieve the goal of a sustainable and robust insurance system for the inevitable cyber-hurricane.

THERE ARE CONCRETE STEPS THAT WE CAN TAKE TO DEVELOP A SUSTAINABLE MODEL OF INTERNET SECURITY

A. What We Are Doing

The mantra of the Internet Security Alliance is that since the Internet is largely owned and operated by the private sector, it is up to the private sector to provide Internet security.

Consistent with that policy, the Internet Security Alliance has executed and supported a wide range of activities within the private sector to improve security.

INFORMATION SHARING

ISAlliance was founded in April 2004---5 months before the tragedy of 9/11 placed an increased emphasis on security because, even then, we realized the need for advanced information sharing. We established one of the first and most sophisticated information sharing operations in conjunction with our partners at Carnegie Mellon University's CERT/cc. This became the model used by DHS, which eventually took over that function from us with the creation of US-CERT.

BEST PRACTICE DEVELOPMENT

One of the under-reported stories of Internet security is that we actually know how to solve much of these problems. Best Practices in various areas of Internet security have been developed in the private sector and research has empirically demonstrated that these Best Practices work: though corporations, who follow them invariably still get attacked, they can better withstand and manage the attacks suffering little if any down time or financial loss.

ISAlliance has been a leader in the development of best practices, and has published a continuing series of works that communicate those best practices to the full range of large, small, and medium size enterprises.

Unfortunately, so far, only a minority of corporations follow these best practices.

WORKING WITH THE INSURANCE INDUSTRY

AIG insurance has, in conjunction with ISAlliance, attempted to stimulate wider adoption of these best practices by offering credits on cyber insurance for corporations who comply with them. Working closely with the ISAlliance technical team and Carnegie Mellon University, AIG developed the first cyber-insurance certification tool to be used in conjunction with ISAlliance's Best Practice Guides. This tool permits companies to show that they are meeting the standards of the Best Practice Guides and are entitled to insurance credits where permitted by law.

SMALL COMPANIES

In 2004 the private sector, in conjunction with DHS, held the first national Cyber Summit. The very first recommendation to come out of that summit was that something had to be done to bring more small companies into the perimeter of a secure cyber space.

The ISAlliance was asked to create a program specifically to address the needs of smaller companies. In the past two years we have developed a separate set of best practices for them, developed a self assessment tool to assess these needs, offered private incentives such as lower insurance rates for compliant companies and created an innovative mechanism for small companies to participate in our information sharing and educational programs. Since the cyber summit, the ISAlliance has increased its reach into the small company community by several hundred new companies.

REACHING OUT TO THE INVESTMENT COMMUNITY

Next month we, along with several coalition partners such as the Council on Competitiveness and BITS, will be holding a major event at NASDAQ. The purpose of that event is to reach out to the investment community who we believe have been undervaluing corporate investment in security and business resilience. Based on recent research we hope to convince the investment community that companies who do invest in business resiliency projects are indeed better investments. That is, companies that invest in cyber security are not dumping money in to economic black-hole. Rather, an investment in cyber security not only makes a company more resilient but also produces a positive return on investment. Clearly, if we can make this case strongly it would have a major impact on increasing the market incentive for improved security.

REVIEWING CORPORATE STRUCTURES

In addition, based on a series of recent studies, we believe that in many corporations there is insufficient integration among CSO's, CIO's and Risk Managers leading to less commitment from the COO, CEO and Boards of Directors for security and resiliency investments. As a result, we are engaged in a program to get this message out and achieve results in improved corporate governance.

ADDRESSING PARTNERSHIP AND OUT-SOURCING SECURITY ISSUES THROUGH MODEL CONTRACTS

Companies who participate in organizations like the Internet Security Alliance are often also among those "best practices" companies who are actually doing a very good job of assuring the security of their own cyber systems. However, with a shared infrastructure like the Internet you are only as secure as the company with whom you are interacting. Hence, we needed to develop a market system to expand the state-of-the-art procedures we follow to all our partners including those who are based off-shore. The mechanism we chose was commercial agreements recognizing that the agreement was an inherent part of setting up shared infrastructure. We developed a set of model contract terms and conditions which provide contract trading partners with a market mechanism that assures that both sides are following the necessary procedures to assure each other's compliance, while at the same time cutting legal costs.

Our work in this model contract project was endorsed by the Information Systems Security Association, an international professional association of over 10,000 information security professionals.

COORDINATING WITH RECOGNIZED STANDARD SETTING BODIES

As a next step within the Model Contracts Project, ISAlliance is collaborating with the American National Standard Institute (ANSI). We have agreed to work cooperatively to take the adopted standards for information security programs and develop contract language that embraces these standards. We are also hoping to broaden this effort to embrace international standards, and are working with internationally based partner corporations to incorporate legal requirements in other countries.

INTEGRATION OF MULTI-FACETED SECURITY ISSUES

It is a misnomer that cyber security is a technical problem. While it obviously has many technical aspects maintaining cyber security has technical, legal, business operational and public policy dimensions. Unfortunately, many organizations are ill-equipped to address these issues in an integrated fashion leading to uncoordinated and inefficient security programs. In cooperation with our partners at Carnegie Mellon University CyLab, ISAlliance is developing integration programs including legal/technical and business analysis coordinated with web-based education and training to improve our member's performance in their own management of cyber security as part of the business agenda.

ADDRESSING THE INSIDER THREAT

Many of the breakdowns in cyberspace (including the recent highly publicized personal security breeches on the part of agencies of the federal government) have been the function of personnel misconduct rather than technology failures. DHS Chief for Cyber Security research, Scott Borg, has reported that the single biggest vulnerability in industry is the lack of adherence of senior corporate personnel to cyber security policies and best practices. ISAlliance in conjunction with CMU and the US Secret Service has developed a separate set of best practices for addressing insider threats. This is coupled with web-based training which is also made available to Congressional and government personnel at no charge.

COOPERATION WITH INDUSTRY AND GOVERNMENT COALITIONS

The ISAlliance contributes both time and resources to support a range of voluntary industry and government coalitions such as the Information Technilogy Sector Specific Council, the Telecommunications Sector Specific Council, The National Cyber Security Partnership, and US-CERT.

B. What government Can Do

BACKGROUND

As I have already outlined, the private sector must take a leadership role in assuring the security of cyber space. Many organizations, including ISAlliance, its members, and the many coalition partners we have referred to above are doing a great deal.

But, the current level of effort is not enough.

Although research indicates that by following already identified best practices companies can make substantial progress toward mitigating the effect of cyber attacks. However, current research also suggests only about ¼ of corporations adhere to them.

The biggest obstacle is cost, weighed against perceived value.

The National Strategy to Secure Cyberspace, published almost exactly 4 years ago, correctly concluded that reliance upon government regulation in this domain was not the proper course of action. Given the ever changing nature of the Internet, it would be largely ineffective and most likely counter productive for American industry.

Yet, we have also maintained, since our comments filed in the development of that document, that there was a missing link in the strategy. While regulation would likely be ineffective, largely for the reasons detailed above, a pure voluntary program would also likely fail.

Although many have hopefully suggested that there would be a positive return on investment to cyber security spending, it has not so far been demonstrated effectively in most corporate board rooms.

Since the publication of the National Strategy, the ISAlliance has campaigned for the development of an incentive program to assure an effective and sustainable program of cyber infrastructure protection.

The road has been a long one, involving substantial dialogue and productive analysis of the alternatives available. Here are several notable activities to which the ISAlliance has contributed.

CISWG

In 2004, the then Chairman of the House Information Policy Subcommittee on Government Reform appointed a group of 45 industry executives to present a program that would take a deregulatory approach to cyber security. I was honored to serve as co-chair (along with ISAlliance COO Larry Clinton) of the Incentives Committee. We issued a series of fairly detailed reports covering issues such as best practices, educational outreach, and incentives.

WYE II

In 2005, the National Cyber Security Partnership engaged with DHS and 13 federal agencies in a series of off-site meetings built on DHS's own conference on cyber security held in December of 2004 at Wye River. The Wye II program also recommended an incentive program built on and extending the work done by CISWG.

NIPP and the SECTOR COORDINATING COUNCILS

In 2006, as part of the process in developing the National Infrastructure Protection Plan (NIPP), DHS requested that each sector form a Coordinating Council to help

provide input on and eventually implementation of the Sector Specific plans that are expected to grow out of the NIPP.

As with the CISWG reports and the WYE II reports, both the IT and Communications Sector Coordinating Councils provided almost identical comments to DHS suggesting that the NIPP include the need to develop a value proposition and market incentives to improve and sustain cyber security.

NIPP ESTABLISHES THE NATIONAL SECURITY LINK FOR ESTABLISHING A VALUE PROPOSITION FOR INDUSTRY INCLUDING INCENTIVES

The NIPP was published on June 30, 2006. It embraces the notion that as a matter of national security and homeland security a value proposition for industry must be developed including the creation of economic incentives.

"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)

ISAlliance wants to thank and congratulate DHS Assistant Secretary for Infrastructure Protection Bob Stephan and Acting Cyber Security Director Andy Purdy and their staff for making this paradigm shifting assessment and including it in the National Infrastructure Protection Plan.

NOW IT'S TIME FOR CONGRESS

It is now time to move from the general notion of recognizing the national security need to develop a value proposition for industry for improved security to the much harder question, "how exactly do we do it?"

The ISAlliance does not come to the Committee today with legislative language to be introduced. That is premature today, but it may not be in a few months. What we do come to you today is specific legislature ideas which, once agreed to, will then be translated into suggested legislative language.

Congress should continue the process you have started today and hold hearings on the various ideas we have identified for creating an incentive-based security model so that we can address the issue with the attention that the national security perspective suggests.

What I can provide for the members today is a fairly specific list of suggestions that have been developed through the CISWG, WYE II and NIPP comment processes I have discussed. In brief we can identify numerous paths, most with Congressional precedent for Congressional action to provide incentives that are in the national interest. These are all appropriate for adaptation and application in the cyber security space.

Among the alternatives we believe are appropriate for Congressional review are:

1. Congress can tie incentives such as civil liability safe harbors or procurement credits to companies who can demonstrate compliance with market generated best practices for cyber security. As I previously noted, research has demonstrated that a substantial minority of corporations currently follow industry generated cyber best practices which yield empirical success. The problem is motivating more companies to adopt these procedures. In the last Congress Chairman Putnam of the Information Policy Subcommittee of

Government Reform created the Corporate Information Security Working Group. The Incentives Committee of that group proposed a system though which this can be accomplished.

2. Congress can stimulate the stunted cyber insurance market. Cyber insurance can help achieve social goals by managing government risk in a cyber hurricane while providing a mechanism to maximize corporate security behavior that is dynamic enough to address the fast changing and international characteristics of cyberspace. This can be done by:
   a. Having government serve as an insurer of last resort to stimulate the market (Precedent: Terrorism Risk Insurance Act of 2002).
   b. Establish a revolving fund reinsurance system funded by taxes on insurance products (Precedent: Federal Aviation Act 1958).
   c. Requiring government contractors to purchase cyber insurance. (Precedent: Federal Acquisition Regulations)
   d. Promote cyber security information sharing allowing for the creation of better actuarial tables resulting in lower premium costs, increased competition and broader coverage. (Precedent The Year 2000 Information Readiness Disclosure Act of 1998)
3. The Congress can create an industry/government/university consortium to stimulate the needed research, development and adoption of security protocols. This will enable government, academia and industry to work together to replace today's security poor Internet protocols with security rich protocols. Congress followed a similar model (Sema-Tech) in the late 1980s to address the computer chip gap.
4. The Congress can use tax incentives to motivate corporations to adopt security practices beyond those already justified by their own corporate needs but conducive to the national and Homeland Security needs cited in the National Infrastructure Protection Plan (NIPP July 2006). (Precedent: IRS Code 26 U.S.C; IRS Code 26 U.S.C.832 (e); Energy Policy Act 2005).
5. The Government can create awards programs to highlight the contributions of corporations and senior executives who have gone beyond their own corporate interests and expended resources. In the 1980s when industry believed that "Quality" was a luxury they could not afford the federal government initiated the "Baldrige Awards" for quality which eventually became a sought after market differentiator for corporations.
6. The government can support private sector initiatives to use market forces to enhance cyber security. As noted, the ISAlliance, in conjunction with the ISSA and ANSI is developing a series of publications of model contract language that enable traditional and emerging standards of security within commercial agreements utilizing the market power of business alliances as a means to expand security. The ISAlliance in conjunction with BITS and the Council on Competitiveness is sponsoring a series of studies and forums educating the investment community as to the business benefits of security/resiliency and the corporate organizational reforms needed to expand this concept. All this is simultaneously in the public's national security interest. DHS, the Department of Commerce and other federal agencies should identify, promote and support these programs aggressively as a cost effective mechanism; doing so serves to expand their culture of security message.

I would like to thank the committee again for allowing ISAlliance to testify today and I would be happy to answer any questions the Committee may have.

MR. UPTON. Thank you all for your testimony. It seems as though we have our work cut out for us. I am glad that my Chairman is here, because that means if we do all the things that you explain, Mr. Clinton, that we would have jurisdiction over all the other committees, and I think we would welcome that here.

MR. CLINTON. Know your audience, Mr. Chairman.

MR. UPTON. Mr. Foresman, how long has this vacancy been in terms of the Assistant Secretary at DHS?

MR. FORESMAN. Mr. Chairman, as you know, Secretary Chertoff now announced last July the second stage review and the creation of the Preparedness Director and the creation of this new position that was officially established on October the 1st, so since that period of time.

MR. UPTON. So almost a year?

MR. FORESMAN. That is correct.

MR. UPTON. And I am pleased to hear that you are getting close. Is this a position that has to be confirmed by the Senate?

MR. FORESMAN. No, sir, it does not.

MR. UPTON. Good. That may be the best news we have this morning.

I would like, as you go back this morning, to just underscore the need to see that this position is filled as quickly as we can, so that we can, in fact, have a high profile leadership spot willing to tackle this and to be able to work with the other agencies that are out there.

Mr. Weafer, we appreciated your testimony. I would be very interested in the difference or the changes in the attacks from perhaps this year to previous years. You talked a little bit about a rapid response. Obviously, the impact of what would happen to the economy, but I am interested how these attacks change as particularly the private sector has prepared themselves for it. What has been the next stage? What has been the evolution?

MR. WEAFER. Well, the good news is we do believe a lot of people have listened to some of the best practices defense in depth, which is why some of the pandemic, the local events have died down. However, they have been replaced by a level of intensity in volume that we have not seen since a long time for us. We are seeing this driven by fraud, cyber crime, people trying to invade personal privacy. Largely, it is also driven by the use of broadband connectivity and home users, bringing work home, having data leakage from there.

MR. UPTON. Do a lot of these attacks originate from overseas?

MR. WEAFER. Actually, we find that most of the attacks originate within the U.S., attacking victims inside the U.S. Of course, cyber crime is very international. The people controlling those machines could be

sitting over in Europe or South America, or anywhere around the world. So it is a very international problem.

MR. UPTON. Mr. Powner, you indicated in your testimony, you said that the Internet recovery was by far incomplete. We had real threats. You painted a pretty bleak picture. Do you see that we are making some progress? What are the most critical things that we can do in the coming months?

MR. POWNER. Well, clearly there is some progress with some of the plans and working groups that are being put in place within the Department, but--and I think some of the panel members mentioned we need to move beyond plans and some of the initial stages.

One of the key things that we learned in our study for you, Mr. Chairman, is that what the private sector wants during a time of crisis isn't exactly where we are right now within the Department of Homeland Security with their planning efforts. They want items like what we learned in Katrina: help with logistics, help with prioritization, backup communications. Those types of things aren't being discussed. We are talking about these great large-scale plans, and we need to get together on the same page on this to have a plan that would be helpful to the private sector infrastructure owners.

MR. UPTON. I know that you studied the Business Roundtable report that was put out. Did you find that it helped you interface at all in terms of your report that you made?

MR. POWNER. The Business Roundtable report was very consistent with the number of findings that we had, and a number of those recommendations were quite consistent. We obviously weren't as critical as the private sector, because we couldn't look at that.

When you look at that report, and I think some of our panel members mentioned today, it is clear there is room for improvement on the private sector side of things also. There was one recommendation in that report, though, that talked about another group being formed. I think we need to stop forming groups and we need to hold the current groups accountable. We have enough groups that are looking at this. Let us just get some accountability here and get the job done.

MR. UPTON. That leads, actually, to my next question to Mr. Kurtz, who said we needed more of a role by the White House and others that try and take a leadership role. Now, Mr. Kurtz, I don't know all of your background, but I know that you once worked at the White House. Is that correct?

MR. KURTZ. Correct. In the early part of the first term of the Bush Administration, President Bush spent a great deal of time looking at putting together a national strategy to secure cyberspace. It came out in February '03. It is actually a good document. The problem is since that

strategy was issued in February of '03, we have actually been running in place. We--keep in mind--

MR. UPTON. Do you think that once an assistant secretary is named, that that will be a big help?

MR. KURTZ. I think it will help. One of the issues that I am trying to point out in the testimony is that DHS, under Homeland Security directive Presidential 7 and under the National Strategy, clearly have a lead coordinating role in putting together our national strategy to secure cyberspace. But what we need to understand is that while DHS has that leading role, there are multiple other agencies involved in this process, in particular, when we talk about an issue that is important to this committee when it comes to recovery and reconstitution issues. You know, agencies like the FCC have a role. Agencies like DOD have a role. The classic example is Hurricane Katrina. At the end of the day when the problems were so significant with Hurricane Katrina, the President ultimately turned to DOD for their assistance.

So what would happen in an event of a large-scale cyber disaster? What is the chain of command? Who is calling the shots? And at the end of the day, you may not have a situation where the Internet is, if you will, dark, that there is a blackout. In fact, I think that would be a pretty extreme case. But what you may have is a situation where you have very limited bandwidth or certain sectors cannot connect with each other. That means real decisions about priority need to be made. What traffic gets through? What traffic gets stopped? Likewise, can FedEx or UPS deliver their packages by the way--they base all their operations on the Internet.

A lot of these key questions require resolution, and that is why we are arguing for a national information assurance policy to put in place a directive across agencies, so we have a firm understanding of roles and responsibility and who is doing what in the event of a crisis.

MR. UPTON. My time is expired.

Mr. Gonzalez.

MR. GONZALEZ. Thank you very much, Mr. Chairman.

The first thing I want to do is read from Mr. Clinton's submitted written testimony. I don't think you covered it, Mr. Clinton, but I really liked it, and I think it tells the American people exactly what we are talking about. It says "First we need to realize that the Internet is unlike anything we have ever dealt with before. 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." It seems that what I am hearing is that we have got a piecemeal way of addressing

many of these different uses and such, and we really need something that is holistic. I just really enjoyed reading what is a very thoughtful written statement.

It appears that we are talking about a couple of things, of course. One is prevention. Obviously, we need to prevent the disruption of this incredible system that we have in the United States. The other thing is what do we do to respond once we have the disruption or the attack or whatever. And yet, we don't seem to be coordinated or getting a handle on what the problem really is. We haven't even figured out where the agencies--we are not even staffing them timely. It seems so overwhelming, and I don't mean to sound defeatist, but if we took the totality of your testimony today, we would have to admit that Congress is not really meeting its challenge effectively or timely. I am part of that Congress.

The first thing that comes to mind is the lack of cooperation between government and the private sector, more so on the private sector. In fact, I think Mr. Powner indicated that there is somewhat--I guess they guard jealously what they may sense is proprietary in nature, the edge, or whatever it is.

I want to break down the players in this scheme when we talk about the Internet. We have networks, AT&T, cable, and so on, right? We have ISPs, the Internet service providers, and we have the content aggregators, the search engines, the Googles. Everybody that goes out there--and this is all part of a communication system. It seems to me, Mr. Powner, that the private sector really is looking to the Government when there is disruption to make sure that it is minimal and will not interfere or interrupt or disrupt the doing of business, yet, they don't see that it is a two-way street, that they have to be making their contribution to make sure that we prevent and that we are able to respond. Am I correct in that particular assumption?

MR. POWNER. I think when you look at a potential large-scale disruption, it is very clear that we need to work collectively on it. So the private sector, the owners of the Internet components, telecom companies, the route server operators, all those folks clearly are in charge of recovery.

What can the Federal government do to assist? That is really the question, because the private sector is ultimately in charge. They know their equipment, they deal with minor disruptions on a daily, weekly basis. They know how to respond to things. But when it becomes at a certain scale, when does the Government get involved? That is unclear. What is their role on involvement? That is really what needs to be defined moving forward.

MR. GONZALEZ. The other thing that we touched on is, of course, the information security and the security of the systems themselves, and the fact that we have many in the private sector in users that don't take that into account at all. Again, Mr. Powner, I think you heard Mr. Clinton and others saying that--and I am going to go back, I guess, to Mr. Clinton's testimony, if I can find it quickly, about trying old methods in an environment that doesn't work anymore. A regulatory scheme, maybe, and I know that someone indicated that maybe this will be a conflict of philosophies. This is from Mr. Clinton's testimony. "We cannot manage what is essentially the 21st Century technology solely using regulatory models designed 2 centuries ago. A new, more creative model built on market incentives and creative solutions must be developed and added to the mix."

Mr. Powner, in your research and what you have done, do you agree that there has to be maybe a totally different way of approaching and getting these parties together and involved?

MR. POWNER. Mr. Gonzalez, that is an excellent point, looking at market incentives. I have been involved in critical infrastructure since the mid-'90s when Presidential Directive Decision 63 was initially signed, left the Government for a while, worked for a major telecommunications company, and since have come back. So I have been on both sides of the fence.

Frankly, we haven't been successful from the mid-'90s on having an approach to secure our critical infrastructures. We have had a lot of good starts. We have progressed certain ways. We have taken some steps backwards. But when you look at how we identify threats, whether we are working collectively in public/private partnerships, we have had mixed success dating back to the mid-'90s. So I think looking at some new approaches, I think that we ought to keep our eyes open and consider those ideas.

MR. GONZALEZ. Okay. I sure do thank you, and my time is up.

MR. UPTON. Mr. Shimkus.

MR. SHIMKUS. Thank you, Mr. Chairman. A great debate, great hearing, an important one, as you all have noted.

In listening and trying to get a handle on where we are at and where we need to go, I am struck by this whole debate on who is supposed to do what, when, where, and how, and that is what we are trying to get focused. Hopefully getting an assistant secretary will at least bring some coordination and focus and leadership. It is really all a definition of leadership and getting people to move and setting the tone and going forward.

The private sector has a--especially those who are highly invested in data issues--I mean, they have a compelling financial reason to secure

their data and to harden it. Isn't that correct? Anyone want to--let us start with Mr. Kurtz, and then we will go to Mr. Clinton.

MR. KURTZ. Yeah, I would agree, and this goes back to the point that Mr. Gonzalez said. I would actually disagree with you in part about where the private sector is on this. I can answer both at the same time.

The private sector, over the past several years, and Larry can add to this as well, over a decade, at least, has spent a great deal of time working to try to protect the critical infrastructure and working to shore up the critical information infrastructure in large part, for their own reasons. The energy and oil has to flow through the pipelines, over the power lines. The banking systems need to work; the health systems need to work. They all need to do that for their own reasons, and I think in fact a great deal of progress has been made along the way. I would also note that there are several organizations, the National Cybersecurity Partnership, organizations that have been set up at the behalf of the Department of Homeland Security, like the IT Sector Coordination Council, that have been stood up to address issues with regard to cybersecurity.

We are, if you will, Larry and I are a piece of a much larger set of people, both in Washington and across the country, that are working on IT security issues on behalf of the private sector. I think the key issue that we are at today, if I may, is looking for more government leadership to work with the private sector to solve some of those key questions that I outlined in my testimony. What happens when the balloon goes up? What happens when we really have a problem? The private sector, for its own part, wants and needs to ensure the critical information infrastructure, but there will be problems, so what happens when that happens? Who is in charge, who is supposed to do what? That is what we are looking for.

MR. SHIMKUS. Thank you.

Let me stop you. I am going to interject, and then I am going to allow Mr. Clinton to respond also, because for us, large versus small, what do you define? What is large breach, and then if--based upon testimony, if there is--the other question I am going to throw out eventually will be do you believe that whatever is defined as a large disruption, will all communications go dark, or will there be a reduced bandwidth? And if there is a reduced bandwidth, then I agree definitely that there needs to be some--in fact, we already do it. I pulled out of my wallet this Government Emergency Telecommunications Service little phone--fortunately, I have never had to use it, and sometimes I forget it is even here, but someone is going to allow me in a degraded environment for telecommunications, if I have to call back to

Washington then I hopefully will get some expedited service because of this.

So we are already doing this at the national level in one arena of communications. So really, the debate is bandwidth, what the prioritization or what would go through and how it would go through.

Mr. Clinton, why don't you add, subtract, or delete.

MR. CLINTON. Maybe I can just extend.

MR. SHIMKUS. Good.

MR. CLINTON. First of all, let me thank Mr. Gonzalez and refer partly to, Mr. Shimkus, with respect to a point that Paul made that I, too, think that probably the record for the private sector, in the instance of a major disruption, is actually very good, including the sharing of information and bypassing some of the concerns that they would have on a normal instance. I think it is real important that we segment the problem here. You have the concern about the major, the big one, the Hurricane Katrina, and then you have the hurricanes of all the other sorts that we also face every day. So it is two different things.

With respect to the big one, people--just like they did on 9/11, bypassed their normal concerns. They just get in and they do what they need to do, and that has been the case. But you are correct sir, Mr. Shimkus, that what we need is a unifying motivator to get people to do the right thing all the time so that when the big one hits--if I can use the Chairman's metaphor a little bit, the levees are higher already. And what we are arguing for is that sort of resilience needs to be put into the system, and frankly, the private sector, just like the Federal government, and perhaps even the Congress, needs to readjust because we are dealing with something very, very different.

You are right. There is a compelling interest for companies to defend their systems, but frankly, the research indicates that corporations are not currently valuing that responsibility as highly as they probably should.

We are having a big event next month, up at NASDAQ, where we are going out to the investment community and saying you guys are not properly valuing the investments on security and resiliency that the companies are making, so you are providing a disincentive to do this. So we have to find a way to get the market incentive moving so that the levees are built and people better appreciate that. If we can do that, when the big one hits we won't have to worry about bypassing our normal concerns and sharing information we would otherwise normally--would be in position. So that is what we need to do, and that is going to require reorganization at DHS, the White House, in corporate America--and we can go into that in greater detail if you like, and perhaps even in the Congress, because it is difficult to deal with you guys.

MR. SHIMKUS. I got elected in 1996, took office in '97. We had this big disaster coming in the future, which now seems pretty minimal, which was Y2K. There was a financial aspect of the private sector to get their act in order so that come the change over of the clock that there wouldn't be--how many people on December 31, 1999, as they welcomed in the new year, were kind of looking at the lights to see if the lights would continue to be on?

And so it is good to have leadership, is it good that we fill this position so that we can have communication. We started talking about how you prioritize, and we appreciate your testimony. Hopefully, this will lead us forward in ensuring that we are ready to define minor versus major and that--we know we live in a dangerous world, and we just have to do--we don't want to be sitting on the sidelines and say we didn't act.

So thank you, Mr. Chairman. My time is expired.

MR. UPTON. Ms. Eshoo.

MS. ESHOO. Thank you, Mr. Chairman, for holding this important hearing on an issue that I think has really, for the most part, been overlooked. It is too important to overlook. As a member of the House Intelligence Committee, I take very seriously the range of threats to our country, from terrorists and other enemies, including threats to our basic infrastructure, which includes our telecommunications network and the Internet. If you spend any time with the NSA, you know that this is not only the most valued of infrastructures, but how it serves our national security. So this hearing is really important, not only to identify how we can cooperate with one another, but also really to put, I think, the Administration's feet to the fire on this, in plain English.

We have gone without a cybersecurity czar for far too long. I heard some testimony that an application and its approval is in the works, but make no mistake about it--to have gone this long without any attention to this and without having someone direct this part of the orchestra, I think is dangerous for our country, in plain English. I am not one to try to hype up fear and all of that, but simply put, we have placed ourselves in a real ditch here by not having the Administration name someone.

I remember when Richard Clark, former cybersecurity czar, described the potential for a telecom disaster as an electronic Pearl Harbor. And whether he is there or not, I think his words should be taken seriously here.

So I have a couple questions. Why has it taken so long to fill this position?

MR. FORESMAN. Congresswoman, let me make two points first. This is not--

MS. ESHOO. I mean, there hasn't even been a permanent director, so this is just like having erased something very important on the blackboard. We are just operating without--

MR. FORESMAN. Congresswoman--

MS. ESHOO. --anyone there.

MR. FORESMAN. --I would strenuously object to that characterization.

MS. ESHOO. Well, who has been in charge?

MR. FORESMAN. I have been in charge since January.

MS. ESHOO. January of this year?

MR. FORESMAN. January of this year. And let me offer that the success or failure of efforts in the Nation's cybersecurity efforts does not rest with one position in one agency or organization.

When you look at the challenge that we have gone through, and I am sure you are aware, Congresswoman, that to get an--

MS. ESHOO. Do you wear any other hat, or you are full-time as cybersecurity czar?

MR. FORESMAN. Congresswoman, as I think you know, I am the Under Secretary of Preparedness. I have a number of areas of responsibility, of which cybersecurity is--

MS. ESHOO. What percentage of your time do you spend on cybersecurity?

MR. FORESMAN. Approximately 25 percent of my personal time, and I have a deputy who is assigned to it 75 percent of his time.

MS. ESHOO. And who is that deputy, is he or she here?

MR. FORESMAN. No, ma'am, but I will make the point that Andy Purdy, who has been our Acting Director of the National Cybersecurity Division, Andy has done an exceptional job and Congresswoman, I understand the importance of getting this position filled, but I want to be very clear with you. This was the number one personnel priority that I had on my plate when I walked into this position. We have been through numerous candidates, Congresswoman, and we have had a wide variety of candidates who, for a variety of reasons, have not made it through the process. We have had a number who started into the process and decided that the vestiture of their businesses, many of them were owners of firms in the IP community--

MS. ESHOO. Does that fit with other timelines in terms of hiring people?

MR. FORESMAN. It doesn't, and I think it points to the unique nature, just as all of the panelists have talked about, with dealing with IT issues. The sector is unique--

MS. ESHOO. I want to get to another point, and I have 33 seconds to do that.

Given the many vulnerabilities which exist as a result of users and businesses with inadequate security or vulnerable networks, what are you identifying that should establish an environment where users and the private sector do what is appropriate to really fill this gap to protect our telecommunications infrastructure? That is what we are here for. We need to identify that. I am still not pleased with your answer. I mean, if, in fact, we are on this big search for a cybersecurity czar and you are saying that you have spent 25 percent of your time, we have someone that is really able that spends 75 percent of their time, but they are not even here to testify about it, that says to me that we have a problem. You may not agree, but I think that we do.

So given the responsibility that you say is 100 percent covered, where is the plan to pull industry, businesses, private sector, and the Government together? Because as far as I can see, we don't have a plan, and that is equally as disturbing.

MR. FORESMAN. Congresswoman, no, we have action. We have a Sector Coordinating Council that is working across the IT sector to--

MS. ESHOO. We don't have any standards or anything that has been pulled together. We heard that in testimony here today.

MR. FORESMAN. Absolutely, Congresswoman, and that is why we have this group working to develop those standards. This is not something the Federal government is going to mandate on industry. I think you heard all of the panelists from the private sector note that, and we are providing the leadership to get the players in the room to have the discussion to adopt the best practices.

MS. ESHOO. I think that we can lead in this area. I think that we have to lead, and you know, you used the word mandate. I think that we can create something where people buy into it without forcing something on them. But I think unless we do take a leadership position, it is not going to happen.

Mr. Clinton, you wanted to say something?

MR. CLINTON. Yeah. Congresswoman, what I wanted to try to do is offer an example of where we are working together. Under the National Infrastructure Protection Plan, there is a requirement for each individual sector to prepare its own infrastructure protection plan, and I happen to be working on the IT sector-specific plan, working in partnership with some of the folks at the Department of Homeland Security. We are making progress and we are seeking to make that, if you will, a joint plan. In other words--

MS. ESHOO. Who has bought into it?

MR. CLINTON. Right now, it is very much at the working level. In other words, we have individuals within the private sector who are working on that plan in draft form. We are working with our

counterparts at DHS. Now, if I were to offer some criticism here, and I think I have to, I wish there were more senior level involvement in the preparation of that plan, not only DHS, frankly, but other agencies as well, because there are critical policy questions that need to be addressed.

But I don't want to leave the impression that nothing is happening between the private sector and the Department of Homeland Security and other agencies. There are things happening. It is more leadership and attention to the problem that would be very useful and critical.

MR. UPTON. The gentlelady's time is expired.

MS. ESHOO. Can I have Mr. Clinton give an answer to the committee? I think he wanted--

MR. UPTON. Very briefly.

MR. CLINTON. Well, very briefly, I worked with Paul on the infrastructure protection plan, the sector-specific plan, and we are working very hard. I am very hopeful about that.

The comment that I wanted to make, however, dealt with the issue of whether or not we don't have any standards. That is--I would beg to differ. I don't think that is actually--we have got a whole lot of stuff already out there: the NRIC standards, the best practices are really good. The ANSI has just come up with a new set of standards. The private sector is well along. As I documented in my testimony, companies that follow these things are really doing a pretty good job. If we could get everybody to do this, and there we need motivation. Some of this we can do on the private sector side. We have a program to establish model contract language so that the good actors, when they engage in contracts with the others, will put into their contract that you have to comply with these ANSI standards, for example. So there is a whole lot of creative stuff that we can do.

We have to do a whole lot more on our side, absolutely, and so does DHS, but we also are really trying to establish an environment of working together. That is something that is tough but we are working on it.

MS. ESHOO. Thank you.

MR. UPTON. Mr. Stearns.

MR. STEARNS. Thank you, Mr. Chairman.

Under Secretary Foresman, let me just sort of follow up a little bit. Ms. Eshoo had been talking about the Department of Homeland Security sponsored exercises such as a cyber storm. Have you found that both the Government and the private industry are unprepared to respond to a major Internet disruption? Can you specifically tell us how bad the situation and what is being done to fix it?

MR. MORAN. Congressman, it is difficult to put a quantifiable measure on where we are, but let me offer a couple--

MR. STEARNS. Don't give me vague and general.

MR. MORAN. I am not going to give you vague and general answers.

As a number of the panelists have said, we have got to have a clear appreciation of the roles and responsibilities of the private sector versus the Department of Homeland Security, and that was identified. And as we go through the update of the National Response Plan, we will do those clarifications.

MR. STEARNS. Well, on a 1 through 10 scale, it says here that you found that both government and private industries are unprepared to respond. Ten being they are very prepared, and 1 being they are not prepared. On a 1 through 10 scale, how unprepared are they to respond to a major Internet disruption?

MR. MORAN. Congressman, with all due respect, I am not going to put a measure on it because it would be unfair to the industry, it would be unfair to government to put a scope or a scale on here when as we have evolved through the development of our infrastructure protection efforts in this Nation, whether you are talking about--

MR. STEARNS. I don't want you to--just give me general language. I would like to get--since the report said government and private industry are unprepared, are they very unprepared or not prepared? In your opinion, how bad are they unprepared? Is this significant?

MR. MORAN. Congressman, let me leave it at this. I would offer that we are moderately well-prepared, and there is more work to be done.

MR. STEARNS. And what should be done to fix it?

MR. MORAN. Well, Congressman, clearly the big thing is there is a wide range of ongoing discussions, planning activities, the exercise activities, the training activities, but I think one of the critical things that Larry Clinton raised in his testimony is that there are a number of policy issues that need to be addressed so that we drive this from a market incentive standpoint. There are certain areas of the critical infrastructure where regulation is appropriate--

MR. STEARNS. Okay.

MR. MORAN. --there are others--

MR. STEARNS. I will just move from there.

Mr. Powner, how would legislative changes improve the ability of the Department of Homeland Security to develop Internet recovery plans? This is your chance to tee off and give the straight scoop here that--

MR. POWNER. I think that two areas could move the ball forward in a large way. Hopefully with the assistant secretary position being filled soon, that there will be greater clarity between the roles between the

National Communication System and the National Cybersecurity Division. Right now, those roles and responsibilities--

MR. STEARNS. So you would want legislative overlap language for that?

MR. POWNER. Well, the question is if they can't figure it out soon, perhaps you could help them.

MR. STEARNS. Okay.

MR. POWNER. Okay? So I think that is the first one.

MR. STEARNS. That is a nice way to put it.

MR. POWNER. So that is the first point. The second point is when you look at the Stafford Act and the lessons learned from Katrina, there were private companies that needed assistance, and they were denied. When we have a major disaster, that should not be the case. We ought to have waivers around some of those things during national emergencies where private companies can be assisted by the Federal government.

MR. STEARNS. Mr. Clinton, what percentage of the United States companies are simply implementing best practices when it comes to protecting the IT infrastructure?

MR. CLINTON. Well, the last part makes it a little bit tougher for me, because the statistic I was just going to quote you goes beyond just the IT infrastructure. Well, the answer I would give you, sir, is that the research that I have seen, which is done by PricewaterhouseCoopers, indicates about 25 percent of corporations are currently following what we would identify as best practices.

MR. STEARNS. So 80 percent, then, are not doing it?

MR. CLINTON. In various degrees, yes, it is about 80 percent.

MR. STEARNS. And is there--within that 80 percent, can you break out in terms of groups? Can you be more specific who those 80 percent are?

MR. CLINTON. Yes, although the degree to which I can do it off the top of my head is--

MR. STEARNS. I don't want to put you to too much trouble. If you could name a couple names that would be helpful.

MR. CLINTON. Well frankly, Mr. Stearns, probably most of the companies that appear before this subcommittee are probably doing a pretty good job. I mean, the major providers, et cetera. It is when we get particularly into the small business environment it becomes really--

MR. STEARNS. But 80 percent is a pretty big number, so is it possible you could give me some examples who are in that 80 percent categories?

MR. CLINTON. Well, we have a major problem with small business overall.

The first recommendation that came out of the National Cybersecurity Summit, which was held a couple years ago, was to reach out to small businesses and--

MR. STEARNS. Under 5 million, under 100 million, what--

MR. CLINTON. Under 50 million is--

MR. STEARNS. Under 250, so that is a lot of companies.

MR. CLINTON. That is a lot of companies, sir. And we did research on that to figure out why was this going on, and to really cut to the chase, we found that all the small companies that we dealt with, series of focus groups held nationwide, had one thing in common. Every small company wanted one thing: to become a big company. And so the economic difficulties, the costs involved, were really the major barriers. So what we have attempted to do is develop a cost efficient way to deliver services to these companies, and we have expanded our reach by several hundred.

So there are efforts that need to be made here. We need more best practices; we have to refine the best practices that are previously established so that they are more applicable to the small companies. They have different needs than larger companies. We have to find ways that we can fund a delivery system that would be far more cost effective for them, develop assessment tools, all of which we have done. So we are doing outreach, but sir, I am absolutely with you. My testimony says a lot more needs to be done. We have to find incentives to get these people more into the boat, and we would love to work with you on that.

MR. STEARNS. Thank you, Mr. Chairman.

MR. UPTON. Mr. Inslee.

MR. INSLEE. Thank you. There is a lot to be concerned about here, and I want to ask some of you gentlemen about excuses for inaction.

We have this blatant failure to have leadership for not filling the Assistant Secretary of Cybersecurity post at DHS. The GAO has found that that has retarded any significant advances on cybersecurity. That is on the Administration's side.

On the Congress's side, the House has failed to pass two meaningful pieces of legislation, the Data Accountability and Trust Act, H.R. 4127. We passed that unanimously on our committee on March 29, 2006. This is supposed to be the big security month in the House, but as far as we know, it is not scheduled for House action. That, of course, would set national standards on how to handle data brokers handle personal information. That hasn't passed. The Provincia Fraudulent Access to Phone Records Act, H.R. 4943, that passed unanimously--I'm not sure it was unanimously—out of this committee on March 16, 2006. That hasn't passed the House of Representatives yet.

So we have supposedly the big security month in the Republican Administration, Republican House. We don't have a leadership post for cybersecurity for the Nation. It has been empty for a year. We have two major bills, one involving pretext calling--by the way, we know this is not an abstract problem. We see at Hewlett Packard the situation where somebody in management basically hired a firm to do pretext calling to violate the privacy rights of the Board members of this corporation to get their phone records. This is going on in the major board rooms of a major Fortune 500 company. This is not an abstract problem. It is happening. And yet, we don't have the House passing either one of these bills to date. I think that is a concern.

So I guess I will ask Mr. Foresman, is there any excuse for either of these failures?

MR. FORESMAN. Congressman, let me first say with regard to what Congress has or has not done. I am not in a position to exercise any level of judgment on that. On the second piece with regard to the cybersecurity post, I would offer to you progress has been made. The absence of an individual in that particular post has not stopped us from moving forward. Earlier, I had talked about the fact that we had a very collaborative relationship with Microsoft just a couple of weeks ago to deal with the vulnerability issue.

So if it were the fact that we had a difficult time finding a candidate to fill this position had we been in neutral the entire time, I think there would be grave concern, but I think we have been in overdrive the entire time, and as all the individuals have said here today, we need to keep the pedal to the metal and continue our efforts forward.

MR. INSLEE. Well, it is great on a ship that the people in the boiler room are doing a good job and the navigator is doing as good a job that he can, without a captain you just don't get the motivation to move an agency. And sitting here, I don't think there is any excuse for that. I don't think there is any excuse for us not passing these two bills, either, that are consensus products.

So I think constituents of any party ought to be dissatisfied with both the Administration and the House today, and I would hope this hearing, which I am glad we are having, I thank the Chair for having this hearing, will motivate all parties to move with the dispatch to get these jobs done.

Thank you.

MR. UPTON. Mr. Walden.

MR. WALDEN. Thank you very much, Mr. Chairman. I appreciation the work of the GAO to give us some guidance, and the testimony of our panelists today.

I want to ask the gentleman from Symantec, is it Weafer?

MR. WEAFER. Weafer.

MR. WALDEN. Weafer. What sort of changes have you seen in the cyber threats over the last couple of years? I mean, we are all subject to them. I get this garbage on my Blackberry, at home and everywhere else, and I realize that is junk mail, but in terms of the threat, what are you seeing?

MR. WEAFER. Well, I think we have seen a very big change from the late '90s, which are very much driven by the teenagers, the cyber vandals, the attention, today are very much driven by criminalization and commercialization.

The criminalization are the ones we have talked about, the phishers, the spammers, the people that are out there. The commercialization is people like adware companies, bad actors, the people who are trying to exploit vulnerabilities, take over websites. They are trying to get sludge onto your machine. So it is the intensity in volume and the absence of high profile events is something of concern to us in terms of creating awareness for users.

We hear this from home users, we hear this from CEOs of companies, which is the problem has been solved because I don't see it on the news anymore, and we are seeing the opposite. We are seeing the intensity of the volumes actually increase over the last couple of years.

MR. INSLEE. And as you see that intensity increase, what sort of damage are you seeing to these systems?

MR. WEAFER. Well, today it is very focused on loss of confidential, personal information: Social Security numbers, personal information stolen from data leakage from corporations. That seems to be where most of the money is concentrated on. That is where most of the attacks are. Certainly, there is a lot of concern about critical infrastructure, not just on today's technology, but as we move into the next generation technologies like smart phones, mobile technologies, there is a lot of concern going forward about how prepared are we with those technologies, which is why one of the recommendations is certainly R&D into some of these new technologies to secure them.

MR. INSLEE. And as you look at what is coming out of the Federal government, I mean, we have heard a lot about the lack of an appointment to the head of this Department and all, how important is that?

MR. WEAFER. We think it is critical. I think, to echo many of the comments made here today, which is we have identified many of the policies, we have identified some of the key players, we just need to implement and get many of these ideas moving.

MR. INSLEE. All right.

Mr. Moran, what kind of security issues should we take into consideration as we migrate from sort of the traditional phone service to Internet-based services and communications?

MR. MORAN. Well, the newer systems, the new Internet-based systems, they are much more open systems. The old systems were closed systems where you had trusted a few people, trusted people, you knew them. They were the ones that had access to like the signaling operations so the networks were easier to maintain the integrity of the networks. The new systems are much more open. The channels that handle the data are the same channels that handle the controls in many cases. This produces a lot of challenges, and it means that anyone who is a part of the system, if they want to maintain secure systems, they have to take a lot of steps to make sure that they are not being sloppy with how their networks are and whether--not being sloppy, but people into those systems that shouldn't be in.

Through the NRIC process, we posed some of those questions to NRIC and we have gotten a number of best practices on how to be more secure in those things to make sure that your system will not be so vulnerable.

MR. INSLEE. All right.

Mr. Kurtz, I guess one of the issues that has always intrigued and yet troubled me with how we deal with the Internet is its international scope. We can have people in place and policies coming out of the United States government. How do you control it when a lot of this stuff is offshore? What do you recommend? How do we get at that issue?

MR. KURTZ. Well, there is an important milestone just passed before the summer recess when the Senate ratified the Council of Europe's Convention on Cyber Crime, which puts in place that common infrastructure for investigating and prosecuting cyber criminals. That was a very important step.

The next step now is to, if you will, take the show on the road and ensure that other countries around the world adopt that same convention, put in place the laws in order to investigate and prosecute cyber criminals. It also requires the United States to reach out, in particular, to key allies and friends, to develop relationships about relating to infrastructure protection, information infrastructure protection. In other words, if we have a major problem in Europe or in Asia with regard to a critical data link or multiple links at the same time, we are obviously going to need to know who is who on the other side so we can have those kind of relationships in place, getting into a broader exercise environment.

I will note that Cyber Storm, if you will, was international in nature. They had some other countries participating, but we need to broaden that scope.

MR. INSLEE. But doesn't it just take one outlier, I mean, one safe harbor, if you will, from international law where they can drive it all through servers and--

MR. KURTZ. Well, it depends on ultimately what you want to do at the end of the day. If you are, in fact, talking about cyber crime, yes, if you want to have somebody who wants to go after people's sensitive personal information, it can be just one outlier. But if you are talking about a concerted cyber attack, that takes more resources, more planning capabilities on the outside and on the inside, in other words, an insider threat capability as well. It takes a little bit more, but it is very difficult with the Internet because I can, if you will, spoof that I am sitting in China or I am sitting in Iran, when I am really somewhere in Iowa. It makes it difficult.

MR. UPTON. Mrs. Blackburn.

MRS. BLACKBURN. Thank you, Mr. Chairman. I thank all of you for being with us today and bringing the information that you have. Listening to you, I tell you, we have--in this committee and in Oversight and Investigations, we have talked quite a bit about looking at the new economy, the electronic commerce needs for drawing some bright lines distinguishing what is large businesses and small businesses. Mr. Kurtz, listening to you it sounds like there again that needs to be a consideration, how we deal with the businesses and the type of business that it is, and then looking into folding that into the laws in the government and their responsibility.

Secretary Foresman, let me come to you first. We talked a lot about what is not done. I have looked at your testimony, and you lay out broad platitudes and goals that are there, and I will tell you quite frankly, reading it, it reminded me a little bit about the hearing that we did in New Orleans post-Katrina on the implosion of healthcare. And as we talked with them about what their emergency preparedness was, we found out that they had a strategy, a plan on paper. What they did not ever do was put in place an implementation plan. So sometimes, we can look at goals, we can look at what a vision is, but that is not going to get things in place to deal with recovery of information or putting a cyber structure back in place, should we have an attack.

So for the record, why don't you articulate the steps that you all have taken, the things that you do have in process.

MR. FORESMAN. Congresswoman, what I propose is to bring back a comprehensive list of those things and how they fit together in terms of implementers, but I am 110 percent with you. The Secretary and I have

talked in the context of cybersecurity. The necessity of first defining the goals and doing that in collaboration with industry in a way that balances security and the national economy--

MRS. BLACKBURN. Okay. If I may interrupt you--

MR. FORESMAN. And then, Congresswoman, if I just might say, we are going to put tangible timelines on all of these things as we move forward. As you saw in the testimony, we are updating the National Response Plan. The sector plan is due by December 31 at the latest, earlier if possible. We are just not going to simply throw them out there without specific deliverable timelines.

MRS. BLACKBURN. So you can give this committee assurance that there are some tangible items that you all--some milestones that you have reached, some things that you have in place that we can point to, and when our constituents say, you know, post-Katrina, there was not communication in Southern Mississippi. What are you looking at if we have a disaster that takes down everything again? You can say when it comes to Internet and to our cyber infrastructure, we have some deliverables that have been reached and we can document that and show you.

MR. FORESMAN. Congresswoman, we will bring that and document it and provide it to you.

MRS. BLACKBURN. Okay, thank you. I appreciate that.

Mr. Kurtz, back to some of your comments, and kind of taking up where Mr. Walden had left off, do you think that the Federal government is capable of putting in place a recovery structure? Do you think that this is something that needs to be done by the private sector and the stakeholders necessarily for helping put that in place for the government? Do you think government has the ability to move quickly enough to address it?

MR. KURTZ. I certainly think the Government has the ability to lead those efforts. If I can go back to the 1980s and 1990s when the national communication system was set up with a divestiture of AT&T, a group of companies came together, the telecom firms came together to work with DOD and the rest of the interagency on telecom issues. If you will, the Government built the field and they all came. I think we really can do the same thing with this situation as well.

MRS. BLACKBURN. Okay.

MR. KURTZ. We can expand the pool to include the IT infrastructure folks, and as well as other key infrastructure providers, the finance and energy folks as well.

I do think it is doable. It is really leadership and sorting out roles and responsibilities in the event of a crisis that is important.

MRS. BLACKBURN. Okay. Mr. Moran, you mentioned the 200 best practices in your testimony that your work had led to, over 200 best practices. So what do you do with that list? Are you actively communicating that or do--

MR. MORAN. Yes, the best practices have been developed. They are actually posted on the NRIC website. But we have an outreach program. We get out to parties who we think need to hear the message. The ones who were involved in NRIC development, they obviously know them, they voted on them, they know what they are. They are very attuned to it. But for example, we get out to--a lot of the FCC focus is on the telecom networks, so one of the things we do, we try to get out to the State telephone associations and we get out and make some presentations about the best practices, why they are important. We try to make the point, by the way, that there are costs to implement best practices, but the risks and the costs of not implementing the best practices and having networks go down, lost revenues among other things, we try to point out that there is a lot of risk and a lot of costs associated with not implementing best practices.

So we get out there. We also get out at national conventions and conferences to get the word out on the best practices. So we think it is extremely important for everyone to know about them who the best practices would be relevant to, and we try to make that happen.

MRS. BLACKBURN. And I would assume that post-Katrina you have some lessons learned that are also included in that?

MR. MORAN. Absolutely, yes.

MRS. BLACKBURN. Thank you, Mr. Chairman.

MR. UPTON. Thank you.

Mr. Gonzalez.

MR. GONZALEZ. Thank you very much, Mr. Chairman, to indulge me this last question. I just didn't want to leave this untreated, because I think we touched on it, but to make sure that we are comprehensive.

We have touched on the role of the major player, of course, government, and then the major players in the Internet, and I think we have identified those as the individuals that come--representatives that testified before our committee, Mr. Chairman. We barely touched on the other, though, and that is going to be small business and consumer. And so this question is more directed to Mr. Weafer, right? Mr. Weafer, your testimony cites a study by the Small Business Technology Institute, small business information security readiness, and I quote "Shockingly, this study found that over 74 percent of small businesses perform no information security planning whatsoever." That is the first point. Now, let us get into the consumer, and I think small business more consumer than anything else. "The growing use of always on broadband

connections by home users and small businesses represents a significant amount of computing power, which left unprotected can be taken over and used as zombie machines to damage our networks and hinder the commerce and services that flow through them."

So on those two points, where are we today in addressing those particular groups that are essential, obviously, if it is going to be comprehensive, and again, what should we be doing if, in fact, you disagree with the progress that we are making at the present time?

MR. WEAFER. Well, I think just a couple of things you need to do. One is increasing awareness and education, particularly for the home user level. I think it is a danger for the home users that they think that the problem is solved through one magic pill. That is not the case. As we have moved from dial-up connections to broadband connections, we have opened up our computers to not only more pressing power, but more threats coming in: network attacks, phishing attacks, spam attacks. I think in many cases people are unaware of the dangers they are opening up.

Every country we look at and we log go, to broadband, we see a complimentary increase in the number of cyber attacks originating from within that country. So it is not just a U.S. concept, we actually see it around the world.

So getting people to understand it is a defense in depth, getting them to understand it is about updating security patches, best practices, social awareness in terms of what parts of the Internet--don't go down the dark alleys of the Internet, what they are downloading on the machine, reading the user agreements, these are part of the education awareness.

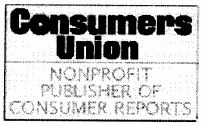
Secondly, the infrastructure itself, we need to make sure we are protecting them as much as we can. Some of this can be done at the telecommunications or the ISP layer, which is protecting them from spam, viruses, and things coming down that pipe towards them. We do recognize a special place the home users have, because, of course, many of us are also remote workers. So if we bring home our work, we are also exposing our company's data as part of this. So this is another reason why we really need to focus on this group and try to get them the incentive as well as the awareness to try and improve security.

MR. UPTON. Thank you, Mr. Gonzalez.

Well, this concludes our hearing. We appreciate your thoughtful remarks and your testimony, as well as in your statements. I must tell you that this subcommittee is going to stay on top of this issue. Mr. Foresman, again, if you could take that message back that we are looking forward to working with an assistant secretary, as we know that this is a potential real problem that will cause just enormous damages if it is not dealt with correctly.

Thank you and have a good day.
[Whereupon, at 11:58 a.m., the subcommittee was adjourned.]

SUBMISSION FOR THE RECORD OF JEANNINE KENNEY, SENIOR POLICY ANALYST, CONSUMERS UNION



September 12, 2006

The Honorable Fred Upton
Subcommittee on Telecommunications
and the Internet
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Edward Markey
Subcommittee on Telecommunications
and the Internet
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Representatives Upton and Markey:

Consumers Union applauds the Subcommittee's ongoing interest in the important issue of cybersecurity.

For your consideration during the Sept. 13 hearing and subsequent subcommittee action on this issue, attached is "CyberInsecurity: Viruses, Spam, Spyware — You're More Vulnerable Than You Think," published in the September 2006 issue of *Consumer Reports.*® The article highlights the findings of Consumers Union's investigation into the scope, costs and threat of cyberassaults on consumers. It includes the results of our annual "State of the Net" survey of online activity and threats.

As our investigation notes, consumers spent $7.8 billion during the past two years for computer repairs, parts and replacements due to failures in cybersecurity. We urge the subcommittee to take additional action to stem the threat of viruses, spyware and spam to consumers in order to reduce the significant costs that failed security imposes on both consumers and our economy.

Among the additional policy solutions the committee may wish to consider are expanded consumer information and education efforts, as well as additional resources and expanded authority for enforcement agencies, including steps to address the significant barriers to cross-border efforts to combat illegal cyberactivity.

Among the findings of our investigation are:

- Consumers spent $7.8 billion over the last two years for computer repairs, parts and replacement as a result of viruses and spyware;
- A consumer's odds of becoming a victim of from cybersecurity failures are one in three;

Consumers Union Headquarters Office
101 Truman Avenue
Yonkers, New York 10703-1057
(914) 378-2029
(914) 378-2992 (fax)

Washington Office
1666 Connecticut Avenue, NW
Washington, DC 20009-1039
(202) 462-6262 Suite 310
(202) 265-9548 (fax)

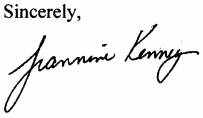
West Coast Regional Office
1535 Mission Street
San Francisco, CA 94103-2512
(415) 461-6747
(415) 431-0906 (fax)

South West Regional Office
1300 Guadalupe, Suite 100
Austin, TX 78701-1643
(512) 477-4431
(512) 477-8934 (fax)

- Nearly one in three households reported that a virus, spyware or phishing scam caused serious computer problems and/or financial losses in the past two years;
- Thirty-nine percent of those surveyed reported infection by a virus over the last two years;
- The average cost of a virus infection was $109, though some consumers reported costs in the thousands;
- In the last two years, virus infections prompted an estimated 2.6 million households to replace their computers;
- In the last six months, spyware infections prompted nearly 1 million households to replace their computers;
- Twenty percent of households do not have anti-virus software installed on their computers;
- Thirty-five percent of households do not use software to block or remove spyware;
- Though most households have firewalls installed on their computers, an estimated 2.4 million consumers with broadband do not.
- Despite modest declines in virus and spyware infections, both problems remain epidemic;
- Among the fastest-growing cyberthreats are legions of personal computers compromised by bots that are leased out to spam, spyware and identity-theft criminals.

Thank you for your consideration and your efforts to address this serious issue.

Sincerely,



Jeannine Kenney
Senior Policy Analyst
Consumers Union

Consumers Union
Headquarters Office
101 Truman Avenue
Yonkers, New York 10703-1057
(914) 378-2029
(914) 378-2992 (fax)

Washington Office
1666 Connecticut Avenue, NW
Washington, DC 20009-1039
(202) 462-6262 Suite 310
(202) 265-9548 (fax)

West Coast Regional Office
1535 Mission Street
San Francisco, CA 94103-2512
(415) 461-6747
(415) 431-0906 (fax)

South West Regional Office
1300 Guadalupe, Suite 100
Austin, TX 78701-1643
(512) 477-4431
(512) 477-8934 (fax)

CR INVESTIGATES

CYBER INSECURITY

VIRUSES • SPAM • SPYWARE

You're more vulnerable than you think

ALSO IN THIS SECTION:

25 BEST SOFTWARE TOOLS
30 BACKUP SYSTEMS
32 TOP LAPTOPS

CR Quick Take

We took an in-depth look at consumer security on the Internet by conducting a survey of online consumers and interviewing experts. Here's what we found:

- Bots, malicious software that controls a computer without your knowledge, are on the rise. Foil them by installing a firewall. Seven of the antivirus software products rated on page 27 feature a firewall.
- Virus and worm attacks are becoming more focused and still cause serious losses for millions. See page 27 for Ratings of antivirus software.
- Spyware infections are still widespread. To block them, run at least one antispyware product (see page 28).
- Phishing, fraudulent e-mail linked to a bogus site to steal personal information, is becoming more damaging.
- Spam remains a threat, despite landmark prosecutions. Use an Internet provider that filters e-mail and consider antispam software (see page 29).

Attacks on the Internet spread like measles across an animated world map in a war-room-style chamber. The red dots advancing across the projected continents signified attempts at unauthorized entry into enterprise or home computers, probably to steal data or spread malicious software. That was the scene our reporter observed when he recently visited the Alexandria, Va., facility of security provider Symantec.

An accompanying tally certified the cyberassaults as a full-blown plague: More than 59 million such attempts had come from North America alone during the previous 24 hours of monitoring.

The 40,000 sensors worldwide monitored by Symantec's private security network represent but a tiny fraction of the Internet. Dozens of similar facilities, run by government, academic, and commercial institutions, monitor the daily onslaught of Internet threats.

Despite the best efforts of all those experts and institutions, the threat is as stark as ever. Nationally, the price of such cyberinsecurity remains staggeringly high. Thanks to viruses and spyware, American consumers spent at least $7.8 billion for computer repairs, parts, and replacement over the past two years, according to the 2006 Consumer Reports State of the Net, our third annual survey of online activity and threats, conducted this spring by the Consumer Reports National Research Center.

A recent rise in prosecutions of online perpetrators might offer hope that you're now less likely to suffer computer damage, financial loss, or both from viruses, spyware, or "phishing" e-mail scams. In fact, according to the survey, your odds of becoming a cybervictim are about 1 in 3, the same as a year ago. The survey results are summarized in the table on pages 22 and 23.

To help you cope with the Internet's hazards, we interviewed experts from industry, government, and public-interest groups. We spoke to national and state law-enforcement officials as well as victims of Internet threats. We collected hundreds of pieces of spam and created thousands of pieces of malicious software, the kind virus writers inflict on consumers.

We also looked at security software products that block viruses, spyware, and spam, and in each category, we found several dedicated products that offer very good or excellent protection against the respective hazard. Software suites, which try to protect against the same three hazards within a single package, weren't usually as successful.

WORLD WATCH

A projection screen at a facility in suburban Virginia shows Internet threats being tracked. The 40,000 sensors worldwide monitored by Symantec Corporation's security network show top threats to consumers online: four viruses and a spyware program. One of many centers operated by government, academic, and commercial institutions, this outpost of cybersecurity tallies, for the previous 24 hours alone, more than 59 million malicious attacks coming from North America.

ATTACKS

Measles-like patterns of "events," attempts to break into business or home computers, pervade North America's population, high-tech, and academic centers. Net threats are truly global, with the number of attacks coming from Asia and Europe growing more quickly than those coming from North America.

PHOTO BY CHRIS HUNTER

Our survey and investigation found declines in virus and spyware infections since last year, but both remain epidemic. As we did last year, we found that some major, well-known companies have continued to support spyware or adware by using it as an advertising medium.

Until things improve, every online consumer must think like a security expert. "It's up to you to be sure all your software is up to date, with automatic scanning functions turned on," says Kathryn Sederquist of retailer Best Buy's Geek Squad technical support service in Riverhead, N.Y. She recently removed a virus that had replicated itself 40,000 times on a customer's home PC. For seven steps you can take to protect yourself online, see "Stay safe online," on page 25.

Here are some of the specific findings from our investigation:

- In a nationally representative sample of more than 2,000 households with Internet access, 29 percent said a virus, spyware, or phishing scam caused serious computer problems and/or financial losses in the past two years. Based on projections from our survey, virus infections prompted an estimated 2.6 million households to replace their computers in the past two years and spyware infections prompted nearly a million in the past six months.
- Too many consumers' defenses are down. Twenty percent of the households surveyed didn't have antivirus software installed. Thirty-five percent didn't use software to block or remove spyware. And consumers in roughly 795,000 households continued to buy products advertised through spam. Most homes had a firewall installed to block hackers. Still, based on our findings, we project that about 2.4 million U.S. households with broadband, who are hackers' prime targets, remain unprotected by a firewall.
- Minors are being targeted online, as

For more information

Free: Tips on protecting yourself online, avoiding viruses, and reporting cybercrimes. Plus a slide show of our visit to Symantec's Internet security monitoring center and more.
www.ConsumerReports.org/security

easy marks for spyware and by predators on social networking sites like MySpace.com (see Alert on page 24).

• Fifty-nine percent of Windows users reported a virus infection during the past two years or a spyware infection in the past six months. But far fewer Macintosh users reported such infections. In recent months, though, Apple Computer has warned of and corrected vulnerabilities in OS X and its Safari Web browser.

• Among the fastest-growing cyberthreats are legions of personal computers compromised by bots (malicious software that controls a computer without its owner's knowledge) that are leased out to spam, spyware, and identity-theft criminals. In June, Microsoft announced that over 15 months, software it had distributed had removed bots from more than 1.7 million Windows-based computers.

Here's the latest news about the major online threats and what's being done to combat them:

VIRUSES: STILL COSTLY

Viruses (malicious programs that infect computers and use them to propagate) and worms (self-replicating programs that bog down computers and networks) are still a major scourge. In our survey, 39 percent of respondents reported an infection in the past two years. Of those, 34 percent had to reformat their hard drives, 16 percent permanently lost important data, and 8 percent had to replace hardware. The median cost of an infection was $109, but some respondents reported costs in the thousands.

Among other new threats is "ransomware," which encrypts the data on a user's hard drive and demands a ransom of up to hundreds of dollars to free it up. Another is the innocent-sounding "rootkit," software that embeds itself on your hard drive, where it can shield malicious software from detection.

A new breed of viruses targets a distinct community, rather than the public at large. On the day we visited Symantec's Virginia security facility, for example, among the hundreds of threats that security analyst John Wagner was tracking was a freshly discovered computer worm named JS.Yamanner@m. This worm didn't raise general alarms across the Internet. Instead, it infected users of Yahoo's e-mail service with spyware. Within hours, antidotes released as updates to antivirus software products were able to limit the damage.

What's being done. Legal action against virus writers often isn't effective because so many of them operate abroad. In May, a Russian convicted of unleashing 4,000 computer viruses received a slap on the wrist—a suspended two-year jail term and a year's probation. The best defense against viruses remains fully updated antivirus software, the best of which proved very effective in our groundbreaking tests (see From Our Labs, on page 26).

SPYWARE: DOWN BUT NOT OUT

Although our survey registered a decline in the number of recent spyware infections, new sources of threats continue to arise. Even Internet search engines can be sources of infection. A study this past January of five major search engines, co-written by Ben Edelman, a spyware researcher who has served as an expert witness in lawsuits against spyware companies, found that sponsored results (the ones advertisers pay to have shown) contained two to four times as many dangerous sites as nonsponsored results. The proportion of dangerous sites displayed was even higher when the searches included keywords like "free screensavers" or "download music."

Among respondents to our survey, two of the biggest risk factors for spyware infection were having used Internet file-sharing software, such as Kazaa, and having minors at home who go online.

In March, 2006, the Center for Democracy and Technology, a Washington, D.C.-based nonprofit, public-interest group, reported that ads for some well-known brands, including ProFlowers, NetZero, eHarmony, and Netflix, had in the past been served by adware produced by 180solutions, a firm the group has accused, in two recent complaints to the

Consumer Reports

STATE OF THE NET 2006

The risks associated with using the Internet remain high. Our third annual State of the Net assesses the likelihood and impact of four leading online hazards, listed in order of incidence, based on the nationally representative survey conducted by the Consumer Reports National Research Center and our follow-up investigation.

SPAM

OVERVIEW

The incidence of heavy spam remains as elevated as last year. Spam still makes up most of the e-mail traffic on the Internet, clogging the In boxes of tens of millions of U.S. households.

NATIONAL INCIDENCE

1 in 2 experienced high levels of spam

VIRUSES

OVERVIEW

The frequency of virus-induced problems is at the same high level as last year. Despite the absence of any highly publicized outbreaks, viruses are still widespread and quite hazardous.

NATIONAL INCIDENCE

1 in 4 had a major, often costly problem

ECONOMIC FALLOUT

Cost per incident **$109**

Total damage **$5.2 billion**

Federal Trade Commission, of unfair and deceptive online trade practices. York Baur, an executive vice president of Zango, which was formed when 180solutions merged with another firm, told us that the company has spent the past year changing its approach in response to critics. "Our mission as a company is not to cause issues for consumers," he said.

What's being done. Legislative efforts against spyware have spread at the state level, if not nationally. In 2005, 12 states enacted antispyware laws and at least 18 states are considering such legislation. As we went to press, the U.S. Senate was considering an antispyware bill similar to the one the House passed last year.

In May, Jeanson James Ancheta, 21, was sentenced in Los Angeles to nearly five years in prison for remotely commanding a network of 400,000 consumers' computers to infect themselves and others with spyware. In October 2005, the New York Attorney General's Office reached a consent agreement with spyware marketing firm Intermix Media that included $7.5 million in penalties.

In a sign of changing times for adware purveyors, Claria, an adware pioneer, said it would leave the adware business.

PHISHING: BOOM TIMES

Phishing e-mails, which appear to come from a familiar financial institution, request personal information such as a password or PIN code. Clicking on a link connects you to a bogus look-alike Web site, where you are conned into divulging information. In May, the Anti-Phishing Working Group, an industry association, detected 12,000 unique sites, a 32 percent leap from February. New variants on phishing have emerged. "Pharming" infects a computer so that even if you type in a legitimate Web address yourself, you're redirected to a fraudulent site. "Spear phishing" targets e-mail addresses stolen from a company or organization with a spoofed message purporting to be from human resources or a colleague. Eight percent of respondents to our survey submitted personal information in response to conventional phishing e-mails. The median cost to those who fell prey was $850, several times more than last year.

What's being done. In July 2005, Virginia became the first state to adopt an anti-phishing law, which AOL cited a few months later when filing lawsuits against three major phishing gangs. California and New York have since followed with their own laws. Some Internet providers try to block phishing e-mail. But until more laws kick in and prosecutions take their toll on perpetrators, consumers are mostly on their own.

SPAM: HEAVY TRAFFIC

More than two years after Congress passed the Can-Spam Act, spam still con-

SPYWARE

OVERVIEW

Despite a decline in the incidence of spyware, its resulting problems remain epidemic. In the previous six months, spyware infections prompted nearly a million U.S. households to replace their computer.

NATIONAL INCIDENCE

1 in 8 had a major, often costly problem

ECONOMIC FALLOUT

Cost per incident **$100**

Total damage **$2.6 billion**

PHISHING

OVERVIEW

Phishing attacks are as rampant as they were last year, while the median cost per victim has increased fivefold. In 2006 alone, the number of fraudulent sites has risen at an alarming rate.

NATIONAL INCIDENCE

1 in 115 lost money from an account

ECONOMIC FALLOUT

Cost per incident **$850**

Total damage **$630 million**

ALERT

SPYWARE THAT STALKS

Close to one in four women surveyed for a Department of Justice study said they'd been physically abused by an intimate partner. Such abuse is often preceded by stalking, which is increasingly taking electronic form. "Technology is showing up in almost every domestic-violence case," says Cindy Southworth, director of technology at the National Network to End Domestic Violence in Washington, D.C. Our national survey supports her observation. In more than 680,000 Internet-using households, we project, someone was harassed or harmed by a person monitoring their activities using spyware.

Southworth notes that more domestic-violence perpetrators are relying on specialized spyware, known as a key logger, which records a victim's keystrokes and sends images of the computer's screen secretly to whoever installed the spyware.

"You can monitor every e-mail, IM, and chat, and log every Web site visited," Southworth says. Such software is extremely easy to find. Using a simple search, we found several examples explicitly targeted at spousal spying. Most were aimed at both genders, but one unabashedly geared toward helping men spy on their wives urged them to "Remember: you have the right to know!"

In a recent case that resulted in indictments of the users and the software's creator, a now-defunct program called LoverSpy installed itself on victims' PCs via electronic greeting cards, then sent records of the victims' every electronic move back to the stalkers.

If you suspect you're being spied upon, here are some first steps to take:

Stay mum. If you're living in the same house with an abuser, don't drop any hints of your suspicions.

Lay low. If an ex-spouse or -partner seems to know too much about you, stop using your computer online. Go to a library, friend's house, or cybercafe.

Get help. Before trying to determine whether there's spyware on your computer, contact a trained advocate or law-enforcement person. Perpetrators are often dangerous when they think they've been discovered. Don't remove the spyware; you might destroy crucial evidence. For more help, call the National Domestic Violence Hotline at 800-799-SAFE.

situtes the majority of e-mail traffic. In our survey, 53 percent of the respondents who received spam said they received apparently fraudulent solicitations and 43 percent perceived an invasion of privacy.

What's being done. Prosecutions under Can-Spam have netted dedicated spammers and legitimate businesses that have erred in their marketing practices.

In January 2006, one of the few people charged under Can-Spam pleaded guilty to three felony counts in federal court in Ann Arbor, Mich. Two weeks later, another guilty plea was entered in a Can-Spam criminal prosecution by the Department of Justice in Phoenix. The FTC has also leveraged the Can-Spam Act to impose fines in several high-profile civil settlements, including a $26,000 penalty for Kodak Imaging Network, formerly Ofoto, which e-mailed customers with no opt-out option.

Despite these successes, scores of heavy spammers continue evading the law by operating offshore.

TOWARD A SAFER FUTURE

Here's how several initiatives to control Internet threats are faring. Some have met opposition from consumer advocates because of their possible side effects.

Aggressive blocking. In the past year, both AOL and EarthLink began providing users with integrated, one-stop installation of firewall, antivirus, spyware, and phishing protection. AOL has been so aggressive in blocking spammers that for periods sometimes lasting days, it has inadvertently blocked legitimate senders.

E-mail postage. AOL has implemented an e-mail service under which legitimate senders outside AOL can pay to bypass its spam blocking. An icon in the recipient's In box certifies the sender's authenticity. DearAOL.com, a coalition of more than 500 organizations, including the Electronic Frontier Foundation, opposes the service as an e-mail tax that threatens to foster a two-tiered Internet, limiting the free flow of communications.

Authentication. E-mail authentication techniques allow the receiving Internet provider to verify the identity of an e-mail's sender. E-mail services from AOL, Microsoft, Yahoo, and 15 other providers now support some form of authentication. Although authentication's effectiveness is still subject to debate, it is becoming more prevalent among corporate users, too. But the lack of an industry standard has kept it from being used more widely in consumer e-mail.

New Windows. Microsoft says that Vista, the latest version of Windows, due for release in early 2007, is designed to be more secure than Windows XP. Vista will have built-in scanning for spyware and other malicious programs, a phishing filter and security status bars for Web surfing. Those features notwithstanding, no program is infallible. We'll test and report on Vista when it's released.

Extending the law's reach. In March 2006 the Senate approved the Undertaking Spam, Spyware and Fraud Enforcement With Enforcers Beyond Borders Act (US Safe Web Act), which would allow the FTC to exchange information on ongoing investigations with foreign law enforcers, boosting the agency's efforts to nab spammers and spyware distributors abroad. However, the House of Representatives has no corresponding bill scheduled for a vote.

ALERT TARGETING CHILDREN ON THE INTERNET

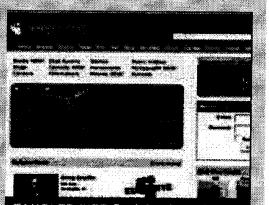
Soon after 10-year-old Matt Turner innocently played a computer game on a gaming Web site in late 2004, ads, including pornographic ones, began popping up on his screen. "I felt violated, intruded upon, alarmed," says his father, Allen, 46, who works for a manufacturer in Wichita, Kan.

The Turners were victims of several notorious spyware programs. When he complained to ABI network, the spyware's distributor, Allen Turner was asked to download a program to rid his son's machine of the hard-to-uninstall software. Instead, he reformatted the hard drive on Matt's computer and started over.

A few months later, Turner researched ABI's parent company, New York-based Direct Revenue, then sent a complaint to Eliot Spitzer, the New York attorney general. In April 2006, Spitzer's office sued Direct Revenue for deceptive and nonconsensual spyware installation, based on numerous consumer complaints, including Turner's. Direct Revenue calls the charges baseless.

Incidents like this aren't as rare as you might think. Our 2006 State of the Net Survey found that in homes where children under 18 used the Internet, there was a 28 percent greater incidence of spyware infection in the past six months than in other homes. Further, in 8 percent of the households we surveyed that had children under 18, a child had inadvertently seen pornographic material as a result of spam.

Other risks exist, too. Recently, social networking site MySpace.com added restrictions on adults contacting youngsters, after a $30 million suit was filed on behalf of a 14-year-old claiming to have been sexually assaulted by an adult she met on MySpace.



TANGLED WEB **Social networking sites like MySpace.com can be risky places for minors.**

Such restrictions are toothless on MySpace.com because the service lacks an age-verification system. In June, a phishing site targeting account information of MySpace.com members, which used a link sent via AOL Instant Messenger to lure victims, was discovered and removed from a computer in California.

Andy Purdy, acting director of the National Cyber Security Division of the U.S. Department of Homeland Security, was surprised to find that his daughter's friend had been exposed to sexually explicit messages from someone claiming to be a 13-year-old, while playing an online checkers game. "You never think that something like that has the potential for misuse," he explains. "We went to the girl's parents and said you have to watch over this stuff."

These cases show that while safe practices are helpful, they alone don't fully protect children. And as our tests of Internet filtering software, published in June 2005, show, neither can such software. Parental supervision is essential.

situtes the majority of e-mail traffic. In our survey, 53 percent of the respondents who received spam said they received apparently fraudulent solicitations and 43 percent perceived an invasion of privacy.

What's being done. Prosecutions under Can-Spam have netted dedicated spammers and legitimate businesses that have erred in their marketing practices.

In January 2006, one of the few people charged under Can-Spam pleaded guilty to three felony counts in federal court in Ann Arbor, Mich. Two weeks later, another guilty plea was entered in a Can-Spam criminal prosecution by the Department of Justice in Phoenix. The FTC has also leveraged the Can-Spam Act to impose fines in several high-profile civil settlements, including a $26,000 penalty for Kodak Imaging Network, formerly Ofoto, which e-mailed customers with no opt-out option.

Despite these successes, scores of heavy spammers continue evading the law by operating offshore.

TOWARD A SAFER FUTURE

Here's how several initiatives to control Internet threats are faring. Some have met opposition from consumer advocates because of their possible side effects.

Aggressive blocking. In the past year, both AOL and EarthLink began providing users with integrated, one-stop installation of firewall, antivirus, spyware, and phishing protection. AOL has been so aggressive in blocking spammers that for periods sometimes lasting days, it has inadvertently blocked legitimate senders.

E-mail postage. AOL has implemented an e-mail service under which legitimate senders outside AOL can pay to bypass its spam blocking. An icon in the recipient's In box certifies the sender's authenticity. DearAOL.com, a coalition of more than 500 organizations, including the Electronic Frontier Foundation, opposes the service as an e-mail tax that threatens to foster a two-tiered Internet, limiting the free flow of communications.

Authentication. E-mail authentication techniques allow the receiving Internet provider to verify the identity of an e-mail's sender. E-mail services from AOL, Microsoft, Yahoo, and 15 other providers now support some form of authentication. Although authentication's effectiveness is still subject to debate, it is becoming more prevalent among corporate users, too. But the lack of an industry standard has kept it from being used more widely in consumer e-mail.

New Windows. Microsoft says that Vista, the latest version of Windows, due for release in early 2007, is designed to be more secure than Windows XP. Vista will have built-in scanning for spyware and other malicious programs, a phishing filter and security status bars for Web surfing. Those features notwithstanding, no program is infallible. We'll test and report on Vista when it's released.

Extending the law's reach. In March 2006 the Senate approved the Undertaking Spam, Spyware and Fraud Enforcement With Enforcers Beyond Borders Act (US Safe Web Act), which would allow the FTC to exchange information on ongoing investigations with foreign law enforcers, boosting the agency's efforts to nab spammers and spyware distributors abroad. However, the House of Representatives has no corresponding bill scheduled for a vote.

ALERT TARGETING CHILDREN ON THE INTERNET

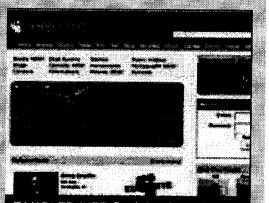
Soon after 10-year-old Matt Turner innocently played a computer game on a gaming Web site in late 2004, ads, including pornographic ones, began popping up on his screen. "I felt violated, intruded upon, alarmed," says his father, Allen, 46, who works for a manufacturer in Wichita, Kan.

The Turners were victims of several notorious spyware programs. When he complained to ABI network, the spyware's distributor, Allen Turner was asked to download a program to rid his son's machine of the hard-to-uninstall software. Instead, he reformatted the hard drive on Matt's computer and started over.

A few months later, Turner researched ABI's parent company, New York-based Direct Revenue, then sent a complaint to Eliot Spitzer, the New York attorney general. In April 2006, Spitzer's office sued Direct Revenue for deceptive and nonconsensual spyware installation, based on numerous consumer complaints, including Turner's. Direct Revenue calls the charges baseless.

Incidents like this aren't as rare as you might think. Our 2006 State of the Net Survey found that in homes where children under 18 used the Internet, there was a 28 percent greater incidence of spyware infection in the past six months than in other homes. Further, in 8 percent of the households we surveyed that had children under 18, a child had inadvertently seen pornographic material as a result of spam.

Other risks exist, too. Recently, social networking site MySpace.com added restrictions on adults contacting youngsters, after a $30 million suit was filed on behalf of a 14-year-old claiming to have been sexually assaulted by an adult she met on MySpace.



TANGLED WEB **Social networking sites like MySpace.com can be risky places for minors.**

Such restrictions are toothless on MySpace.com because the service lacks an age-verification system. In June, a phishing site targeting account information of MySpace.com members, which used a link sent via AOL Instant Messenger to lure victims, was discovered and removed from a computer in California.

Andy Purdy, acting director of the National Cyber Security Division of the U.S. Department of Homeland Security, was surprised to find that his daughter's friend had been exposed to sexually explicit messages from someone claiming to be a 13-year-old, while playing an online checkers game. "You never think that something like that has the potential for misuse," he explains. "We went to the girl's parents and said you have to watch over this stuff."

These cases show that while safe practices are helpful, they alone don't fully protect children. And as our tests of Internet filtering software, published in June 2005, show, neither can such software. Parental supervision is essential.

RESPONSE FOR THE RECORD OF DAVID A. POWNER, DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

United States Government Accountability Office
Washington, DC 20548

October 16, 2006

The Honorable Fred Upton
Chairman, Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
House of Representatives

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

Subject: *Challenges in Developing a Public/Private Recovery Plan*

This letter responds to your request that we answer questions relating to our recently released report and our testimony of September 13, 2006.[1] In that hearing, we discussed challenges in developing a public/private Internet recovery plan. Your questions, along with our responses, follow.

1. *The Government Accountability Office (GAO) report outlines challenges the Department of Homeland Security (DHS) faces in planning for Internet reconstitution. Given the many challenges outlined, what practical steps could DHS take now to begin developing recovery plans?*

DHS could take key steps in the near term that could help with recovery planning. Such steps could include completing the Internet components of the National Response Plan and the National Infrastructure Protection Plan. These plans could be used as a basis to develop a public/private Internet recovery plan that includes input from the private sector and addresses activities we identified in our report, such as providing assistance with the provision of fuel and power, providing access to restricted areas, helping with prioritization, and assisting with funds for backup communications systems. Now that DHS has filled the position of Assistant Secretary of Cyber Security and Telecommunications, the assistant secretary should lead efforts to work with the private sector to complete these efforts.

[1]GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006) and GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO-06-1100T (Washington, D.C.: Sept. 13, 2006).

2. *The GAO testimony questions the sufficiency of several initatives DHS is taking regarding Internet reconstitution. Why aren't these initiatives sufficient?*

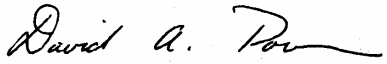
While these activities are promising, some initiatives are not complete, others lack timelines and priorities, and still others lack effective mechanisms for incorporating lessons learned. Specifically, DHS has developed high-level plans for infrastructure protection and national disaster response, but these plans are not complete and lack support from the private sector. Also, at the time of our report, DHS officials had not yet finalized plans, resources, or milestones for future efforts of the Internet Disruption Working Group. Additionally, DHS had not yet identified which group should be responsible for incorporating lessons learned from recent exercises into its plans and initiatives. Other initiatives to improve the nation's ability to recover from Internet disruptions include working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. However, the relationships among these initiatives are not evident.

3. *GAO's recommendations focused on specific roles and actions DHS could take now, based on input from the private sector. Do you anticipate that the government's focus on large scale planning efforts for the National Response Plan and the National Infrastructure Protection Plan will affect its ability to achieve the more specific efforts? If so, how?*

The National Response Plan and National Infrastructure Protection Plan are designed to be high-level frameworks. These frameworks are to provide a structure for more detailed plans, which, if completed appropriately, could lead to the specific roles and actions identified in our report.

In responding to these questions, we relied on previous audit work we preformed in developing our report on Internet recovery. Should you or your office have any questions on matters discussed in this letter, please contact us at (202) 512-9286 or (202) 512-6412, or by e-mail at pownerd@gao.gov and rhodesk@gao.gov.

Sincerely yours,



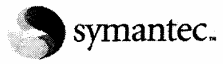
David A. Powner
Director, Information Technology
Management Issues

Keith A. Rhodes
Chief Technologist and Director,
Center for Technology and Engineering

cc: The Honorable Edward J. Markey
Ranking Minority Member
Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
House of Representatives

(310831)

RESPONSE FOR THE RECORD OF VINCENT WEAFER, SENIOR DIRECTOR, SYMANTEC SECURITY RESPONSE, SYMANTEC CORPORATION



October 18, 2006

The Honorable Fred Upton
Chairman, Subcommittee on Telecommunications and the Internet
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Re: Responses to Additional Questions from the Subcommittee on Telecommunications and the Internet hearing on, "Cybersecurity: Protecting America's Critical Infrastructure, Economy, and Consumers"

Dear Chairman Upton:

Thank you for the honor of allowing me to testify before the House Subcommittee on Telecommunications and the Internet at the September 18 hearing on, "Cybersecurity: Protecting America's Critical Infrastructure, Economy, and Consumers". Please find attached my responses to the additional questions which Congressman Dingell submitted to me for additional comment.

It was a privilege to testify before your Committee and I am hopeful that you and your colleagues found my comments to be helpful in your efforts to have Congress better enhance our nation's information security infrastructure.

If I or anyone else at our firm can be of further assistance to you and your colleagues on these important issues please do not hesitate to contact myself or Kevin Richards, Federal Government Relations Manager, for Symantec at 202/742-6582.

Thank you, again, and I look forward to working together with Committee on these issues in the future.

Sincerely,

Vincent Weafer
Senior Director
Security Response

Attachment

cc: The Honorable Edward J. Markey
Ranking Member
Subcommittee on Telecommunications and the Internet

The Honorable John D. Dingell
Ranking Member
Committee on Energy and Commerce

1. What are the risks and benefits of private companies sharing information with the Department of Homeland Security (DHS)?

Information sharing among government agencies and the private sector has emerged as one of the most critical challenges of the post 9/11 era. A key element of this challenge is that while the federal government is expected to keep the U.S. secure, the overwhelming majority (85 to 90 percent) of the nation's critical infrastructure is owned by the private sector.

In structuring its strategy for securing the national critical infrastructure, the Department of Homeland Security (DHS) has been designated as the lead agency and is charged with finding ways to improve information sharing while the IT systems that control the critical infrastructure -- such as telecommunications networks, the electrical power grid, oil pipelines, and water treatment plants -- remain protected from physical and cyberthreats.

In early 2005, the Government Accountability Office (GAO) published a report that criticized the DHS for not doing enough to reach out to the private sector. The report asserted that many organizations responsible for the nation's critical infrastructure "are either unaware of key areas of cybersecurity risks or unprepared to effectively address cyber emergencies. Further, DHS continues to have difficulties in developing partnerships -- as called for in federal policy -- with other federal agencies, state and local governments, and (the) private sector." Without effective partnerships with the private sector, the government's mission to secure our nation’s infrastructure will not be successful.

While information sharing is necessary for critical infrastructure protection, it may also leave participants more vulnerable to attacks. In order to effectively protect the infrastructure, government agencies and private firms must work together to determine what kinds of information should be shared and why, develop the appropriate information sharing mechanisms (such as further development of the IT-ISAC and IT-SCC for the IT Sector), ensure that the public sector shares as much timely information as possible, and make the intelligence more actionable for all parties. Most of the information the private sector has received in the past has been old information or is not enough information to take any specific actions. We have seen some improvement recently in this area. The advent of the Protected Critical Infrastructure Information (PCII) program is also a positive step toward protecting sensitive information and only sharing it with appropriate parties. However, there are still some questions that remain about the PCII program, including how the information which is submitted will be protected and to what extent a company can control the information once submitted.

Before the government can expect the private sector to fully cooperate and share valuable IT information and assets, the government should be able to demonstrate a secure, resilient infrastructure of its own. The most recent FISMA scores signal that many agencies still have a lot more to do in the area of IT Security. By combining the right technologies, processes, and policies, agencies can dramatically reduce the risk of unexpected disruptions, increase their ability to maintain continuity of normal business operations, protect highly sensitive information, and tightly align IT to changing operational goals.

2. What improvements could DHS make in building its working relationships with private sector information technology and communications companies and major industrial users of the Internet?

The Department of Homeland Security should streamline communication with private firms holding a stake in the nation's critical infrastructure sectors. In addition,

DHS should expedite recommendations provided by private sector representatives serving on the National Infrastructure Assurance Council (NIAC).

Symantec's Chairman and CEO, John W. Thompson, was appointed in 2002 to the National Infrastructure Assurance Council (NIAC) by U.S. President George W. Bush. The NIAC was established by the President to provide advice on the security of information systems for critical infrastructure supporting key sectors of the national economy, including banking and finance, transportation, energy, manufacturing, and emergency government services.

During the summer of 2005, the NIAC established a Sector Partnership Model Working Group from a DHS requested study and provided recommendations on its structure, function and implementation.

In October 2005, the Working Group presented its initial report and findings to the NIAC, affirming the structure of the partnership model presented in the National Infrastructure Protection Plan (NIPP), and recommending key operating principles, including that the partnership be considered a collaboration of equals between the government and the private sector. The approach includes sector based and cross-sector partnerships.

We believe that DHS should implement a "sector partnership model" in which leaders from the private sector and government counterparts that do similar work would share information about sector-specific topics. Unlike formal governmental advisory committees that involve private sector voices, these groups of leaders would be self-organized bodies and remain independent of government control.

Symantec recommends that DHS should also continue to work with private industry to discuss the key challenges the Department faces that impede the private sector's willingness to share sensitive information. Some of these key challenges for DHS include:

- defining specific government needs for critical infrastructure information,
- determining how the information will be used,
- assuring the private sector that the information will be protected and who will be authorized to have access to the information, and
- demonstrating to critical infrastructure owners the benefits of sharing the information.

If DHS were able to surmount these challenges, it and other government users may begin to overcome the lack of trust that critical infrastructure owners have in the government's ability to use and protect their sensitive information.

Finally, Symantec has made numerous recommendations over the last several years related to information sharing functions that have been transferred to DHS. One significant area concerns the federal government's CIP efforts, which is focused on the sharing of information on incidents, threats, and vulnerabilities, and the providing of warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector. Although improvements have been made, further efforts are needed by DHS in coordination with the private sector to address the following critical CIP challenges:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;

- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector; and
- providing appropriate incentives for non-federal entities to increase information sharing with the federal government and enhance other CIP efforts.

The success of homeland security also relies on establishing effective systems and processes to facilitate information sharing among and between government entities and the private sector. The ISAC's have identified critical success factors and other key management issues that DHS should consider as it establishes systems and processes to facilitate information sharing among and between government entities and the private sector.

These success factors include establishing trust relationships with a wide variety of federal and non-federal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents. As part of its information technology management, DHS should continue to develop and implement enterprise architecture to integrate the many existing systems and processes required to support its mission and to guide the department's investments in new systems to effectively support homeland security in the coming years. Other key management issues include ensuring that sensitive information is secured, developing secure communications networks, integrating staff from different organizations, and ensuring that the department has properly skilled staff.

3. Describe (a) the involvement of private sector firms in the development of the National Infrastructure Protection Plan and your views on the efforts to develop this plan; and (b) the involvement of private sector firms in the ongoing development of the IT/Communications Sector specific plan in response to NIPP and your view of the process by which the sector-specific plan is being developed.

(A.) As the focal point for critical infrastructure protection, DHS has many cybersecurity and other IT related responsibilities that are called for in law and policy. In 2005 and 2006, DHS initiated efforts to address these responsibilities, but much more remains to be done.

On June 30, pursuant to Homeland Security Presidential Directive 7, the Department of Homeland Security (DHS) released a final (NIPP). The final NIPP builds on the framework established in both the interim and draft versions of the NIPP, issued in February 2005 and November 2005 respectively. Symantec believes that DHS has made significant progress on these responsibilities with the June 2006 release of the National Infrastructure Protection Plan; however, supplemental sector-specific plans have not yet been finalized.

Private sector firms were allowed little time to review and comment on the finalized version of the NIPP. Many IT/Communications sector specific firms had hoped to be consulted earlier by DHS to participate in the drafting process for the NIPP up front as opposed to being asked to comment on a DHS completed document without prior industry consultation.

Symantec is encouraged that the final NIPP includes more references to the IT Sector. However, we believe the plan needs to go one step further by addressing avenues for merging physical and cyber protection. Reconciling the two won't be any easy task but that is what the 17 sector-specific councils are charged with doing in 180 days; that's

the deadline for preparing individual infrastructure protection plans for the telecommunications, IT, financial service, chemical and other industries designated "criticial" by the DHS. These plans will be based on the NIPP and sanctioned and released by DHS, but issued as guidance, meaning compliance by companies will be voluntary. The key part of each of those sector specific plans will be a risk assessment of the possibility of a cyber or physical attack and an estimation of its effects.

Symantec believes that it will be most difficult for security professionals in each industry to merge those two risk assessments, especially given the lack of specificity in the NIPP. There is a complex web of issues which have not been dealt with in the NIPP. For example, a dam -- and most physical assets -- are built to certain specifications in order to resist threats, such as a storm, of a specified magnitude. If the dam breaks, the result can typically be predicted. But if vulnerability in an operating system is exploited, the asset, i.e. the computer, is not damaged. Rather, there is a loss of functionality throughout a network, the extent of which cannot be predicted in advance. Symantec is concerned that the sector-specific plans will confine network security to the backseat as concern over dams, rivers, buildings and other physical assets drives each plan. The NIPP focuses more directly on protection of physical assets and still needs greater emphasis on cybersecurity. Symantec recommends greater inclusion of cyber security in the NIPP. We have identified several clear and present cyber security threats to U.S. critical infrastructure which exist from many sources.

(B.) Symantec is a member of the Information Technology Sector Coordinating Council (IT-SCC) which was established on January 27, 2006 for the purposes of bringing together companies, associations, and other key IT sector participants on a regular basis to coordinate strategic activities and communicate broad sector member views associated with infrastructure protection, response and recovery that are broadly relevant to the IT Sector.

The IT-SCC was formed, in part, to support the "Sector Partnership Model" developed by DHS and endorsed by the NIAC. Symantec remains closely engaged with DHS, specifically the National Cyber Security Division (NCSD) as our lead Sector Agency, in CIP policy development and coordination. For operational information sharing issues, the IT-ISAC will take leadership, with the support of the IT SCC. The IT sector envisions a secure, resilient, and protected global information infrastructure that can rapidly restore services if affected by an emergency or crisis, ensuring the continued and efficient function of information technologies, infrastructures and services for people, governments, and businesses worldwide.

Symantec and other Council members are working in partnership with DHS in developing risked based, private sector driven critical infrastructure protection (CIP) initiatives. Specifically, the IT SCC is working with the NCSD to develop a new understanding of IT assets that is function based, as opposed to the traditional physical structure conception of assets. The IT SCC has developed a Plans Working Group to coordinate the IT SCC's input to the government's National Infrastructure Protection Plan (NIPP) and co-development of the IT Sector Specific Plan (SSP).

Additionally, the IT-SCC is looking to build more robust information sharing between DHS and the private sector. As such, the IT SCC has asked DHS to use the powers granted to it in Section 871 of the Homeland Security Act and develop a FACA exempt structure to more easily share information. The April 2006 announcement by DHS of the formation of the Critical Infrastructure Protection Advisory Committee (CIPAC) responds to that need, and the IT-SCC is working with DHS to refine architecture and operation of that committee. Additionally, the IT-ISAC continues to engage DHS on operational information sharing.

Symantec has been pleased with our participation in the IT SCC and the process to collaboratively work together with other industry players on an IT sector specific plan.

4. What factors make private/public working groups more/less effective in planning for or responding to major Internet disruptions?

The Internet and its communications infrastructure serve as the backbone of information exchange that is vital to our nation's security and our economy. Yet many feel the United States is not sufficiently prepared for a major attack, software incident or natural disaster that would lead to disruption of large parts of the Internet. Despite a series of efforts in recent years to address this issue, some gaps still exist in the response plans of the U.S. government and the private sector for reconstituting the Internet in the event of an unprecedented massive Internet disruption.

The primary factor that can make private/public working groups ineffective in planning for or responding to major Internet disruptions is that there is currently no well-coordinated processes or roles and responsibilities which exist today that would integrate the disparate plans of industry and government to restore Internet functioning when recovering from a major cyber attack. Some of the recent government exercises demonstrate that there is much to improve on from both sides.

According to the GAO, DHS has so far failed to establish a comprehensive plan for responding to cyberthreats against critical infrastructure. Criminal groups, foreign intelligence services and terrorists all have the ability to launch disruptive physical and cyberattacks. While the DHS developed high-level plans for infrastructure protection, components that address Internet recovery are "incomplete. In addition, while the DHS has begun working with private industry on processes for jointly responding to cyberattacks, the initiatives are "immature" and lack deadlines for completion.

Also hampering the department's efforts to establish a recovery plan is a lack of agreement over what the agency's role should be when a disruption does occur and when it should get involved. In addition, the private sector has been reluctant to share information with the DHS because "it doesn't currently see a value in sharing" and lacks trust in the leadership.

A July 2005 GAO report has stated that the government is not prepared to effectively coordinate public and private-sector plans for recovering from a major Internet attack. "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," the report noted.

That said, there are definite benefits to having private/public working groups in planning for or responding to major Internet disruptions. Specifically, by working together, stronger trust relationships can built, processes can be developed and streamlined, roles can be identified, and actionable information can be shared to better protect our nation's infrastructure.

Symantec encourages more comprehensive exercises by DHS such as the Cyber Storm Exercise involving simulated cyberattacks against the nation's critical infrastructure that were conducted in February. Cyber Storm was conducted by the DHS's NCSD on Feb. 6-10. More than 110 public, private and international organizations took part in the exercise, which simulated a cyberattack directed at critical infrastructure. Among the key findings in the report is the need for a well-established chain of command in a time of crisis, the importance of information sharing across government and industry sectors and a better ability to correlate incident information across the two groups. There was some negative press regarding this exercise, but the important thing to remember is that exercises are conducted specifically to find the problem areas or gaps and fix them before the next exercise or real-life event occurs.

Symantec looks forward to continuing important work with private industry, Congress and the Administration to better enhance our nation's preparedness for a major Internet disruption or physical attack. As I noted in my testimony to the Committee, I firmly believe that it's not a question of "if", but "when". Thank you.

RESPONSE FOR THE RECORD OF PAUL B. KURTZ, EXECUTIVE DIRECTOR, CYBER SECURITY INDUSTRY ALLIANCE

CSIA's responses to follow-up questions from the September 13, 2006 hearing, "Cybersecurity: Protecting America's Critical Infrastructure, Economy, and Consumers," House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet.

1. What are the risks and benefits of private companies sharing information with the Department of Homeland Security (DHS)?

Private sector companies and organizations have invested enormous financial and human resources into developing proactive and effective partnerships with government to protect our valuable critical information infrastructure. Despite significant progress, barriers remain, and more needs to be done to improve the quality of information sharing partnerships between government and industry.

Risks: Private sector companies and the government have identified a number of risks and barriers with respect to sharing information with DHS or other federal entities. The U.S. Government Accountability Office released a report in April, 2006 that identified the following items as key challenges that impede the private sector's willingness to share sensitive information:

- defining specific government needs for critical infrastructure information;
- determining how the information will be used;
- assuring the private sector that the information will be protected and who will be authorized to have access to the information; and
- demonstrating to critical infrastructure owners the benefits of sharing the information.

Separately, the National Cyber Security Partnership's Working Group on Information Sharing identified additional barriers that require improvement:

- Industry is brought into the process once government consensus is achieved, which makes meaningful change or input difficult.
- Government consensus on major initiatives developed prior to substantial industry input creates resistance when presented to industry, on both substantive and partnership grounds.
- Every process that DHS develops to collect information (i.e., HSIN, US-CERT) should be done with industry partnership to ensure that both industry and government will have something to gain out of sharing information and thus an incentive to share.
- Outdated clearance requirements do not fit new-era information sharing requirements. A new, enhanced partnership with the private sector requires a new information classification system.

Both of these lists identify fundamental problems with the existing information-sharing process that require clarity of purpose on the part of DHS, and inclusion of the private sector on program planning and implementation. In order to establish functional and effective information-sharing partnerships, DHS and other government agencies need to establish trust among organizations and create "true" partnerships.

Establishing Trust

DHS operates under the premise that once information or data is provided, it is then "owned" by DHS and can be used as DHS sees fit. This impedes trust and eliminates any incentive by industry for information sharing. Unfortunately, the Final Rule regarding

procedures for Handling Critical Infrastructure Information issued by DHS this September (implementing the Critical Information Infrastructure Act of 2002) provides no further clarity for industry. Industry needs a clear understanding of what information they are being asked to provide, why they are being asked for it, and how it will be used. They have concerns with sharing sensitive proprietary information, and industry needs assurance that this information, when shared, will be protected. Conversely, DHS needs to reciprocate by providing industry with critical information in a timely manner.

Establishing a "true" partnership

There are many barriers to establishing a "true" partnership. DHS must ensure the partnership reflects all relevant parties and sector-specific entities. Senior leadership buy-in and support from both DHS and industry are critical in establishing this "true" partnership. Finally, the information sharing partnership must be **voluntary** and built on trust; each member must be personally responsible for their trusted behavior.

Benefits: There are several businesses and organizations with the tools, resources and expertise that can provide invaluable information DHS may not otherwise have access to, or the ability to produce. Likewise, DHS and other government agencies have their own internal organizations, plus, previously-established public-private partnerships that have made strides in information sharing and program and policy development.

Private sector organizations can gather data on threats and malicious Internet activity and present this information to DHS and other government agencies in order to raise awareness and encourage action. McAfee's AVERT Labs, for example, has developed a general ranking system that indicates the severity of known global threats and how they impact the Internet, business operations, and home users' systems. Their 100 researchers in 14 countries continuously monitor the latest threats and provide remediation. Internet Security Systems' (ISS) X-Force Threat Analysis Service (XFTAS) provides real-time threat information from ISS' international network of Security Operations Centers and delivers customized information about potential threats to networks.

Likewise, Symantec Corporation releases a semi-annual Internet Security Threat Report, or ISTR, which is a comprehensive analysis of security activity in today's information economy. It offers an overview of threat activity over a six-month period and is based on data collected from more than 40,000 sensors deployed in over 180 countries in addition to a database covering more than 18,000 vulnerabilities affecting over 30,000 technologies from more than 4,000 vendors. The Report includes an analysis of network-based attacks on the Internet with a review of known threats, vulnerabilities, malicious code and other security risks. It also offers security best practices for consumers and businesses in order to help them protect themselves against current and emerging cyber threats. The underlying data associated with such reports can help guide the government and Congress toward addressing the problem.

Presidential Decision Directive 63 (PDD63), Homeland Security Presidential Directive (HSPD-7) and Executive Order 13231 (EO - 13231) helped promote the idea of a concentrated effort regarding the sharing of various sector issues leading to unified and strengthened industry sectors entities. The IT-ISAC, or Information Sharing and Analysis Center, is a non-profit organization, providing users with real-time information about urgent alerts, security news, vulnerabilities, viruses and other Internet threats, thus providing a coherent picture of the current health of the Internet to IT-ISAC members. The purpose of the IT-ISAC is also to provide a forum for sharing threat related information, and ways to protect against those threats. Members can submit vulnerability, virus and general notifications for distribution.

Below is a description of other public-private partnerships, organizations and committees that generate strategies, programs, and best practices, where sharing critical cyber information data with the federal government has certainly been a benefit:

CERT-CC: a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University; it studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to help improve security.

National Security Telecommunications Advisory Committee (NSTAC): created by President Ronald Reagan in September 1982; it is composed of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies, and provides industry-based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy.

National Infrastructure Advisory Council (NIAC): an advisory committee within DHS that is composed of a maximum of 30 members, appointed by the President from private industry, academia, and state and local government; they provide the President through the Secretary of the Department of Homeland Security with advice on the security of the critical infrastructure sectors and their information systems.

North American Network Operators Group (NANOG): an educational and operational forum for the coordination and dissemination of technical information related to backbone/enterprise networking technologies and operational practices.

National Cyber-Forensics and Training Alliance (NCFTA): provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia and law enforcement.

National Cyber Security Alliance (NCSA): a non-profit, public-private partnership that offers resources for cyber security awareness and education for home user, small business, and education audiences. NCSA sponsors include the DHS, the Federal Trade Commission, and many private-sector corporations and organizations. NCSA provides tools and resources to empower home users, small businesses, and schools, colleges, and universities to stay safe online.

National Cyber Security Partnership (NCSP): led by the Business Software Alliance (BSA), the Information Technology Association of America (ITAA), TechNet, and the U.S. Chamber of Commerce; a voluntary public-private partnership with academicians, CEOs, federal government agencies and industry experts tasked to develop shared strategies and programs to better secure and enhance America's critical information infrastructure.

2. What improvements could DHS make in building its working relationships with private sector information technology and communications companies and major industrial users of the Internet?

Since the establishment of DHS, there has been a tension regarding what entity – public or private - is responsible for the protection of the critical information infrastructure. DHS has jurisdiction over these matters, however industry generally owns and operates the critical infrastructure; unfortunately, this tension interferes with producing a constructive industry-government partnership.

Both DHS and industry can take steps to improve this partnership:

Delineation of Roles and Responsibilities

Clear, defined roles for DHS/Federal agencies and industry must be established regarding situational awareness and early warning, emergency communications, continuity of operations planning, reconstitution, and resiliency. As Paul Kurtz, the Executive Director of CSIA stated in his testimony, currently, there is little strategic

direction or leadership from the federal government in the area of information security. CSIA believes the government has a responsibility to lead, set priorities, and coordinate and facilitate protection and response.

DHS must consider and articulate how it will work with the private sector to respond to and recover from a massive failure of information technology systems – whether from a cyber attack or a natural disaster. In preparing to respond to a significant cyber event, the question that should be asked is: What is a suitable role for DHS as well as other key federal agencies, including DoD and the FCC, in facilitating recovery and reconstitution from a cyber "incident of national significance? The existing DHS "plan" for recovery cites more than a dozen federal departments and agencies with "coordinating" responsibility – not including state, local and tribal governments. DHS needs to articulate a chain-of-command for each step of recovery and reconstitution. For example, the DHS's U.S. Computer Emergency Readiness Team (US-CERT) may be aware of a network attack, but the North American Network Operators Group (NANOG) as the operational forum for backbone/enterprise networking, will play the key technical role in actually mitigating and recovering from a cyber attack.

In the event of a natural disaster, a terrorist attack, or a failure of any kind of our critical infrastructure, both the private and public sector need to have timely access to situational information; they need to communicate with one another in order to assess and remedy the situation, and oversee COOP, reconstitution and recovery efforts. Having distinct responsibilities identified and carried out in practice scenarios will result in stronger public-private working relationships, proper planning, and effective response.

Identification of Specific Needs for Information Sharing

According to the aforementioned GAO report, DHS has not explicitly identified or defined specific needs, nor has it explained how the information submitted to the Critical Infrastructure Information (CII) Program Office will be utilized. GAO also recognized that the information that has already been submitted to the Program Office has not been utilized to issue advisories, alerts or warnings. GAO recommends that DHS define the CII needs of the department and other agencies, specify how that information will be used, assure the information will be protected, and demonstrate the benefit of information sharing.

Early and Substantive Engagement/Reciprocity of Information-Sharing

DHS should coordinate with the private sector prior to developing plans or activities designed to protect critical infrastructures in order to get a better understanding of the sector-specific characteristics and operational realities. Too often, the government develops a plan which fails to reflect unique sector needs and requirements, and the government later tries to sell the plan to the private sector. Likewise, the private sector needs to provide expertise, time and resources to identify CIP issues, and provide guidance on sector-specific issues associated with infrastructure protection and response planning.

Develop and Endorse Cyber Security Best Practices

The private sector needs to coordinate across infrastructure sectors, national borders, and industries to develop cyber security best practices that are realistic, responsive, adaptable, and forward-looking. The government should then encourage and endorse private sector cyber security best practices. It is important, however, that these best practices are viewed as advisory, flexible enough to accommodate differences in risks, and not be prescriptive.

3. Describe (a) the involvement of private sector firms in the development of the National Infrastructure Protection Plan and your views of the efforts to develop this plan; and (b) the involvement of private sector firms in the ongoing development of the IT/Communications Sector Specific Plan in response to NIPP and your views of the process by which the sector specific plan is being developed.

The National Infrastructure Protection Plan (NIPP) provides a basic flexible framework to translate the needs of both the government and private sector into planning activities to enhance national and economic security. The IT-Sector-Specific Plan (SSP) provides a unique vehicle for articulating common goals for partnering to accomplish specific objectives.

The private sector and government security partners over the past six months have jointly engaged to develop an Information Technology (IT) Sector Specific Plan (SSP) as required under the NIPP. While we have made good progress, the IT Sector Coordinating Council (SCC), the IT Government Coordinating Council (GCC), and the National Cyber Security Division (NCSD) have identified three sets of issues that require resolution to ensure effective implementation of the IT SSP.

I. Managing Risk

There are at least three issues requiring resolution between government and the IT sector.: (a) designation of critical functions, (b) risk assessment and mitigation, (c) the resources necessary to identify and protect critical functions.

(a) Critical Functions: Under the NIPP, each sector is required to identify critical infrastructure assets. Given the dynamic nature of the information infrastructure, government and private sector partners jointly agreed to focus on critical *functions* associated with the IT infrastructure.

(b) Risk Assessments: Implementing the IT Sector risk assessment approach outlined in the SSP and mitigating vulnerabilities in an effective and efficient manner requires clarity on process. Owners and operators of the IT infrastructure today engage in risk assessments based on widely accepted standards and best practices in order to ensure uninterrupted service to customers in both the public and private sector, and significant corporate resources are dedicated to performing risk assessments on a regular basis. In most cases, current best practices would be sufficient for identifying the critical functions outlined above. In some cases, risk mitigation may exceed what is required to serve customers, especially in the case of low probability catastrophic losses. In such instances, the private sector needs clarity on how such assessments are performed, how conclusions can be protected from public disclosure, and how any recommendations for mitigation shall be adjudicated.

(c) Resources: In such instances identified above in (b), the IT sector needs clarity on who shall pay for additional risk assessments and any subsequent mitigation if deemed necessary.

II. Cyber Incidents of National Significance (CINS)

There are three related issues associated with Cyber Incidents of National Significance: (a) there are no clear criteria for designating a CINS; (b) there is no clear protocol for reaching such a decision; and (c) there is no clarity on such a declaration's legal or policy significance. The third issue is most critical as owners and operators in the private sector need to understand the meaning and potential liability if such a declaration is issued. The issues related to CINS are very important. The Business Roundtable issued a June report ("Essential Steps Toward Strengthening America's Cyber Terrorism Preparedness") highlighting the importance of this issue. Specific

programs have not been implemented by DHS which need to be. Congress should ask DHS about its programs via oversight hearings.

(a) Criteria for Designating a Cyber Incident of National Significance: The National Response Plan (NRP) defines incidents of national significance and the NRP's Cyber Incident Annex describes at a high level what may constitute a CINS.

(b) CINS Protocol: There is no protocol for determining a declaration for a disruption of the Internet or communications infrastructure sufficient to cause catastrophic risk to public health and safety. Such a protocol should include consultation with the White House and appropriate federal agencies as well as the leadership of the IT and/or Communications Sector Coordinating Councils and other potentially affected sectors.

(c) Implications of Declaring a CINS: There is no clear understanding of the policy or legal authority of a CINS declaration for the IT sector.

III. Response, Recovery and Reconstitution

(a) Recovery and Reconstitution: Policies and procedures are needed to clarify the roles and responsibilities of both government and the private sector in response, recovery, and reconstituting in the event a CINS is declared. DHS leadership should facilitate efforts to create these policies and procedures.

(b) Ensuring Robust Response: The capability to respond and recover from a CINS is critical to promoting the resiliency of critical infrastructure sectors. An all hazards operational response and recovery capability that brings government and the private sector together to coordinate activities involving events (whether potential or actual CINS) is needed. Existing operational capabilities for prevention, detection, response, and recovery (e.g., US-CERT) need additional resources to ensure that necessary enhancements are made. In addition, new capabilities are needed to ensure effective communication and reconstitution of data, services, and networks.

4. What factors make private/public working groups more or less effective in planning for or responding to major Internet disruptions?

Many of the impediments (described in our answer to Questions #1) have made public/private working groups less effective. DHS has consistently prepared plans and reports without first seeking industry input; trust has not effectively been established between the public and private sector; proper roles and responsibilities have not been delineated; and manageable, pointed plans for next steps have not been carried out or implemented. Ineffective partnerships result in ineffective planning and response.

As the GAO report noted, creating a trusted environment for information sharing among the private sector will lead to stronger and more organized working groups. Currently, the lack of defined specific needs of DHS, the uncertainty of what information is needed, how it will be used, and who or what entities will have access to it all prevent proper, trusted information sharing. And without proper, trusted information sharing, neither the government nor the private sector has the proper tools, ideas, or strategies that will lead to effective planning for or response to major Internet disruptions.

Congress' Role: Congress can oversee the progress of breaking down these boundaries and minimizing these risks by holding oversight hearings, and requesting progress reports from both DHS and from established public-private working groups. Specifically, Congress should request updates from DHS and industry to report on progress toward achieving top objectives such as:

- **Increase Leadership:** The assistant secretary for cyber security and telecommunications should crystallize and take steps toward achieving key priorities
- **Sponsor Prevention and Mitigation Programs:** DHS should establish programs that aim to prevent or minimize a major cyber disruption, such as greater focus on research and development (R&D) and viable uses of private-sector insurance coverage for cyber attacks
- **Establish an Early Warning System:** There are similar warning mechanisms in place, such as the Information Sharing and Analysis Centers (ISACs), but we still lack a federally-supported, formal system that provides rapid and clear indication that an attack is underway and alerts all key stakeholders. DHS should support the ISACs and ensure that a more holistic system is put into place.
- **Institute Command and Control Procedures:** DHS should work with industry to establish a clear "chain of command" in the case of massive failure of information technology systems, either due to a cyber attack or natural disaster. There are critical questions to be answered such as: what defines an incident of national significance? which government agencies should be involved? which private sector entities? what is the legal significance of such a declaration?
- **Articulate an Emergency Communications System:** DHS should ensure that we have a resilient communications system in place to execute command and control in the case of a major cyber disruption. Such a system will need to work even when telecommunications and Internet connectivity are unavailable. This requires processes and protocols to communicate reliably and effectively and advance identification of the key stakeholders who need access to the emergency communications systems in order to perform their recovery and reconstitution duties.
- **Create a National Information Assurance Policy:** A national policy is needed that outlines the key roles that relevant government agencies should play in the protection of our cyber infrastructure. While the establishment of a national information assurance policy is not solely the responsibility of DHS, it has a critical role to play in its development and implementation and its support of such a government-wide policy is needed.

RESPONSE FOR THE RECORD OF LARRY CLINTON, CHIEF OPERATING OFFICER, INTERNET SECURITY ALLIANCE

ANSWERS TO QUESTIONS RAISED BY THE HONORABLE JOHN DINGELL AT THE HEARING ON "CYBER SECURITY PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE, ECONOMY AND CONSUMERS" SEPTEMBER 13, 2006. SUBMITTED BY LARRY CLINTON, CHIEF OPERATING OFFICER OF THE INTERNET SECURITY ALLIANCE

1. What are the risks and benefits of the private sector sharing information with the Department of Homeland Security?

As was the case of 9/11 and after hurricane Katrina, industry will generally sweep aside long standing concerns and provide whatever assistance the government needs, information or otherwise, in times of crisis.

I doubt this will ever change.

However, cyber security is more than crisis management. It is an ongoing fight fueled by thousands of attacks on the system every day. A reliable and sustainable system of defense must be established.

Industry has often remarked, through a variety of fora, that information sharing with the government is critical to the maintenance of the Internet in cases of Cyber Incidents of National Significance (CINS).

Industry needs prompt, reliable and actionable information about significant impending threats as well as an ongoing flow of information to address the steady stream of threats and incidents that occur every day.

Moreover, industry and government need to share information on a regular basis to address the thousands of attacks the Internet experiences every day. It is also these chronic attacks, not just the prospect of an acute CINS, which drive the need for a reliable exchange of information between the government and industry.

For the relationship between industry and government to operate in the most efficient manner, cyber defense requires a far greater degree of trust.

Much of the risk industry perceives in sharing information with DHS has to do with uncertainty:

What is a CINS, specifically?

What are the roles and responsibilities to share information (as well as other tasks) between industry and government in case of a CINS, specifically?

How can industry be sure that information it provides the government will not be misused?

Why are so many government requests placed on such short timelines? And why so often are there no clear explanations as to what the information requested will be used for, even post facto?

The lack of trust in the current relationship between government and industry is the prime impediment to more efficient and effective information sharing.

2. What changes could DHS make in building its working relationships with private sector information technology and communications companies and major industrial users of the Internet?

First, it should be noted that there is general consensus within the IT and Communications communities that there has been substantial progress made in improving the relationship between DHS and these sectors over the past year and a half.

The Internet Security Alliance, in conjunction with the National Cyber Security Partnership, organized an off-sight meeting with DHS and numerous other government agencies in the fall of 2005 (called "Wye II") which highlighted a wide variety of issues that needed to be addressed along these lines.

Many of these issues have been, at least initially, addressed.

In particular, DHS has demonstrated willingness to bring the private sector into its planning process at a far earlier time period than previously.

In addition, DHS has shown some willingness to actually develop plans in conjunction with the private sector rather than developing their own plan and putting it out for comment. The latter process often resulted in little more than lip service.

These attitude changes have led to improvements in the recently published NIPP and appear at this stage to be evident in the drafting of the Sector Specific Plans as well.

However, the "Wye II" process also produced a list of items that could still be addressed more comprehensively. Among the recommendations to come out of the Wye II process are those quoted below:

- The partnership's objectives must be clearly defined and embody common goals
- Institutionalized processes are important to provide lasting benefits
- The partnership needs to be an evolving relationship
- The partnership needs champions and institutional support
- Working members of the partnership should interact frequently
- The partnership should build on existing organizations and mechanisms first; while people may come and go, the institution remains
- Legal and liability issues can be powerful tools that may *align* the interests of the partners; legal issues can be points upon which cohesion can be built

3. Describe (a) the involvement of private sector firms in the development of the National Infrastructure Protection Plan and your views on the effort to develop this plan and (b) the involvement of firms in the ongoing development of the It Sector Specific plan in response to the NIPP and your views on the process by which the sector specific plan is being developed.

As stated above, the NIPP process was generally seen as a major step forward in the development of a real partnership between the government and the IT and Communications sectors.

In addition to the process improvements I have already referred to, there were some substantial policy directions articulated that are very promising.

One principle example is the NIPP's articulation of the need to develop a value proposition for industry as part of the NIPP.

Clearly, companies will do what they perceive in their own corporate interest to protect their information systems. And as stated above, they have proven willing to go the extra mile(s) needed in time of crisis.

But Cyberspace is a shared space, and there are likely gaps between what the government feels it needs to defend it and what is automatically done via convenient corporate self-interest.

It is vital to identify any such gaps and provide a value proposition for industry to fill them in, because they are, by definition, beyond what they will do in their own corporate interest. The NIPPs recognition and commitment to developing this value proposition is a critical element in developing the sort of partnership that will create an effective and sustainable cyber defense.

As to the Sector Specific Plans, apart from some of the process improvements, there remains substantial issues that are still being addressed (we are just over the half way mark in the process at this writing).

In general, there are still a number of key issues that lack definition. The required delineation of roles and responsibilities are currently lacking. The question of resources has not been directly addressed and there has not been ample time to fully integrate the wide range of companies into the process which attempts to deal with extremely complicated problems.

These and other issues have been commented on in the current developmental drafts and we can only hope there will be acceptable progress by the Congressionally imposed deadline---which may have been overly optimistic in light of the difficulty of the task.

After all, the important thing is to get these plans right in terms of effectiveness, sustainability and real world practicality.

4. What factors make private/public working groups more or less effective in planning for or responding to major internet disruptions.

There are many factors that relate to the effectiveness of these efforts but the most important are:

A) The tendency to try to do too much and force a "regulatory fix" of the problem; and
B) The lack of resources devoted to planning efforts; and
C) Needed basic research is not funded.
D) In point of fact, we already know a great deal about good cyber defense. Large independent studies tell us that the corporations that engage in best security management (not necessarily technical) practices have great success in preventing, mitigating and recovering from attacks. If the IT SSP would simply start with encouraging the 75% of US corporations who do not currently follow these practices to do so (probably by reaching out directly to senior executives) real progress in overall cyber defense could be made rather quickly. Instead, we have a plethora of random programs and consultant driven grand schemes geared toward regulatory solutions that cannot possibly work.
E) Almost all of the private sector efforts in cyber security that I am familiar with are being done by a small cadre of volunteers from the private sector. There is virtually no money available for the sort of planning and practice that would engender long term cyber security, probably because such efforts are not glitzy enough. But clearly more priority driven funding is required.
F) The core protocols upon which the Internet is based are 30 years old. They were never designed with the current environment in mind and they are in need of a heavy lift of R&D. This is not something the private sector is ever going to do. It will require a government effort in cooperation with industry and academia similar to the SemaTech program of the 1980s.

RESPONSE FOR THE RECORD OF THE HON. GEORGE W. FORESMAN, UNDER SECRETARY OF PREPAREDNESS, U.S. DEPARTMENT OF HOMELAND SECURITY

Questions from Representative John Dingell

1. After more than a year since announcing the position, I was pleased to see the appointment of a new Assistant Secretary for Cybersecurity shortly after our Committee's hearing.
Please describe how this new position will elevate the matter of cybersecurity and differ from the Acting Director position of the past two years. Specifically:

• What new resources, budget, and staff will the Assistant Secretary have, and how does that compare to the Acting Director's prior resources, budget, and staff?

Response: The Department of Homeland Security (DHS) is very pleased that Mr. Greg Garcia has been appointed the Assistant Secretary for Cyber Security and Telecommunications (CS&T). The position of Assistant Secretary reflects the importance of cyber security and communications to our homeland security and to the Department. Assistant Secretary Garcia comes to the Department with significant expertise and has the ability to focus resources for cyber security and communications in a manner that is consistent with our risk-based approach to homeland security.

In addition to the existing position of Director and Deputy Director of the National Cyber Security Division (NCSD), the staffing for the Assistant Secretary will include the following new positions: Deputy Assistant Secretary for CS&T, Chief of Staff, and an executive assistant. DHS is working expeditiously to fill these positions.

With respect to CS&T budget and resources, the Assistant Secretary will continue to leverage and expand collaborative efforts with cyber security and communications stakeholders and will be working under the President's Budget for Fiscal Year 2007. Additional needs will, of course, be evaluated as part of ongoing budget development.

• What new authorities does the Assistant Secretary have, and how does that compare to the Acting Director's prior authorities?

Response: The Assistant Secretary for CS&T occupies an elevated tier within the DHS organizational structure and reports directly to the Under Secretary for Preparedness, whereas the Acting Director reported to the Acting Assistant Secretary for Cyber Security and Telecommunications. The Assistant Secretary will continue to operate under the *National Strategy to Secure Cyberspace*, Homeland Security Presidential Directive 7, and the National Infrastructure Protection Plan. In addition, the Assistant Secretary has both a mandate for integrating cyber security related to national security and emergency preparedness (NS/EP), as well as communications needs for Federal, State, local and tribal governments and private industry, including mandates

outlined in Executive Order 12472. Moreover, with the recent enactment of the DHS Appropriations Act for Fiscal Year 2007, the Assistant Secretary will also be responsible for the new Office of Emergency Communications established in Subtitle D of the Act.

• What new levels of access to senior decision makers within the Department will the Assistant Secretary have, and how does that compare to the Acting Director's prior level?

Response: The Assistant Secretary joins the DHS senior leadership participating in high level Departmental decisions. He reports to the Under Secretary for Preparedness. Previously, the Acting Director of NCSD reported to the Acting Assistant Secretary for Cyber Security and Telecommunications, who in turn reported to the Under Secretary for Preparedness. One of my key responsibilities is to enable effective discussion and decision-making on key issues. As such I will ensure Mr. Garcia is both actively and intimately engaged.

• What new programs, initiatives, or operations will the Assistant Secretary be launching that were not contemplated or designed under the Acting Director? Will any programs or initiatives that the Acting Director was administering be discontinued under the Assistant Secretary?

Response The Assistant Secretary has responsibility for NCSD, the National Communications System (NCS), and the new Office of Emergency Communications. The Assistant Secretary is currently conducting program reviews within CS&T. Once the Assistant Secretary has had an opportunity to fully evaluate the depth and breadth of existing programs, initiatives, and operations, he will make programmatic adjustments as necessary. We will, of course, engage Congress as appropriate in these actions.

2. Following the release of the National Infrastructure Protection Plan (NIPP), the Department is charged with assuring that each of the critical infrastructure sectors develops a sector-specific plan.

• What, specifically, are these plans supposed to yield? For example, will they be emergency blueprints? Will they be overall strategic plans as to how corporations should organize and perform ongoing security operations?

Response: The release of the final NIPP Base Plan formalized a framework for assessing and addressing the risk to our national critical infrastructure in a public/private partnership. The implementation of the NIPP and the accompanying 17 Sector Specific Plans (SSPs) will help build a safer, more

secure, and more resilient America by enhancing protection of the Nation's Critical Infrastructure and Key Resources (CI/KR).

Based on guidance from DHS, SSPs are developed jointly by Sector-Specific Agencies (SSAs) in close collaboration with Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and others, including State, local and tribal homeland security partners with key interests or expertise appropriate to the sector. The SSPs provide the means by which the NIPP is implemented across all sectors and each SSP is tailored to address the unique characteristics and risk landscapes of the 17 CI/KR sectors.

The objective of the SSP is to outline each sector's unique implementation of the NIPP risk management framework. It will also provide a statement of security goals and objectives and identify initiatives to meet these goals. Lastly, it will identify resources needs and performance metrics for ensuring that the goals can be met which will be sustained by an ongoing process for coordinated private and public sector planning.

The SSPs are intended for long-term enhancement of CI/KR protection including proactive identification and management of risks. While enhancement of CI/KR protection may improve emergency response capabilities of all security partners, the SSPs are not emergency blueprints. Rather the SSPs describe each sector's unique implementation of the NIPP risk management framework, provide jointly developed public and private sector security goals and objectives; identify and align initiatives to meet these goals; and create an ongoing process for coordinated private and public sector planning.

The SSPs are strategic policy and planning documents that may include suggestions of best practices for security partners, but their primary purpose is to establish the framework for public and private partners to work together and align their respective efforts to protect the Nation's CI/KR.

• My understanding is that the Department is attempting to engage the private sector in the development of these plans. What is the specific degree of private sector participation in the IT/Communications Sector specific plan?

Response: The SSPs for both the Information Technology (IT) and Communications Sectors are currently under development with significant private sector participation. Within the NIPP construct, DHS is the Sector Specific Agency (SSA) responsible for both the IT and Communications Sectors. The SSA responsibility for the IT Sector is handled by NCSD within CS&T, which works closely with the IT-Sector Coordinating Council (IT-SCC). The SSA responsibility for the Communications Sector is handled by NCS within CS&T, which works closely with the Communications Sector Coordinating Council (CSCC). Through these partnership arrangements, the Department is fostering robust working relationships with the private sector toward the development of SSPs.

DHS/NCSD has engaged the private sector in every aspect of the plan. There are approximately 7 working groups made up of SCC and GCC members engaged in identifying the basic principles and ideas for each chapter of the plan. Each of these working groups meets about once a week to review

comments and propose changes. The draft plan has been reviewed by the GCC and a large part of the SCC multiple times within the last two months.

The IT SCC was formally launched in January 2006 and is comprised of over thirty members from across the sector, including hardware, software, IT system and service providers. For the IT SSP, NCSD has been working closely with the IT SCC on the development of the plan. In anticipation of the final release of the NIPP Base Plan, the IT SCC and IT GCC held a joint meeting in May to develop a process for co-writing the IT SSP. A writing team was established, consisting of members from the IT GCC and IT SCC to ensure overall coordination of the IT SSP. This team developed a consensus outline for the IT SSP based on the SSP Guidance and then divided into working groups with members from both the IT GCC and IT SCC to collaboratively write each chapter of the plan. The writing team meets on a monthly basis to review and incorporate the chapter working groups' products into iterative drafts of the IT SSP. The collaborative and iterative process has ensured a coordinated plan with broad participation from both the public and private sectors.

DHS/NCS, has historically engaged with the private sector on many plans and initiatives. Their Sector Specific plan has been compiled from NCS' work and vetted to the private sector multiple times since as a draft. The private sector is engaging with NCS on methodologies and processes for the plan.

For the Communications SSP, the NCS initiated a series of meetings with the Communications Sector to coordinate NIPP activities and draft the Communications SSP in 2004. Working closely with DHS, the CSCC was established in May 2005, to work with the NCS on matters related to the NIPP, including: the identification of communication critical infrastructure and resources; critical infrastructure protection (CIP) policy issues; and drafting a sector specific plan. In addition, the CSCC seeks to foster and facilitate the coordination of sector-wide policy related activities and initiatives designed to improve both physical and cyber security of communication critical infrastructure. The CSCC is made up of communication owners and operators, and is led by an executive committee of corporate senior executives from wireline companies, wireless companies and the Telecommunications Industry Association.

3. The NIPP generally takes the laudable perspective of dealing with the largest needs first, but seems to be less clear when it begins to consider "awareness."

- Describe the Department's vision of "awareness" efforts, and how the Department plans to engage senior network operators in specific cybersecurity initiatives.

Response: The Department's vision is to improve situational awareness of the IT sector within normal operations and during significant threats and disruptions, intentional or unintentional incidents, crippling attacks (cyber or physical) against IT Sector infrastructure, technological emergencies and/or failures, and Presidentially declared disasters. In order to realize this mission, the IT sector and the government need to collaborate, develop, and share

appropriate threat and vulnerability information more efficiently. When completed, the SSP will establish the mechanisms through which the Department can engage all stakeholders regarding cyber security initiatives. HITRAC has also just announced a program to hire private sector critical infrastructure experts to collaborate with DHS Intelligence and Infrastructure Protection analysts on the Department's sector assessments and related products.

The NIPP addresses the importance of awareness towards its overall goal of building a safer, more secure, and more resilient America by enhancing the protection of the Nation's CI/KR and strengthening national preparedness. As such, the NIPP Base Plan highlights the need to build national awareness to support CI/KR protection, related protection investments, and associated protection activities by ensuring a focused understanding of the threat environment.

With respect to cyber security, the Department's vision of "awareness" efforts is based on Priority III of the *National Strategy to Secure Cyberspace*, "A National Cyberspace Security Awareness and Training Program". The *Strategy* calls for promoting a comprehensive national awareness program to empower all Americans, including the business community, the general workforce, and the general population, to secure their own parts of cyberspace. NCSD maintains an Outreach and Awareness program that includes working with stakeholders to raise the cyber security awareness of the general public. NCSD works with the National Cyber Security Alliance (NCSA) to reach home users, small businesses, and all levels of students. NCSD also works with the Multi-State ISAC (MS-ISAC) to enhance cyber security awareness among state information security professionals and the general public. In collaboration with NCSA and the MS-ISAC, NCSD promotes the annual National Cyber Security Awareness Month, which occurs each October. This year, the National Cyber Security Awareness Month initiatives included all fifty states and promoted cyber security awareness to approximately 75 million Americans through TV, radio, print, web and other media. Key programs also included Congressional outreach, educational webcasts for 4th and 5th graders, and, a Small Business Workshop Series.

With respect to engaging senior network operators in specific cyber security initiatives, the Department engages in a number of activities. For example, the United States Computer Emergency Readiness Team (US-CERT) established the Government Forum of Incident Response and Security Teams (GFIRST), which makes up the government's critical group of cyber first responders. GFIRST meets regularly, and DHS has hosted two GFIRST conferences to enhance information sharing and collaborative efforts to secure government cyberspace. With respect to the private sector, US-CERT has established working relationships with a number of groups representing network operators, including the Information Technology Information Sharing and Analysis Center (IT-ISAC), the North American Incident Response Group, and the North American Network Operators' Group (NANOG).

• In terms of spending priorities, how much money is the Department devoting to reaching out to the senior executives who control much of our Nation's IT/communications infrastructure?

Response: The overall budget for NCSD is $92,000,000, and the budget for NCS is $143,272,000. Outreach and collaboration with the private sector is a key component of nearly all cyber security and communications programs and related activities. Significant examples include the following:

- The NCSD coordinates with the IT-Sector Coordinating Council (IT-SCC) and IT-ISAC. In each of its program areas, as a lead for the IT Sector, NCSD's activities involve senior executives on control systems security, software assurance, and Internet disruption.
- Similarly, NCS engages senior executives in the Communications Sector through the Communications Sector Coordinating Council (CSCC), the National Coordinating Center for Communications (NCC), and the Communications Information Sharing and Analysis Center (ISAC).
- The NCS serves as the executive secretariat for the President's National Security Telecommunications Advisory Committee (NSTAC). The NSTAC, made up of up to 30 Chief Executive Officers (CEOs) and other senior executives in the Communications Sector, provides advice to the President on communications matters. DHS works closely with the NSTAC on a wide range of NS/EP, CIP, and response and recovery issues.

4. The NIPP encourages the private sector to implement recommendations in the National Strategy to Secure Cyber Space. At our hearing, witnesses from the private sector indicated that a series of incentive programs would be critical to create the necessary effect, and the Government Accountability Office supported these comments. Does the Department recommend any specific measures to develop the sort of incentive plans alluded to in the NIPP?

Response: DHS recognizes that the private sector makes cyber security risk management decisions based on the return on investment, including ensuring business continuity. Market-based incentives for cyber security investments include protection of intellectual capital, security influenced procurement, market differentiation, and public confidence.

The private sector acknowledges that there must be collaborative approach with the Federal Government to secure cyberspace. DHS is committed to working closely with the private sector to ensure that this partnership increases overall preparedness. The NIPP value proposition is based on sharing the responsibility of cyber security with industry and State and local governments, and DHS believes that this cooperation will help encourage all parties to take the proper steps to secure cyber assets. As CI/KR protection efforts mature, DHS will examine specific incentive programs tailored to each sector to encourage private sector participation in CI/KR protection.

5. GAO reports that the private sector has expressed concerns about the Department's ability to execute its plans and is reluctant to share information with the Department. Does the Department recommend any steps that can be taken to improve its working relationships with private sector information technology and communications companies?

Response: The Department relies heavily on its engagement with the private sector and has taken a number of steps to improve its working relationships with the private sector in general, specifically with information technology and communications companies.

The Department has taken significant measures to provide for a more conducive information sharing environment, including establishing and improving the Protected Critical Infrastructure Information (PCII) Program and, importantly, establishing the Critical Infrastructure Partnership Advisory Council (CIPAC) to provide for the public-private collaboration for the NIPP framework. The CIPAC encompasses all seventeen critical infrastructure sectors and facilitates the information sharing and collaborative environment needed to implement the NIPP.

In addition to these measures, the Department continues to build its working relationships with information technology and communications companies through collaboration with the IT-SCC and CSCC. Furthermore, NCSD/US-CERT and NCS/NCC strive to provide the analysis and information aggregation functions that enable timely and actionable dissemination of information to the private sector, including the IT-ISAC and the Communications ISAC. The continued enhancement of the information sharing process through collaboration between the Department and the private sector helps to build a working partnership which allows critical information to flow efficiently between all stakeholders.

○