AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBERSECURITY: ASSESSING THE IMMEDIATE THREAT TO THE UNITED STATES

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, HOMELAND DEFENSE AND FOREIGN OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 25, 2011

Serial No. 112–55

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

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

U.S. GOVERNMENT PRINTING OFFICE

70–676 PDF WASHINGTON : 2011

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana
JOHN L. MICA, Florida
TODD RUSSELL PLATTS, Pennsylvania
MICHAEL R. TURNER, Ohio
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
CONNIE MACK, Florida
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
ANN MARIE BUERKLE, New York
PAUL A. GOSAR, Arizona
RAÚL R. LABRADOR, Idaho
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
JOE WALSH, Illinois
TREY GOWDY, South Carolina
DENNIS A. ROSS, Florida
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas
MIKE KELLY, Pennsylvania

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
EDOLPHUS TOWNS, New York
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
DANNY K. DAVIS, Illinois
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
CHRISTOPHER S. MURPHY, Connecticut
JACKIE SPEIER, California

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
ROBERT BORDEN, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, HOMELAND DEFENSE AND FOREIGN OPERATIONS

JASON CHAFFETZ, Utah, *Chairman*

RAÚL R. LABRADOR, Idaho, *Vice Chairman*
DAN BURTON, Indiana
JOHN L. MICA, Florida
TODD RUSSELL PLATTS, Pennsylvania
MICHAEL R. TURNER, Ohio
PAUL A. GOSAR, Arizona
BLAKE FARENTHOLD, Texas

JOHN F. TIERNEY, Massachusetts, *Ranking Minority Member*
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
STEPHEN F. LYNCH, Massachusetts
MIKE QUIGLEY, Illinois

CONTENTS

	Page
Hearing held on May 25, 2011	1
Statement of:	
McGurk, Sean, Director, National Cybersecurity & Communications Integration Center, U.S. Department of Homeland Security; Phillip Bond, president, TechAmerica; James A. Lewis, director, Technology and Public Policy Program, Center for Strategic and International Studies; and Dean Turner, director, Global Intelligence Network, Symantec Corp.	9
Bond, Phillip	23
Lewis, James A.	24
McGurk, Sean	9
Turner, Dean	33
Letters, statements, etc., submitted for the record by:	
Chaffetz, Hon. Jason, a Representative in Congress from the State of Utah, prepared statement of	4
Lewis, James A., director, Technology and Public Policy Program, Center for Strategic and International Studies, prepared statement of	26
McGurk, Sean, Director, National Cybersecurity & Communications Integration Center, U.S. Department of Homeland Security, prepared statement of	12
Turner, Dean, director, Global Intelligence Network, Symantec Corp., prepared statement of	35

CYBERSECURITY: ASSESSING THE IMMEDIATE THREAT TO THE UNITED STATES

WEDNESDAY, MAY 25, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, HOMELAND DEFENSE AND FOREIGN OPERATIONS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 3 p.m. in room 2157, Rayburn House Office Building, Hon. Jason Chaffetz (chairman of the subcommittee) presiding.

Present: Representatives Chaffetz, Labrador, Tierney, Quigley and Kucinich.

Staff present: Ali Ahmad, deputy press secretary; Thomas A. Alexander, senior counsel; Molly Boyl, parliamentarian; Kate Dunbar, staff assistant; Mitchell S. Kominsky, counsel; John Ohly and Tim Lewis, professional staff members; Kevin Corbin, minority staff assistant; Scott Lindsay and Carlos Uriarte, minority counsels; and Amy Miller, minority professional staff member.

Mr. CHAFFETZ. The subcommittee will come to order.

Good afternoon and welcome to today's hearing, Cybersecurity: Assessing the Immediate Threat to the United States.

We appreciate your patience and understanding as we had votes earlier. I know we are getting off to a delayed start, but I appreciate you all being here and participating.

Welcome, Ranking Member Tierney and members of the subcommittee. I appreciate everybody being here today.

Today's hearing is designed to act as a prelude to the full committee hearing which will be conducted a week later on June 1st, just a short time from now. It is entitled, "Cybersecurity: Assessing the Nation's Ability to Address the Growing Cyber Threat."

During today's hearing, the subcommittee is scheduled to receive testimony from the administration, industry and civilian cyber threat experts, all of whom will likely state that cyber-related intrusions pose one of the greatest threats to our national security.

The intent is to obtain detailed information from various sources and from various perspectives as to what the current threat actually entails so the committee can later delve more deeply into how effective the Nation has been in confronting the immediate cyber threat as well as building defenses which safeguard us from what appears to be a daunting future cyber-security environment.

Given the unusual nature of the cyber threat, it cannot be addressed solely by using the traditional national security apparatus. In short, the Federal Government is currently incapable of securing

the Nation against cyber threats on its own and must embrace the broad, transparent involvement of non-government entities.

Like other countries, approximately 85 percent of the Nation's critical infrastructure is owned by the private sector—many of which are small businesses. Because the Nation relies so heavily on private industry to protect this infrastructure, trusted partnerships between the government and the private sector must also be a priority.

In the words of the President, "Cybersecurity is a challenge that we as a government or as a country are not adequately prepared to counter." In addition, in a recent interview, Howard Schmidt, the U.S. Cybersecurity Coordinator, emphasized the critical nature of public-private partnerships as it relates to cybersecurity.

Unfortunately, Mr. Schmidt refused to testify today. I truly do find this unfortunate because I believe he should be here in this important discussion. I am deeply concerned that Mr. Schmidt, as the executive branch's Cybersecurity Coordinator, charged with the responsibility for "orchestrating the many important cybersecurity activities across the government," believes that his management of this critical issue is exempt from congressional oversight. That is certainly inconsistent with what I have heard the administration and this President say about the openness and transparency of the administration.

In his absence, the administration sent to us an expert from the Department of Homeland Security. There was quite a debate whether the administration would allow him to sit on the same panel as the industry experts sitting in front of us today. I am glad the issue was resolved, in a matter of a few hours ago and we will now be able to receive testimony from both the public and private perspective together on one panel. In the future, I hope this is not so difficult.

That said, I must stress my sincere disappointment in the number of days waste debating the need to hear testimony from government and private witnesses alike at the same time on the same panel in a manner that allows Members to most effectively oversee this critical public/private partnership.

I believe it is critical that while we focus on the cyber threat, we also keep in mind the need to develop well coordinated, strategic cybersecurity partnerships with the private sector in order to confront the threat. The administration has made repeated public statements about the importance of this partnership. Even the White House-directed cyberspace policy review concluded that the United States cannot succeed in securing cyberspace if it works in isolation and should enhance its partnerships with the private sector.

Cybersecurity experts agree that given the likely national security impact of cyber attacks on the economy, our critical infrastructure such as transportation, energy and communications, both private and public sectors must work together closely and in a very transparent way. This would also appear to be in line with the President's stated commitment to "create an unprecedented level of openness in government" and "to establish a system of transparency, public participation and collaboration."

The ever changing face of the cyber threat means that the authorities and capabilities needed to confront the threat will likely need to be changed or updated on a regular basis. This is the reason why Congress must be as attentive to the threat as any other part of the government. I do not believe anybody knowledgeable of cyber security would deny that cyber threat is a major national security issue for the United States.

The National Security Strategy published in May 2010 highlights that cyber security threats represent one of the most serious national security, public safety and economic challenges we face as a Nation. Therefore, a national dialog in securing the Nation's digital infrastructure must happen now and continue indefinitely.

It is my sincere hope that this dialog can include many segments of society and can be done in a nonpartisan way. It is my hope that we as a Nation bring to bear against this threat all expertise that resides within the country. Strangely, we are faced with the critical national security threat to which the expertise needed to confront it does not necessarily reside solely in the Federal Government but also in the private sector.

A recent research project conducted by McAfee and the Center for Strategic and International Studies looked at the threats to power grids, oil, gas and water across 14 countries. It concluded that there had been dramatic increases in cyber attacks against critical infrastructure with as much as 80 percent of the companies experiencing "large scale attacks."

According to the project report, nearly 30 percent of the companies believed they were unprepared for the attack and more than 40 percent expected a major cyber attack within the next 12 months. Also, according to an Office of Management and Budget report, the number of reported cyber incidents affecting U.S. Federal agencies shot up 39 percent in 2010, approximately 41,776 reported attacks, up from roughly 30,000 the year before.

I am positive the witnesses will elaborate on the threat and I look forward to hearing from the panel.

[The prepared statement of Hon. Jason Chaffetz follows:]

5/25/2011

Subcommittee on National Security, Homeland Defense, and Foreign Operations hearing:

"Cybersecurity: Assessing the Immediate Threat to the United States."

Good afternoon and welcome to today's hearing: "Cybersecurity: Assessing the Immediate Threat to the United States."

Welcome Ranking Member Tierney and members of the Subcommittee. Thanks for being here today.

Today's hearing is designed to act as a prelude to the full Committee hearing which will be conducted a week later on June 1, 2011, titled "Cybersecurity: Assessing the Nation's Ability to Address the Growing Cyber Threat."

During today's hearing, the Subcommittee was scheduled to receive testimony from the Administration, industry and civilian cyber threat experts, all of whom would likely state that cyber-related intrusions pose one of the greatest threats to our national security. The intent was to obtain detailed information from various sources and from various perspectives as to what the current threat actually entails, so that the Committee can later delve more deeply into how effective the Nation has been in confronting the immediate cyber threat as well as building defenses which safeguard us from what appears to be a daunting future cybersecurity environment.

Given the unusual nature of the cyber threat, it cannot be addressed solely by using the traditional national security apparatus. In short, the federal government is currently incapable of securing the Nation against cyber threats on its own and must embrace the broad, transparent involvement of non-government entities.

Like in other countries, approximately 85 percent of the nation's critical infrastructure is owned by the private sector – many of which are small businesses. Because the nation relies so heavily on private industry to protect this infrastructure, trusted partnerships between the government and the private sector must be a priority.

In the words of the President, "cybersecurity is a challenge that we as a government or as a country are not adequately prepared to counter." In addition, in a recent interview, Howard A. Schmidt, the U.S. Cybersecurity Coordinator, emphasized the critical nature of public-private partnerships as it relates to cybersecurity.

Unfortunately, witnesses such as Mr. Schmidt refused to testify today.

I am deeply concerned that Mr. Schmidt, as the Executive Branch's Cybersecurity Coordinator, charged with the responsibility for "orchestrating the many important cybersecurity activities across the government," believes that his management of this critical issue is exempt from Congressional oversight.

In his absence, the Administration offered to send two experts from the Department of Homeland Security, but would not allow them to sit on the same panel as the experts sitting in front of us today. This action seems in stark contradiction to the Administration's repeated public statements about the importance of public/private partnerships. Even the White House directed Cyberspace Policy Review concluded that the United States cannot succeed in securing cyberspace if it works in isolation and should enhance its partnerships with the private sector.

Cybersecurity experts agree that given the likely national security impact of cyber attacks to the economy and our critical infrastructure such as transportation, energy and communications, both private and public sectors must work together closely and in a transparent way. This would also appear to be in line with the President's stated commitment "to create an unprecedented level of openness in Government" and "to establish a system of transparency, public participation, and collaboration." However, the fact that we are hearing from only non-government witnesses today makes me question the Administration's commitment to public participation.

The ever-changing face of the cyber threat means that the authorities and capabilities needed to confront this threat will likely need to be changed or updated on a regular basis. This is the reason why Congress must be as attentive to the threat as any other part of the Government.

I do not believe anybody knowledgeable of cybersecurity would deny that the cyber threat is a major national security issue for the United States. The National Security Strategy, published in May 2010, highlights that cybersecurity threats

represent one of the most serious national security, public safety, and economic challenges we face as a nation. Therefore, a national dialogue on the securing the Nation's digital infrastructure must happen now and continue indefinitely.

It is my sincere hope that this dialogue can include all segments of society and can be done in a non-partisan way. It is also my hope that we as a nation bring to bear against this threat all expertise that resides in this country. Strangely, we are faced with a critical national security threat to which the expertise needed to confront it does not necessarily reside solely in the Federal government, but also in the private sector.

A recent research project conducted by McAfee and the Center for Strategic and International Studies looked at the threats to power grids, oil, gas and water across 14 countries. It concluded that there had been a "dramatic" increase in cyber attacks against critical infrastructure, with as much as 80 percent of the companies experiencing a "large-scale attack." According to the project report, nearly 30 percent of the companies believed they were unprepared for the attack and more than 40 percent expected a major cyber attack within the next year.

Also, according to an Office of Management and Budget report, the number of reported cyber incidents affecting U.S. federal agencies shot up 39 percent in 2010, approximately 41,776 reported attacks, up from 30,000 the year before.

I am positive that the witnesses will elaborate on the threat, so I look forward to hearing from the panel.

Mr. CHAFFETZ. I will now recognize the distinguished ranking member, the gentleman from Massachusetts, Mr. Tierney, for his opening statement.

Mr. TIERNEY. Thank you, Chairman Chaffetz, for convening this hearing today. Thank you to our witnesses for agreeing to testify.

I particularly want to thank the administration's witnesses here today, Sean McGurk, the Director of the Control Systems Security Program at the Department of Homeland Security's National Cyber Security Division. Mr. McGurk has agreed to testify before the subcommittee on very short notice and during a week in which the Department of Homeland Security will testify at five different cybersecurity hearings, including a similar hearing held this morning.

Next week, the full committee is going to hold another hearing on cybersecurity featuring four different senior-level administration witnesses to discuss the administration's comprehensive legislative proposal to improve cybersecurity with a focus on our Nation's critical infrastructure and the Federal Government's own networks and computers.

The proposal was drafted in response to numerous legislative proposals introduced in the last Congress and specific requests from congressional leadership. That White House legislation won't be the focus of today's hearing, but is still a much needed starting point for very important conversation.

As someone who doesn't purport to be a techie at all, I can tell you I have a great deal of concern about the exposure we have in this area, particularly having served a number of years on the Intelligence Committee and where that conversation goes should cause some sleepless nights for a lot of people.

As computer technology has advanced, Federal agencies and our Nation's critical infrastructure, such as power distribution, water supply, telecommunications and emergency services, have all become increasingly dependent on computerized information systems to carry out their operations and to process, maintain and report essential information.

Public and private organizations increasingly rely on computer systems to transfer money and sensitive and proprietary information, conduct operations and deliver services. The interconnected nature of these systems creates risks for our national security, economic security and public safety.

Just last month, in Massachusetts, a virus called "W32.QAKBOT" was discovered on computers at the Executive Office of Labor and Workforce Development. As a result, the Labor Department said as many as 210,000 unemployed workers may have had data compromised, including their names, social security numbers, employer identification numbers, addresses and email addresses.

Although the virus was originally discovered back in April, it wasn't until last week that the Labor Department realized the virus had survived its early eradication efforts and results in a data breach. That specific example happened at a State government agency, but highlights the potential threat to Americans across the country if our Federal computer networks are not adequately protected.

As many commentators have documents, cyber attacks on our Federal IT systems are on the rise. The chairman just went through the numbers on that. It is becoming increasingly clear that current efforts to counteract the attacks are woefully insufficient.

The connectivity between information systems, the Internet and other infrastructures also creates opportunities for attackers to disrupt telecommunications, electrical power and other critical services. Some industry sectors are so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security or public health and safety.

Federal law enforcement and intelligence agencies have identified multiple sources of threats to our information systems and our critical infrastructure. These threats include foreign nations engaged in espionage and information warfare, criminals, hackers, disgruntled employees and contractors. In one recent example, it has been alleged that the Chinese Government spread a virus that attacked Google and at least 80 other U.S. companies.

Not all threats to Federal cybersecurity are external. In June 2010, Wikileaks released thousands of classified Department of State and Department of Defense documents. Immediately following the release of those documents, the Secretary of Defense commissioned two internal Department of Defense studies to evaluate any weaknesses in their systems.

The studies found that the Department's policies for dealing with an internal security threat were inadequate and that the Department had limited capability to detect and monitor anomalous behavior on its classified computer networks.

These examples simply underline the need for a comprehensive legislative approach that will protect our national security and the health and safety of the American people. We have an obligation to ensure that the government's IT systems are secure and that any critical infrastructure is protected from the threat of a cyber attack. The failure to properly secure these networks could have dire consequences.

I look forward to this hearing and learning more about the threat landscape and the challenges we face in addressing this growing problem.

Again, I thank our witnesses and the chairman for bringing this hearing.

Mr. CHAFFETZ. Thank you.

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

We will now recognize the panel.

Mr. Sean McGurk is the Director of National Cybersecurity & Communications Integration Center at the U.S. Department of Homeland Security. Mr. Phillip Bond is the president of TechAmerica. Mr. James A. Lewis is the director, Technology and Public Policy Program at the Center for Strategic and International Studies. Mr. Dean Turner is the director, Global Intelligence Network Security Response at Symantec.

Again gentlemen, we appreciate your being here. I would like to recognize each of you for 5 minutes for an opening statement. If

you will try to keep it to 5 minutes, any additional information you want to provide we will submit to the record.

Pursuant to committee rule, all witnesses must be sworn before they testify. Please rise and raise your right hands.

[Witnesses sworn.]

Mr. CHAFFETZ. Let the record reflect that all witnesses answered in the affirmative.

We will now recognize Mr. McGurk for 5 minutes.

STATEMENTS OF SEAN MCGURK, DIRECTOR, NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER, U.S. DEPARTMENT OF HOMELAND SECURITY; PHILLIP BOND, PRESIDENT, TECHAMERICA; JAMES A. LEWIS, DIRECTOR, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES; AND DEAN TURNER, DIRECTOR, GLOBAL INTELLIGENCE NETWORK, SYMANTEC CORP.

STATEMENT OF SEAN MCGURK

Mr. MCGURK. Thank you, Chairman Chaffetz, Ranking Member Tierney and distinguished members of the committee. My name is Sean McGurk. I am the Director for the National Cybersecurity & Communications Integration Center [NCCIC]. Thank you for inviting me today to discuss this important issue along with this distinguished panel of experts on cyber threats and the impact on critical infrastructure.

As both the chairman and ranking member have already identified, sensitive information is routinely stolen from both government and private sector networks. Last year, we saw an increase in the threat as a result of not what was being taken from networks but what was being left behind in the result of what was known as Stuxnet.

Successful cyber attacks could potentially result in physical damage and loss of life. There are many challenges in the current landscape, strong and rapidly expanding capabilities, lack of comprehensive threat and vulnerability awareness and our information infrastructure is dependent upon its continual availability for our way of life.

The cyber environment is not homogenous under a single department or agency or the private sector. We recognize that cybersecurity is a team sport. Government does not have all the answers, so we must work closely with the private sector to provide solutions. There is no one size fits all and there is no magical line to protect the cyber domain. It is about information sharing and it is about sharing knowledge collectively. Knowledge is only power when it is shared. We must leverage our expertise and our access to information along with industry's specific needs, capabilities and timelines.

Each partner has a significant role to play and a unique capability in this environment. In my 34 years of experience, with over 28 years serving in the U.S. Navy, you learn that everyone has an ability to contribute. The mission in cyber is manyfold and our goals are clear.

In the law enforcement environment, they work closely with the other agencies to identify and prosecute cyber intrusions. The intelligence and military community work to attribute, to defend and to pursue those individuals. DHS, along with the private sector, including the financial services sector, the energy sector, communications and others, work to prepare, prevent, respond, recover and restore. Coordinating the national response to domestic emergencies is more of a matter of what and how and not necessarily of who and why until much later.

To that end, I would like to emphasize that my responsibilities from an operational standpoint are focused on preventing and resolving attacks, not attributing the source of those threats.

I would be willing to take any questions in the future regarding the cyber threats and the cyber capabilities of other countries with the committee under an appropriately classified setting with the available interagency representatives.

NCCIC or the National Cybersecurity & Communications Integration Center, works closely with government and all levels of the private sector to coordinate the integrated and unified response to cyber communications incidents. Sponsoring security clearances for the private sector enables us to have our industry partners on the watch floor in a classified environment looking at actionable intelligence and providing information to asset owners and operators in near real time.

The DHS components have all been integrated into the NCCIC along with representatives from other agencies such as the National Security Agency, U.S. Cyber Command, the FBI, the U.S. Secret Service, and representatives from the intelligence community at large. In addition, we have private sector representatives sitting on the watch floor from the communications sector, the IT sector, the financial services sector and the energy sector. Additionally, we have representatives from State, local, tribal and territorial governments represented by the Multistate Information Sharing and Analysis Center.

In conclusion, within our current legal authorities, we continue to engage, collaborate and provide analysis of vulnerability and mitigation assistance to the private sector. We have experience and expertise in dealing with the private sector in planning steady state and crisis scenarios. We have deployed numerous incident response teams and assessment teams that enable us to prevent, respond, recover and restore from cyber incidents.

Finally, we work closely with the private sector and our interagency partners in law enforcement and in the intelligence community to provide the full complement and capabilities of the Federal Government for the private sector in response to a cyber incident.

Chairman Chaffetz, Ranking Member Tierney and distinguished members of the panel, let me conclude by reiterating that I look forward to exploring opportunities to advance this mission in collaboration with the subcommittee and my colleagues in the public and private sector.

Also, if the committee has any questions regarding the administration's legislative proposal, I will be happy to defer those issues to the policy representatives testifying before the full committee next week.

Thank you again for this opportunity to testify and I would be happy to answer any of your questions.

[The prepared statement of Mr. McGurk follows:]

Statement for the Record
of
Department of Homeland Security

Before the
United States House of Representatives
Subcommittee on National Security, Homeland Defense and Foreign Operations
Of the Committee on Oversight and Government Reform
Washington, DC

May 25, 2011

Introduction
Chairman Chaffetz, Ranking Member Tierney, and distinguished Members of the Subcommittee, the Department of Homeland Security is extremely appreciative of your focus on cybersecurity. This testimony will provide an overview of the current cybersecurity environment, the cybersecurity mission carried out by the National Protection and Programs Directorate (NPPD), and the coordination of this mission with our public and private sector partners.

We look forward to exploring how we might work collaboratively with the Committee, and we applaud the Committee for holding this hearing as a step toward such important cooperation. Moving forward, we would like to work more closely with you to convey the relevance of cybersecurity to average Americans. Increasingly, the services we rely on for daily life, such as water distribution and treatment, electricity generation and transmission, healthcare, transportation, and financial transactions depend on an underlying information technology and communications infrastructure. Cyber threats put the availability and security of these and other services at risk.

The Current Cybersecurity Environment
The United States confronts a combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process and, as bad as the loss of precious national intellectual capital is, we increasingly face threats that are even greater. We currently cannot be certain that our information infrastructure will remain accessible and reliable during a time of crisis.

We face persistent, unauthorized, and often unattributed intrusions into Federal Executive Branch civilian networks. These intruders span a spectrum of malicious actors, including nation states, terrorist networks, organized criminal groups, or individuals located here in the United States. They have varying levels of access and technical sophistication, but all have nefarious

intent. Several are capable of targeting elements of the U.S. information infrastructure to disrupt, dismantle, or destroy systems upon which we depend. Motives include intelligence collection, intellectual property or monetary theft, or disruption of commercial activities, among others. Criminal elements continue to show increasing levels of sophistication in their technical and targeting capabilities and have shown a willingness to sell these capabilities on the underground market. In addition, terrorist groups and their sympathizers have expressed interest in using cyberspace to target and harm the United States and its citizens. While some have commented on terrorists' own lack of technical abilities, the availability of technical tools for purchase and use remains a potential threat.

In the virtual world of cyberspace, malicious cyber activity can instantaneously result in virtual or physical consequences that threaten national and economic security, critical infrastructure, public health and welfare, and confidence in government. Similarly, stealthy intruders can lay a hidden foundation for future exploitation or attack, which they can then execute at their leisure—and at their time of greatest advantage. Securing cyberspace requires a layered security approach. Moreover, securing cyberspace is also critical to accomplishing nearly all of DHS's other missions successfully.

In cyberspace, we need to ensure that the federal environments are secure and that legitimate traffic is allowed to flow freely while malicious traffic is prevented from penetrating our defenses. Similarly, we need to support our state and local government and private sector partners as they secure themselves against malicious activity. Collaboratively, public and private sector partners must use our knowledge of these systems and their interdependencies to prepare to respond should our defensive efforts fail. This is a serious challenge, and DHS is continually making strides to improve the nation's overall operational posture and policy efforts.

The DHS Cybersecurity Mission

The Department of Homeland Security is responsible for helping Federal Executive Branch civilian agencies secure their unclassified networks. DHS also works with owners and operators of critical infrastructure and key resources (CIKR) sectors—whether private sector, state, or municipality-owned—to bolster their cybersecurity preparedness, risk assessment and mitigation, and incident response capabilities. The Department has a number of foundational and forward-looking efforts under way, many of which stem from the 2008 Comprehensive National Cybersecurity Initiative (CNCI). We are reducing and consolidating the number of external connections federal agencies have to the Internet through the Trusted Internet Connections (TIC) initiative. Further, DHS continues to deploy its intrusion detection capability, known as EINSTEIN 2, to improve the security of communications entering or leaving the federal government through those TICs. In addition, through the United States Computer Emergency Readiness Team (US-CERT), we are working more closely than ever with our public and private sector partners to share what we learn from EINSTEIN 2 and to deepen our collective understanding, identify threats collaboratively, and develop effective security responses.

In a reflection of the bipartisan nature with which the federal government continues to approach cybersecurity, President Obama determined that the CNCI and its associated activities should evolve to become key elements of the broader national cybersecurity efforts. These CNCI initiatives play a central role in achieving many of the key recommendations of the President's

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Following the publication of those recommendations in May 2009, DHS and its components developed a long-range vision of cybersecurity for the Department and the nation's homeland security enterprise, which is encapsulated in the Quadrennial Homeland Security Review (QHSR). The QHSR provides an overarching framework for the Department and defines our key priorities and goals. One of the five priority areas detailed in the QHSR is safeguarding and securing cyberspace. Within the cybersecurity mission area, the QHSR identifies two overarching goals: to help create a safe, secure and resilient cyber environment; and to promote cybersecurity knowledge and innovation.

In alignment with the QHSR, Secretary Napolitano consolidated many of the Department's cybersecurity efforts under the National Protection and Programs Directorate (NPPD). The Office of Cybersecurity and Communications (CS&C), a component of NPPD, focuses on reducing risk to the nation's communications and information technology infrastructures and the sectors that depend upon them, as well as enabling timely response and recovery of these infrastructures under all circumstances. The functions and mission of the National Cybersecurity Center (NCSC) are now supported by CS&C. These functions include coordinating operations among the six largest federal cyber centers. CS&C also coordinates national security and emergency preparedness communications planning and provisioning for the federal government and other stakeholders. CS&C comprises three divisions: the National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System.

Teamwork—ranging from intra-agency to international collaboration—is essential to securing cyberspace. Simply put, the cybersecurity mission cannot be accomplished by any one agency; it requires teamwork and coordination. Together, we can leverage resources, personnel, and skill sets that are needed to accomplish the cybersecurity mission.

NCSD collaborates with federal government stakeholders, including civilian agencies, law enforcement, the military, the intelligence community, state and local partners, and private sector stakeholders, to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of civilian government and private sector critical infrastructures. NCSD also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and private sector constituents. To that end, NCSD carries out the majority of DHS' non-law enforcement cybersecurity responsibilities.

National Cyber Incident Response

The President's *Cyberspace Policy Review* called for "a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident." DHS coordinated the interagency, state and local government, and private sector working group that developed the National Cyber Incident Response Plan. The plan provides a framework for effective incident response capabilities and coordination among federal agencies, state and local governments, the private sector, and international partners during significant cyber incidents. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines. In September 2010, DHS hosted Cyber Storm III, a response exercise in which members of the domestic and international cyber incident response community addressed the scenario of a coordinated cyber event. During the event, the National

Cyber Incident Response Plan was activated and its incident response framework was tested. Based on observations from the exercise, the plan is in its final stages of revision prior to publication.

Cyber Storm III also tested the National Cybersecurity and Communications Integration Center (NCCIC)—DHS' 24-hour cyber watch and warning center—and the federal government's full suite of cybersecurity response capabilities. The NCCIC works closely with government at all levels and with the private sector to coordinate the integrated and unified response to cyber and communications incidents impacting homeland security.

Numerous DHS components, including US-CERT, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the National Coordinating Center for Telecommunications (NCC), are collocated into the NCCIC. Also present in the NCCIC are other federal partners, such as the Department of Defense (DoD) and members of the law enforcement and intelligence communities. The NCCIC also physically collocates federal staff with private sector and non-governmental partners.

By leveraging the integrated operational capabilities of its member organizations, the NCCIC serves as an "always on" cyber incident response and management center, providing indications and warning of imminent incidents, and maintaining a national cyber "common operating picture." This facilitates situational awareness among all partner organizations, and also creates a repository of all vulnerability, intrusion, incident, and mitigation activities. The NCCIC also serves as a national point of integration for cyber expertise and collaboration, particularly when developing guidance to mitigate risks and resolve incidents. Finally, the unique and integrated nature of the NCCIC allows for a scalable and flexible coordination with all interagency and private sector staff during steady-state operations, in order to strengthen relationships and solidify procedures as well as effectively incorporate partners as needed during incidents.

Providing Technical Expertise to the Private Sector and Critical Infrastructure
US-CERT provides remote and onsite response support and defense against malicious cyber activity for the Federal Executive Branch civilian networks. US-CERT also collaborates and shares information with state and local government, industry, critical infrastructure owners and operators, and international partners to address cyber threats and develop effective security responses.

In addition to specific mitigation work we conduct with individual companies and sectors, DHS looks at the interdependencies across critical infrastructure sectors for a holistic approach to providing our cyber expertise. For example, the electric, nuclear, water, transportation, and communications sectors support functions across all levels of government including federal, state, local, and tribal governments. Government bodies and organizations do not inherently produce these services and must rely on private sector organizations, just as other businesses and private citizens do. Therefore, an event impacting control systems has potential implications at all these levels, and could also have cascading effects upon all 18 sectors. For example, water and wastewater treatment, chemical, and transportation depend on the energy sector, and failure in one of these sectors could subsequently affect the operations of state, local, or even federal government.

NCCIC's operations are complemented in the arena of industrial control systems by ICS-CERT. The term "control system" encompasses several types of systems, including Supervisory Control and Data Acquisition (SCADA), process control, and other automated systems that are found in the industrial sectors and critical infrastructure. These systems are used to operate physical processes that produce the goods and services that we rely upon, such as energy, drinking water, emergency services, transportation, postal and shipping, and public health. Control systems security is particularly important because of the inherent interconnectedness of the CIKR sectors and their dependence on one another.

As such, assessing risk and effectively securing industrial control systems are vital to maintaining our nation's strategic interests, public safety, and economic well-being. A successful cyber attack on a control system could result in physical damage, loss of life, and cascading effects that could disrupt services. DHS recognizes that the protection and security of control systems is essential to the nation's overarching security and economy. In this context, as an example of the many related initiatives/activities, DHS—in coordination with the Department of Commerce's National Institute of Standards and Technology (NIST), the Department of Energy, and DoD—has provided a forum for researchers, subject matter experts and practitioners dealing with cyber-physical systems security to assess the current state of the art, identify challenges, and provide input to developing strategies for addressing these challenges. Specific infrastructure sectors considered include energy, chemical, transportation, water and wastewater treatment, healthcare and public health, and commercial facilities. A 2010 published report of findings and recommendations is available upon request.

ICS-CERT provides onsite support to owners and operators of critical infrastructure for protection against and response to cyber threats, including incident response, forensic analysis, and site assessments. ICS-CERT also provides tools and training to increase stakeholder awareness of evolving threats to industrial control systems.

A real-world threat emerged last year that significantly changed the landscape of targeted cyber attacks on industrial control systems. Malicious code, dubbed Stuxnet, was detected in July 2010. DHS analysis concluded that this highly complex computer worm was the first of its kind, written to specifically target mission-critical control systems running a specific combination of software and hardware.

ICS-CERT analyzed the code and coordinated actions with critical infrastructure asset owners and operators, federal partners, and Information Sharing and Analysis Centers. Our analysis quickly uncovered that this sophisticated malware has the ability to gain access to, steal detailed proprietary information from, and manipulate the systems that operate mission-critical processes within the nation's infrastructure. In other words, this code can automatically enter a system, steal the formula for the product being manufactured, alter the ingredients being mixed in the product, and indicate to the operator and the operator's anti-virus software that everything is functioning normally.

To combat this threat, ICS-CERT has been actively analyzing and reporting on Stuxnet since it was first detected in July 2010. To date, ICS-CERT has briefed dozens of government and

industry organizations and released multiple advisories and updates to the industrial control systems community describing steps for detecting an infection and mitigating the threat. As always, we attempt to balance the need for public information sharing while limiting the information that malicious actors may exploit.

Looking ahead, the Department is concerned that attackers could use the increasingly public information about the code to develop variants targeted at broader installations of programmable equipment in control systems. Copies of the Stuxnet code, in various different iterations, have been publicly available for some time now. ICS-CERT and the NCCIC remain vigilant and continue analysis and mitigation efforts of any derivative malware.

ICS-CERT will continue to work with the industrial control systems community to investigate these and other threats through malicious code and digital media analysis, onsite incident response activities, and information sharing and partnerships.

Protecting Federal Civilian Government Networks

In addition to its support of private sector owners and operators of infrastructure, DHS also collaborates with its partners to increase the security of Federal Executive Branch civilian agency networks. As part of the CNCI, DHS works with the Office of Management and Budget (OMB) to reduce and consolidate the number of external connections that federal agencies have to the Internet through the TIC initiative. This initiative reduces the number of potential vulnerabilities to government networks and allows DHS to focus monitoring efforts on limited and known avenues through which Internet traffic must travel. DHS conducts onsite evaluations of agencies' progress toward implementing TIC goals.

In conjunction with the TIC initiative, the EINSTEIN system is designed to provide the U.S. government with an early warning system for intrusions to Federal Executive Branch civilian networks, near real-time identification of malicious activity, and automated disruption of that malicious activity. The first iteration of EINSTEIN was developed in 2003 and automates the collection and analysis of computer network security information from participating agency and government networks to help analysts identify and combat malicious cyber activity that may threaten government network systems, data protection and federal communications infrastructure. The second phase of EINSTEIN, developed in 2008 as part of the CNCI, incorporates intrusion detection capabilities into the original EINSTEIN system. DHS is currently deploying EINSTEIN 2 to Federal Executive Branch civilian agency TIC locations and Networx Managed Trusted Internet Protocol Services (MTIPS) providers, which are private internet service providers that serve federal agencies, to assist them with protecting their computers, networks and information. EINSTEIN 2 has now been deployed at 15 of the 19 large departments and agencies who maintain their own TIC locations. Also, the four MTIPS providers currently provide service to seven additional federal agencies. In 2010, EINSTEIN 2 sensors registered 5.4 million "hits," an average of more than 450,000 hits per month or nearly 15,000 hits per day. A hit is an alert triggered by a predetermined intrusion detection signature that corresponds to a known threat. Each hit represents potential malicious activity for further assessment by US-CERT.

DHS is currently developing the third phase of the EINSTEIN system—an intrusion prevention capability which will provide DHS with the ability to automatically detect and disrupt malicious activity before harm is done to critical networks and systems. In advance of this development, DHS, in coordination with the National Security Agency (NSA), conducted the CNCI Initiative 3 Exercise. US-CERT successfully met the objectives of the CNCI Initiative 3 Exercise, including the successful deployment of one signature, scenario and countermeasure, and the demonstrated ability to share alert data with DoD. As a result of the countermeasures deployed during the exercise, US-CERT was successful in denying the entry of more than 36,473 potentially malicious threats into the federal agency customer's network infrastructure. The CNCI Initiative 3 Exercise advanced the potential capabilities of the EINSTEIN system by demonstrating defensive technology, sharing near real-time threat information with DoD for enhanced situational awareness, and providing a platform upon which an oversight and compliance process can be implemented for the evolving set of EINSTEIN capabilities. The Department's Privacy Office and its Office for Civil Rights and Civil Liberties carefully reviewed the exercise concept of operations, and the Privacy Office worked with US-CERT to publicly release a detailed Privacy Impact Assessment evaluating the exercise. US-CERT also briefed the exercise to the cyber subcommittee of the independent DHS Data Privacy and Integrity Committee.

Beyond the TIC initiative and the EINSTEIN system, DHS, OMB, and the National Institute for Standards and Technology work cooperatively with agencies across the federal government to coordinate the protection of the nation's federal information systems through compliance with the Federal Information Security Management Act of 2002 (FISMA). US-CERT monitors EINSTEIN 2 sensors for intrusion activity and receives self-reported incident information from federal agencies. This information is reported to OMB for use in its FISMA oversight capacity. In 2010, DHS also began to administer oversight of the CyberScope system, which was developed by the Department of Justice. This system collects agency information regarding FISMA compliance and, as DHS, OMB and their agency partners move toward automated reporting, the system will enable real-time assessments of baseline security postures across individual agencies and the federal enterprise as a whole. This activity complements the development of reference architectures that DHS designs for federal agency stakeholders that are interested in implementing security solutions based on standards and best practices. DHS also works with the General Services Administration to create Blanket Purchase Agreements that address various security solutions for federal agencies.

The DHS Cybersecurity Workforce

As DHS continues to make progress on initiatives such as TIC and EINSTEIN, the Department is also mindful that the cybersecurity challenge will not be solved by a single technology solution. Multiple innovative technical tools are necessary and indeed, technology alone is insufficient. The mission requires a larger cybersecurity professional workforce, governance structures for enhanced partnerships, more robust information sharing and identity protection, and increased cybersecurity awareness among the general public. Responsibility for these solutions is, and will remain, distributed across public and private sector partners.

DHS is focused on building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals—computer engineers, scientists, and analysts—to secure the nation's digital assets and protect against cyber threats to our critical infrastructure and key resources.

NCSD continues to hire cybersecurity and information technology professionals, nearly tripling its cybersecurity workforce in FY 2009 and nearly doubling that number again in FY 2010. NCSD currently has more than 230 cybersecurity professionals on board, with dozens more in the hiring pipeline.

Several initiatives are designed to increase the nation's number of highly qualified cybersecurity professionals. DHS and NSA co-sponsor the Centers of Academic Excellence in Information Assurance Education and Research programs, the goal of which is to produce a growing number of professionals with information assurance expertise in various disciplines. DHS and the Department of State co-hosted Operation Cyber Threat (OCT1.0), the first in a series of government-wide experiential and interactive cybersecurity training pilots designed to apply learning concepts and share best practices in a secure, simulated environment to build capacity within the federal workforce. In December 2010, the Institute of Electrical and Electronics Engineers Computer Society, the world's leading organization of computing professionals, formally recognized the Master of Software Assurance (MSwA) Reference Curriculum, which DHS sponsored through its Software Assurance (SwA) Curriculum Project. The MSwA program is the first curriculum of its kind to focus on assuring the functionality, dependability, and security of software and systems. Finally, DHS co-sponsored the annual Colloquium for Information Systems Security Education and the Scholarship for Services (SFS) Job Fair/Symposium, which brought together 55 federal agencies and more than 200 SFS students.

The National Initiative for Cybersecurity Education (NICE) has the dual goals of a cyber-savvy citizenry and a cyber-capable workforce. Working with NIST, which is the overall interagency lead, DHS heads the NICE awareness elements and co-leads the training and professional development components with DoD and the Office of the Director of National Intelligence.

Interagency and Public-Private Coordination

Overcoming new cybersecurity challenges requires a coordinated and focused approach to better secure the nation's information and communications infrastructures. President Obama's *Cyberspace Policy Review* reaffirms cybersecurity's significance to the nation's economy and security. Establishment of a White House Cybersecurity Coordinator position solidifies the priority the Administration places on improving cybersecurity.

No single agency controls cyberspace and the success of our cybersecurity mission relies on effective communication and critical partnerships. Many government players have complementary roles—including DHS, the Intelligence Community, DoD, the Department of Justice, the Department of State, and other federal agencies—and they require coordination and leadership to ensure effective and efficient execution of our collective cyber missions. The creation of a senior-level cyber position within the White House ensures coordination and collaboration across government agencies.

DHS works closely with its federal, state and local partners to protect government cyber networks. In September 2010, DHS and DoD signed a memorandum of agreement that aligns and enhances America's capabilities to protect against threats to our critical civilian and military computer systems and networks, including deploying a National Security Agency support team

to the NCCIC to enhance the National Cyber Incident Response Plan and sending a full-time senior DHS leader and support team to the National Security Agency.

This initiative builds upon pre-existing liaison exchanges DHS has with the National Security Agency/Central Security Service Threat Operation Center (NTOC), United States Cyber Command and United States Northern Command. Liaisons to DHS operate out of US-CERT and the NCCIC. The initiative also further supports DHS' already active partnership with DoD. The partnerships ensure that agile coordination and technical capabilities support any cyber contingency.

In November 2010, the Multi-State Information Sharing and Analysis Center (MS-ISAC) opened its Cyber Security Operations Center, a 24-hour watch and warning facility, which will both enhance situational awareness at the state and local level for the NCCIC and allow the federal government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to state and local governments. An MS-ISAC analyst/liaison is collocated in the NCCIC.

Private industry owns and operates the vast majority of the nation's critical infrastructure and cyber networks. Consequently, the private sector plays an important role in cybersecurity, and DHS has initiated several pilot programs to promote public-private sector collaboration. In its engagement with the private sector, DHS recognizes the need to avoid technology prescription and to support innovation that enhances critical infrastructure cybersecurity.

In February 2010, DHS, DoD, and the Financial Services Information Sharing and Analysis Center (FS-ISAC) launched a pilot designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information. In June 2010, DHS implemented the Cybersecurity Partner Local Access Plan, which allows security-cleared owners and operators of CIKR, as well as state technology officials and law enforcement officials, to access secret-level cybersecurity information and video teleconference calls via state and local fusion centers. In November 2010, DHS signed an agreement with the Information Technology Information Sharing and Analysis Center (IT-ISAC) to embed a full-time IT-ISAC analyst and liaison to DHS at the NCCIC, part of an ongoing effort to collocate private sector representatives alongside federal and state government counterparts. The IT-ISAC consists of information technology stakeholders from the private sector and facilitates cooperation among members to identify sector-specific vulnerabilities and risk mitigation strategies.

In December 2010, DHS and NIST signed a Memorandum of Understanding with the Financial Services Sector Coordinating Council. The goal of the agreement is to speed the commercialization of cybersecurity research innovations that support our nation's critical infrastructures. This agreement will accelerate the deployment of network testbeds for specific use cases that strengthen the resiliency, security, integrity, and usability of financial services and other critical infrastructures.

In July 2010, DHS worked extensively with the White House on the publication of a draft National Strategy for Trusted Identities in Cyberspace, which seeks to secure the digital identities of individuals, organizations, services and devices during online transactions, as well

as the infrastructure supporting the transaction. This fulfills one of the near-term action items of the President's *Cyberspace Policy Review*. The strategy is based on public-private partnerships and supports the protection of privacy and civil liberties by enabling only the minimum necessary amount of personal information to be transferred in any particular transaction. Its implementation will be led by the Department of Commerce.

Public Education and Outreach

While considerable activity is focused on public and private sector critical infrastructure protection, DHS is committed to developing innovative ways to enhance the general public's awareness about the importance of safeguarding America's computer systems and networks from attacks. Every October, DHS and its public and private sector partners promote efforts to educate citizens about guarding against cyber threats as part of National Cybersecurity Awareness Month. In March 2010, Secretary Napolitano launched the National Cybersecurity Awareness Challenge, which called on the general public and private sector companies to develop creative and innovative ways to enhance cybersecurity awareness. In July 2010, seven of the more than 80 proposals were selected and recognized at a White House ceremony. The winning proposals helped inform the development of the National Cybersecurity Awareness Campaign, *Stop. Think. Connect.*, which DHS launched in conjunction with private sector partners during the October 2010 National Cybersecurity Awareness Month. *Stop. Think. Connect,* a message developed with the private sector, has evolved into an ongoing national public education campaign designed to increase public understanding of cyber threats and how individual citizens can develop safer cyber habits that will help make networks more secure. The campaign fulfills a key element of President Obama's *Cyberspace Policy Review*, which tasked DHS with developing a public awareness campaign to inform Americans about ways to use technology safely. The campaign is a component of the NIST National Initiative for Cyber Education (NICE).

Throughout its public and private sector activities, DHS is committed to supporting the public's privacy, civil rights and civil liberties. Accordingly, the Department has implemented strong privacy and civil rights and civil liberties standards into all of its cybersecurity programs and initiatives from the outset. To support this, DHS established an Oversight and Compliance Officer within NPPD, and key cybersecurity personnel receive specific training on the protection of privacy and other civil liberties as they relate to computer network security activities. In an effort to increase transparency, DHS also publishes privacy impact assessments on its website, www.dhs.gov, for all of its cybersecurity systems.

Conclusion

Set within an environment characterized by a combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness, the cybersecurity mission is truly a national one requiring collaboration across the homeland security enterprise. The Department of Homeland Security is committed to creating a safe, secure and resilient cyber environment while promoting cybersecurity knowledge and innovation. We must continue to secure today's infrastructure as we prepare for tomorrow's challenges and opportunities. It is important to recognize that we do not undertake cybersecurity for the sake of security itself, but rather to ensure that government,

business and critical societal functions can continue to use the information technology and communications infrastructure on which they depend.

Distinguished Members of the Committee, we would like to reiterate that we look forward to exploring opportunities to advance this mission in collaboration with the Committee and our colleagues in the public and private sectors.

Mr. CHAFFETZ. Thank you.

Mr. Bond, you are now recognized for 5 minutes.

STATEMENT OF PHILLIP BOND

Mr. BOND. Thank you, Mr. Chairman, Ranking Member Tierney, members of the committee. I am honored to be here on behalf of TechAmerica, the largest industry trade association in the United States with some 1,000 member companies. I will offer just a few thoughts on the challenge in cyber and the policy response we need.

First, I would observe that cyber criminals respond rapidly; they are creative. In 2010, McAfee Labs identified more than 20 million new pieces of malware globally. A 2011 online fraud report from RSA, the security division of EMC, found that the U.S has consistently hosted and been the target of a majority of the worldwide cyber attacks.

Economic impact is serious. It is about $6 million a day when a corporationsite is down, on average, and worldwide, the economy loses some $86 billion a year due to cyber attacks. Protecting our networks, is as the Chair has observed, a public/private shared responsibility. Neither one of us can do it alone.

The private sector's responsibility is to innovate and operate its own infrastructure in a safe way. The government has an obligation to share timely and accurate information so that the private sector can secure itself and turn around and help to secure the government.

I will defer to our witness from Symantec on a little bit more technical descriptions of some of the threats. I would just underscore this. The range of threat actors—especially right now—including advanced, persistent threats, APTs—you will hear more about that—are going directly after the end user.

They attempt to trick them into downloading malware or divulging sensitive information. Again, it is the actual user being targeted, not the mechanical system, the software or whatever. It is going after human error. As criminals probe for a soft spot in a system, they are also probing now the individuals who connect to that network.

With the increased reliance on all IT devices now, we see the great shift to mobile devices and that too will be an opportunity for cyber criminals. Applications many times are downloaded by users and not always being properly vetted.

We would submit that the policymakers and the industry as well and the government need to view security as an absolute basic, not to be added on after but to be built-in from the ground up. I would observe many companies are doing exactly that. We need everybody to do that.

I want to spend a couple of my remaining minutes on some thoughts for you to consider as you draft legislation, but let me break here to underscore something that needs to be said. Technology and innovation are a huge net positive for the U.S. economy and for government, for government service as well. They are our key to national security, the war fighter has an advantage, the key to homeland security, the key to economic security, high paying jobs, where we need to be as an economy, but with those advan-

tages there also have been some down sides. That is what we are attempting to talk about today.

Please consider, first, in policy, Congress should do no harm. Do not undermine innovation; it is our advantage. One size fits all will not work. Second, government should promote an outcome-based, layered security approach. Government should develop processes to manage and measure performance associated with real security. Third, government should adopt a risk-based approach to our Nation's infrastructure. That means critical infrastructure should be defined to include only that which is of the utmost importance to national security and then truly work to secure it.

Fourth, we believe government can provide incentives to encourage industry to invest in best practices in security, for example, safe harbor, from data breach notification, when an organization does what it should in advance of a breach incident.

Fifth, Congress should update our government's Federal information security practices and laws to perform in a more nimble environment, so we strongly support updating FISMA. I know the committee knows about that.

Finally, if industry is to act at the behest of government, it is necessary that there be clear liability protections, so if you do what you should do or at the government's behest, you should also be protected from unintended consequences or liabilities.

Again, on behalf of the industry, thank you for holding this hearing. We look forward to doing all that we can to be a part of the public/private partnership to find a solution and maintain our national advantage in innovation.

Mr. CHAFFETZ. Thank you.

Mr. Lewis, you are recognized for 5 minutes.

STATEMENT OF JAMES A. LEWIS

Mr. LEWIS. Thank you, Mr. Chairman. I thank the committee for the opportunity to testify. I am really impressed with the energy that the committee is bringing to this issue. It is something we need.

We depend, as a Nation, on the Internet, but it is not secure and this gives criminals and foreign opponents real opportunity to damage the United States. Cyber threats fall into two categories: high end attacks that cause damage, destruction or casualties and threats from cyber crime and cyber espionage.

Five countries, including Russia and China, can launch high end cyber attacks. Another 30 countries are developing these capabilities. States use skilled proxies, cyber criminals and hackers to help them. Cyber attacks could destroy critical infrastructure or disrupt essential networks and services. At the moment, however, no nation is likely to attack the United States because they fear retaliation.

Terrorists do not yet have cyber attack capabilities, nor do dangerous nations like Iran and North Korea. However, they are eagerly pursuing these cyber capabilities. We do not know how close they are to acquiring them, but the moment they acquire them, we can expect to see damaging cyber attacks.

The immediate threat to the national interest comes from crime and espionage. The Internet, with all its weaknesses, created a

golden age for espionage and the United States has been the chief victim. We have lost military technology, intellectual property for high tech companies, oil exploration data and confidential business information. Banks suffer million dollar losses almost every month.

None of this attracts much attention and some companies prefer to conceal their losses and in some cases, companies may not even know they have been hit. Our estimates of the damages, as you heard, are in the billions of dollars. Weak cyber security damages our economic competitiveness and technological leadership.

What can we do about this? There is certainly a new energy in Washington about approaching this problem, which is great. First, we need to accept that we need a new approach that puts cyber security as a major, national security problem. The most dangerous threats in cyberspace come from foreign militaries and foreign intelligence agencies.

Second, this new approach needs to combine trade policy, law enforcement, military strategy and critical infrastructure protection. For critical infrastructure, this means that DHS must be able to mandate risk-based performance standards. Public/private partnerships are an important part of this. It would help, however, to differentiate where the private sector is strongest in things like information sharing and innovation and where government action is needed.

The immediate question is whether we can improve our defenses before there is a damaging attack. Most of the experts I know believe this is not possible, that America will only act after a crisis. I believe that the work of this committee and others can help us avoid that fate and let us do what is necessary to improve public safety and national security in cyber space.

Thank you for the opportunity to testify and I look forward to your questions.

[The prepared statement of Mr. Lewis follows:]

House of Representatives Committee on Oversight and Government Reform
Subcommittee on National Security, Homeland Defense and Foreign Operations
"Cybersecurity: Assessing the Immediate Threat to the United States"
James A. Lewis, Center for Strategic and International Studies
May 25, 2011

No one expected the internet to become a critical global infrastructure, least of all the people who designed and built it. So we should not be surprised that it is not very secure and that it is easy for malicious actors to exploit. There is an asymmetry between our considerable dependence on the new technology and our ability to secure it – the internet is incredibly valuable but it is easy to attack. This asymmetry gives potential attackers an advantage that they have not been slow to seize. The result has been to create two broad categories of threats to American security, or for that matter, the security of any nation that uses the internet.

The first set of threats arises from the potential for cyberspace as a new avenue of attack for military purposes. The second threat arises from the ongoing use of cyberspace for crime and espionage, including economic espionage. The distinction between these two threats revolves around whether a malicious action in cyberspace is equivalent to the use of force, to an attack using conventional weapons. We tend to call everything bad that happens in cyberspace an attack, but it is more realistic to say that if there is no damage, death or destruction, it is not an attack. We know of only three cyber incidents that rise to this level – the Stuxnet attack, the reported blackout in Brazil, and the interference with air defenses in the Israeli raid on a Syrian nuclear facility. Everything else qualifies as crime or espionage.

Cyber warfare will involve disruption of crucial network services and data, damage to critical infrastructure, and the creation of uncertainty and doubt among opposing leaders. The Russian use of cyber exploits during their clash with Georgia suggests how cyber attacks might be used – to complement conventional forces rather than to replace them. The air raid against the Syrian nuclear facility is a good example of this. While jets streaked across Syria, air defense radars showed an empty sky. This "informational" aspect of cyberwar, where an opponent might scramble or erase data, or put in false information to mislead an opponent, is a new and forceful aspect of military conflict.

Most people know about the Stuxnet worm, when a cyber attack destroyed equipment at an Iranian nuclear facility. Stuxnet confirmed what a test at the Idaho National Labs in 2007 had already shown – that an attacker could remotely interfere with the software controlling critical infrastructure and damage or destroy machinery and equipment. This kind of "military grade" cyber attack is best seen as a new capability for long range, very rapid strikes against critical infrastructure, information and networks. Cyber attacks are faster than a missile and have a global reach, but their payload is much less destructive. This military aspect of the cyber problem is like other military threats to U.S. security, deterred in part by our capability for response.

At this time, only a few nations with advanced military or intelligence agencies have the ability to launch Stuxnet-like cyber attacks that could disrupt critical infrastructure. There are perhaps five or six such nations. Our most advanced cyber opponents have carried out network

reconnaissance against America's critical infrastructure. None of the countries with advanced cyber attack capabilities are likely to use them frivolously against the United States, but they are certain to use cyber attacks if we enter into a military conflict with them.

There is, of course, the possibility of miscalculation, if one of our opponents in cyberspace carries out an experiment or weapons test that goes out of control, or a reconnaissance effort that accidently disrupts critical services. This sort of miscalculation or error could result in events escalating from a single incident to a more damaging conflict, which is one reason why many nations worry about cyber warfare.

Our research suggests that thirty-six countries have military doctrine for cyber conflict. Very few admit to offensive capabilities, but it is reasonable to assume that many have, as part of developing defensive capabilities, at least considered offensive use. Cyber attack will be like the airplane – within a few years, no self respecting military will be without this capability. Cyber attack capabilities are easier to acquire than airplanes, and to quote the head of Israeli military intelligence, "cyberspace grants small countries and individuals a power that was heretofore the preserve of great states."

As cyber attack capabilities spread, our ability to prevent attacks will diminish. Confrontational states such as North Korea and Iran do not yet have the capability to launch cyber attacks, but both North Korea and Iran are making serious efforts to acquire cyber attack capabilities. It is inevitable that they will succeed, which is one reason why it is important for the United States to strengthen its defenses as soon as possible. The most sophisticated cybercriminals, who sometimes act as irregular forces for their host governments - could launch damaging cyberattacks, but their interest is in making money or carrying out espionage activities. This could easily change. We have not yet seen advanced cyber criminals act as attackers or as mercenaries, but this remains a possibility. The future will be the "commoditization" of advanced attack techniques that will enable a range of groups to consider cyber attack as an option.

Terrorists currently lack the capability to launch cyber attacks. If they had it, they would have already used it. The day a terrorist group can launch a cyber attack, it will do so. A few terrorist groups have expressed interest in acquiring cyber attack capabilities. They have said one of their goals is to disrupt the American economy – this was the alleged motive for the effort by al Qaeda in the Arabian Peninsula to tamper with printer cartridges sent via in air cargo. We have a few years before terrorist groups or irresponsible nations like Iran or North Korea become sufficiently advanced in their cyber attack capabilities to launch strikes against the United States.

However, most nations are afraid of unleashing cyberwar. They are possibly deterred by fear of a U.S. military response. They are careful, therefore, to stay below the threshold of what could be considered, under international law and practice, the use of force or an act of war. They concentrate their efforts on espionage and crime which, in cyberspace, carry almost no risk. There is little or no consequence for malicious cyber activities that do not involve the use of force. So while countries are very cautious in using cyber techniques for attack, they feel very little constraint in using cyber techniques for espionage or crime. Crime, even if state sponsored, does not justify a military response. Countries do not go to war over spying. For these reasons,

the immediate threat in cyberspace involves espionage and crime. These are daily occurrences.

Foreign competitors use cyber espionage to acquire our most advanced military technologies. One way to estimate the threat from cyber espionage is to look at the amount of material already lost. Sources at the State and Defense Departments say that by 2007, they had already lost perhaps six or seven terabytes of information. To put this in perspective, the 130 million books and manuscripts in the Library of Congress take up twenty terabytes. The loss of thousands of pages of documents and designs help explain many analysts say that the internet has created a "golden age" for espionage.

Foreign competitors use cyber espionage to steal business plans, intellectual property and product designs from companies. The effect is to undermine U.S. international competitiveness. While losses from piracy – the illegal copying of entertainment or software products - are significant, economic espionage poses the greatest threat. The U.S. spent $368 billion on research and development (R&D) in 2010, but cyber espionage lets other countries get the results for free. The December 2010 incident where Google and thirty other Fortune 500 companies were hacked and lost data, allegedly to a Chinese entity, illustrate the espionage problem. Google lost technology and its Gmail service was searched for information on Tibetan human rights activists. The technology acquired from Google and other American high tech companies will eventually improve Chinese products. The theft of intellectual property is a major trade issue that deserves greater attention and a real threat to America.

It is hard to estimate the losses from cyber espionage and cyber crime. Companies conceal their losses and some may not even be aware of what has been taken. Crime against banks and other financial institutions probably costs a few hundred million dollars every year. In contrast, the theft of intellectual property and business confidential information – economic espionage –cost developed economies much more. One estimate put U.S. losses of intellectual property and technology through cyber espionage at $240 billion. An estimate of German losses of intellectual property due to cyber espionage puts them at perhaps $20 billion. Since the U.S. GDP is roughly five times the size of Germany, a very simple extrapolation would put U.S. losses from intellectual property theft at $100 billion. These are very crude estimates, but they give some idea of the scope of the problem.

In the context of a $14 trillion economy, these losses appear small and perhaps this is why they do not attract much attention. Still it is baffling why a cyber- bank robbery that stole $11 million, such as occurred in the last year, attracted little attention. If gunmen walked into a local bank and stole a million dollars, it would be on every front page. Robberies of this size probably happen almost every month in cyberspace, yet they rarely attract notice. The theft of credit card data gets more attention. It remains a lucrative field for cyber criminals. A recent example – the theft of credit card data from the Play Station network - affected as many as 99 million people. Some say that so much was stolen that the price of credit card data in cybercrime black markets actually fell because of the glut.

These black markets support cybercrime. In the cyber black market you can buy the latest hacking tools, learn of recently discovered vulnerabilities, rent "botnets" (thousands of remotely controlled computers), or purchase personally identifiable information. Credit card numbers,

social security numbers, and bank accounts, can be bought in lots of five or ten thousand. Buyers can choose between 'raw' information or data that has been tested for accuracy. These black markets amplify the threat of cybercrime and help make it a professional activity.

There is increasing concern about the vulnerability of the American financial system to cyber disruption. How much of this concern is justified is difficult to say, but there are some disquieting signs. Last year's "flash crash," where automated trading systems briefly crashed the stock market shows the potential for cyber disruption. This year's penetration of NASDAQ, while it did not lead to any noticeable losses, shows the potential vulnerabilities of the system. While it is very unlikely that the nations with advanced cyber capabilities would crash the American financial system – they simply have too much invested in it – they could try to do so in the event of a war. It is more likely is that cybercriminals, in an attempt to manipulate stock prices or gain insider information, could inadvertently cause some kind of crash. Federal agencies, financial institutions and the major exchanges are all working to reduce the chances of this kind of damaging event, but it remains a possibility.

Malicious action against the information technology supply chain is another threat. Many nations, including both the U.S. and China, are worried about depending on a global supply chain for information technology products. Discussion of the supply chain problem is usually not very sophisticated. An astute opponent will not build in back doors into a product since these might be discovered. Better to sell a safe product with no errors that will pass inspection, and then exploit the knowledge and access from the sale to gain intelligence advantage and to increase the ability to disrupt infrastructure in a conflict. An obvious example of this would be for a company to sell a product that is completely secure and passes every test, and then to introduce vulnerabilities when they provide the inevitable "patch" to the software. How often do people examine a patch or update?

The growth of table computers and other mobile devices makes downloadable "apps" an interesting vehicle for malware delivery. When was the last time anyone thought about security when they downloaded an app? Apps are screened, of course, but usually to make sure they are interoperable. An astute opponent or criminal might offer an enticing game app for free and then reap the benefits.

Supply chain contamination is a real threat, but heavy-handed measures to reduce supply chain risk, such as intrusive product inspections by national agencies, will backfire. They will only reinforce the plans of other nations to use these techniques and harm American exports. WE need alternate approaches that will build trust. While there has been some useful progress in reducing supply chain risk, it may be impossible to eradicate it, and we may need to step back and ask how we can operate effectively on networks that, despite our best efforts, will have some degree of supply chain contamination.

A final category of cyber threat involves political action, although this may hold greater risk for countries other than the U.S. The European leftists behind the Wikileaks episode intended to damage the United States and to hurt its credibility and influence internationally. The effect was to help our opponents – jihadis and authoritarian regimes. We do not want to overstate the risk from events like Wikileaks, but those hostile to the United States will take advantage of poor

security of information and the global reach of the internet to damage the United States. There is also the threat that a foreign opponent might disrupt American elections. We know for example that campaign databases were hacked and information exfiltrated from both the McCain and Obama Presidential campaigns in 2008. While the data was apparently not used, it is easy to imagine someone leaking it to the media or taking other disruptive actions.

The most dangerous actors in cyberspace bear the unwieldy acronym APT, "advanced persistent threat." We have gone from high school students and "social hackers," who penetrated systems to gain prestige, to well-organized professional criminals and major intelligence agencies. Amateurs cannot defend themselves against these professional opponents – it would be like sending the company softball team against the New York Yankees.

Based on this survey, what can we say generally about threats to the U.S. in cyberspace? They are largely foreign, and foreign governments play a central role in directing or supporting them. They run the gamut from fairly simple fraud aimed at consumers to highly sophisticated espionage efforts. The best description would be that the greatest threats come from advanced, state-sponsored actors who have the skill and resources to overcome most defenses. The trend is that the less sophisticated threats will diminish, while the advanced threats will grow

This has serious implications for policy and helps to explain why so much of what we have done in cybersecurity has been ineffective. Reducing the threat to the United States requires a clear division of responsibility among agencies and between government and companies. But in the past, we have weighted this division too heavily in favor of the private sector. The threats we face come from increasingly professional sources, from intelligence agencies, militaries, state sponsored proxies, and from terrorist groups. No uncoordinated effort that relies on voluntary action will be sufficient to protect us against these threats. The private sector owns most of the shoreline, but we still need a navy. We do not ask airlines to defend our airspace against ballistic missiles, bombers, or fighter jets because they are incapable of defeating these foes. The same is true for cyberspace. We should ask companies to do only what makes sense from a business perspective and not ask them to should national defense burdens for which they are unequipped.

The most important function for a company is to make money, not provide for the national defense. National defense against professional opponents is a function only the Federal government can perform effectively. In some cases, meeting the challenge will require new partnerships – and we have seen successful partnerships in the financial and the defense industrial sectors. In other cases, it will require new incentives and federal authorities. An overview of threats and responsibilities suggests the following division of labor:

-- Innovation in new cybersecurity technologies is best left to the private sector. We would benefit across the board as a nation by removing regulatory and financial obstacles to the private sector's ability to innovate. Fundamental research, however, will require federal investment by institutions such as DARPA or the National Science Foundation. This was how the internet itself was created – the government funded the initial research, then passed it to the private sector for commercialization.

-- Supply chain threats are an area where the private sector is best equipped to understand

and respond to the problem. Some of the new partnership efforts created by the Departments of Defense and Homeland Security, and working with a small number of companies, have made real progress in securing the supply chain (although much work still remains).

-- Dealing with the threat of cybercrime requires close and equal partnership between companies and law enforcement agencies. FBI and Secret Service have worked closely and effectively with the financial community, for example, to pursue cybercriminals. The cybercrime threat can only be met through partnership, combined with strengthened cooperation with other governments.

-- Better information sharing would greatly improve our ability to understand and respond to cyber threats. If we could put together all the information held by cyber security vendors, internet and telecommunications service providers, and the intelligence community, we would have an almost complete picture of malicious activities in cyberspace. This will require new partnerships and new authorities. Government might need to be a partner and a participant rather than a leader. Neither private sector nor government have by themselves that complete picture. Companies complain that they get little useful information from government agencies. Some current laws, such as the 1986 Electronic Communications Privacy Act, may inadvertently hamper the ability to share information. Many of the groups created years ago to share information do not work and should be replaced. Information sharing is an area where partnership is vital, but we need to rethink our laws and find new approaches that serve the needs of both partners.

-- Bot-nets are an embarrassment for the United States. We are, inadvertently, one of the largest sources of cyber crime activity on the planet. Consumers do not know how to protect their computers and we are never going to be able to train them sufficiently. That means they are easy prey for cybercriminals, who seize control of their machines and use them for spam, denial of service attacks and other nefarious activities. Other nations, however, have developed an effective approach to bot-nets that is linked to information sharing. Consumers do not know when their computer has been captured but their service providers do. Making the service provider responsible for cleaning up bot-nets and malware on their costumer's computer would eliminate the problem. How do to this – whether through a voluntary consortia guided by government, as is the case in Australia and Germany, or in some other fashion, remains an open question. There is resistance from some service providers to taking on this responsibility for a variety of reasons, but both security and technology trends will eventually drive us to make service providers responsible for the security of consumer devices.

-- The threat to critical infrastructure also requires a close partnership between companies, the Department of Homeland Security and other regulatory agencies, but we can no longer rely on voluntary approaches or self-regulation in this partnership. We have used voluntary self-regulation for the last thirteen years and it is inadequate for national security. For example, although Stuxnet is the most dangerous cyber attack seen to date, a recent survey found that a third of the surveyed critical infrastructure companies did not even look for it on their networks. The new, more flexible approach to critical infrastructure protection that is modeled after the 109th Congress's Chemical Facilities Anti-Terrorism Standards, where industry develops the standards to meet potential threats and government makes sure they are adequate, offers a

solution that avoids prescriptive regulations without putting national security at risk.

-- The threat from foreign military and intelligence agencies can only be addressed by our own military, law enforcement, and intelligence agencies. No private company can match this class of foreign opponents, who can blend signals intelligence, human agents, and vast resources into an unstoppable package to penetrate networks, collect information, and if they wish, do damage. These opponents can bribe, steal, eavesdrop, spend millions to reverse engineer products, and work simultaneously in many countries around the globe. They draw in some cases on decades of experience in illegal activities and espionage. Defense, homeland security, and international law enforcement are federal responsibilities. We must approach these threats as we would approach any other threat to national security

We face a varied threat landscape in cyberspace. Countering these threats will require a balanced and comprehensive approach that to cybersecurity. This comprehensive approach is within our grasp if we can make a fresh start to addressing the problem. Yet when you talk to most people in the small community of cybersecurity experts, you will find a high degree of pessimism. Most of these experts believe that the U.S. will not adopt effective approaches to cybersecurity and will not move away from the ineffective policies of the past until we have some major incident, some disaster. I do not share this pessimism. The work of this committee and others will let us move ahead in making cyberspace more secure. I applaud the committee's work in calling attention to this and I thank you for the opportunity to testify. I will be happy to take any questions.

Mr. CHAFFETZ. Thank you.

Mr. Turner, you are recognized for 5 minutes.

STATEMENT OF DEAN TURNER

Mr. TURNER. Chairman Chaffetz, Ranking Member Tierney and members of the subcommittee, thank you for the opportunity to testify today as the committee considers cybersecurity and the current threat level to the United States.

Mr. Chairman, on behalf of the nearly 500 Symantec employees based in your district in Linden, we certainly appreciate your focus on cybersecurity issues.

My name is Dean Turner. I am director of Symantec's Global Intelligence Network.

Symantec is the world's information security leader with over 25 years experience in developing Internet security technology. Our best-in-class Global Intelligence Network allows us to capture worldwide security intelligence data. We maintain 11 security response centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. In short, if there is a class of threat on the Internet, Symantec knows about it.

In my written testimony, I have provided the committee with greater detail on the evolving threat landscape, as well as an assessment of some of the real world impacts of cyber attacks on businesses and individuals. I also touch on major challenges and the vulnerabilities associated with securing new technologies and how organizations can better secure their important and critical systems.

In our April 2011 Symantec Internet Security Threat Report, we observed several key threat landscape trends for the calendar year 2010. The year was book-ended by two significant targeted attacks, including Hydraq, otherwise known as Aurora, and Stuxnet. Stuxnet was a game changer, exemplifying just how sophisticated and targeted threats are becoming. It demonstrated the vulnerability of critical national infrastructure to attack and Stuxnet was the first publicly known threat to target industrial control systems.

Social networks continue to be a security concern for organizations as government agencies and companies struggle to find a satisfactory compromise between leveraging the advantage of social networking and limiting the dangers posed by the increased exposure of potentially sensitive and exploitable information.

Leveraging information from social networking sites as part of a social engineering campaign is one of the simplest and most effective ways an attacker can lure their target to a malicious Web site. For example, an attacker can use information gathered from a social networking site to create a target email that then lures a victim to a Web site that hosts malicious code. If the victim visits the Web site, a Trojan, for example a key logger or a backdoor can be installed and that begins ex-filtrating sensitive information back to the attacker.

In 2010, attack tool kits continued to see widespread use. A typical tool kit today is built to allow the cyber criminal to monetize infected machines in every way possible. For example, keystroke loggers are a simple way to capture any password a user types in.

Other Trojans can also steal email addresses found on the machine as well as add additional malware.

Attack tool kits and their ability to update over the Web greatly increase the speed with which new vulnerabilities are packaged, exploited and spread. One of the most significant attack kits known at the moment is the Zeus Trojan and is a favorite of cyber criminals due to its ease of use and low cost, about $400 in the underground economy. It takes little to no technical knowledge to launch this type of attack and it can be extremely profitable for cyber criminals.

With the proliferation of smart phones and mobile devices, users are increasingly downloading third party applications which is creating an opportunity for the installation of malicious applications. In 2010, there was a 42 percent increase in the number of reported new mobile operating system vulnerabilities and most mobile malicious code is now designed to generate revenue. Therefore, there is likely going to be more threats created for these devices as people increasingly use them for sensitive transactions such as on-line shopping and banking.

We have learned many lessons from today's threat landscape and while the sophistication level of attacks is increasing as is the potential and real damage caused by such attacks, we need to turn these lessons into action. In addition to the recommendations contained in my written testimony, the following steps must be taken in order to better protect critical systems from cyber attack.

First, develop and enforce IT policies and automate compliance processes. Second, authenticate identities by leveraging solutions that allow business to ensure only authorized personnel have access to those systems. Third, secure end points, messaging and Web environments. In addition, defending critical internal servers and implementing the ability to backup and recover data need to be top priorities.

Members of the committee, cybersecurity faces a constantly evolving threat and there is no single solution to prevent attacks. Attackers are getting smarter and more resourceful every day. Because of that, any solution must include the private sector's expertise and innovation. We must continue to be vigilant in protecting our economy, our national security and our way of life.

Symantec applauds Congress for focusing much needed attention on cybersecurity and we look forward to continuing this important dialog. I will be happy to answer any questions you might have.

[The prepared statement of Mr. Turner follows:]

Prepared Testimony and
Statement for the Record of

Dean Turner
Director, Global Intelligence Network
Symantec Corporation

Hearing on

Cybersecurity: Assessing the Immediate Threat to the United States

Before the

U.S. House of Representatives
Committee on Oversight and Government Reform
Subcommittee on National Security, Homeland Defense and Foreign Operations

May 25, 2011

2154 Rayburn House Office Building

INTRODUCTION

Chairman Chaffetz, Ranking Member Tierney, and Members of the Subcommittee, thank you for the opportunity to appear before you today as the Committee considers cybersecurity and the current threat to the United States.

My name is Dean Turner and I am the Director of the Global Intelligence Network at Symantec Corporation. My primary responsibilities include designing and delivering our security intelligence data feeds and developing next generation security intelligence toolsets that provide greater visibility into the threat landscape. I have co-authored and managed Symantec's Internet Security Threat Report which is a trusted source of global research and analysis on cyber attack data gathered from the Global Intelligence Network.

Symantec[1] is the world's information security leader with over 25 years of experience in developing Internet security technology. Today we protect more people and businesses from more online threats than anyone in the world. Our best-in-class Global Intelligence Network allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape including emerging cyber attack trends, malicious code activity, phishing and spam. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. In short, if there is a class of threat on the Internet, Symantec knows about it.

In 2010, Symantec security technology blocked more than three billion attacks on individual and enterprise systems. In addition, we saw the threat landscape become exponentially more hazardous, with the discovery of 14 new zero-day vulnerabilities, 163 new mobile vulnerabilities, 6,253 new vulnerabilities, and 286 million new unique variants of malicious code. As an example of the magnitude of the threat, in the time it takes to read this testimony, Symantec will block more than 365,000 attacks against our customers.

At Symantec, we are committed to assuring the security, availability, and integrity of our customers' information. The protection of critical infrastructure is a top priority for us. We believe that critical infrastructure protection is an essential element of a resilient and secure nation. From water systems to computer networks, power grids to cellular phone towers, risks to critical infrastructure can result from a complex combination of threats and hazards, including terrorist attacks, accidents, and natural disasters.

Symantec welcomes the opportunity to provide comments as the Committee continues its important efforts to ensure that adequate policies and procedures are in place, both in the private sector and in the federal government, to monitor and secure critical systems from cyber attack. In my testimony today, I will provide the Committee with:

- Symantec's latest analysis of the evolving threat landscape as detailed in the *Symantec Internet Security Threat Report Volume XVI (ISTR XVI)*;
- An assessment of the real-world impacts of cyber attacks on business and individuals;
- Insights into the major challenges and vulnerabilities associated with securing new technologies; and
- Observations on how organizations can better secure these systems.

---

[1] Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

EVOLVING THREAT LANDSCAPE

In April 2011, we published the latest *Symantec Internet Security Threat Report Volume XVI (ISTR XVI)*[2], where we observed significant changes to the threat landscape that existed in 2010. The volume and sophistication of threat activity increased substantially, with Symantec identifying more than 286 million new threats last year.

However, to understand the evolving threat landscape, we first should understand who is behind the vast array of cyber attacks that we are seeing today. Attacks originate from a range of individuals and organizations, with a wide variety of motivations and intended consequences. Attackers can include hackers (both individual and organized gangs), cybercriminals (from petty operators to organized syndicates), cyber spies (industrial and nation state), and "hacktivists" (with a specific political or social agenda). Consequences can also take many forms: from stealing resources and information, to extorting money, to outright destruction of information systems.

It is also important to recognize that attackers have no boundaries when it comes to who their intended victims are. All organizations and individuals are potential targets of those who seek to do harm. Corporate enterprises are often the object of targeted attacks specifically to steal customer data and intellectual property, but also to disrupt business processes and commerce. Small businesses are often less resilient and the impacts of stolen bank accounts and business disruption can be catastrophic in a very short time frame. End-users or consumers are confronted with the financial and disruptive impacts of identity theft, scams, and system clean-ups, not to mention the lost productivity and frustration of restoring their accounts. Finally, governments are most often the victims of cyber sabotage, cyber espionage, and hactivism, that can have significant national security implications.

To develop the ISTR, Symantec analyzes data from the malicious code intelligence it gathers from more than 133 million client, server, and gateway systems that have deployed our antivirus products. Additionally, Symantec's distributed "honeypot" network collects data from around the globe, capturing previously unseen threats and attacks that provide valuable insight into attacker methods. We also maintain one of the world's most comprehensive vulnerability databases, currently consisting of more than 40,000 recorded vulnerabilities (spanning more than two decades) affecting more than 105,000 technologies from more than 14,000 vendors.

Spam and phishing data are captured through a variety of sources, including the Symantec Probe Network, a system of more than 5 million decoy accounts, MessageLabs™ Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics, as well as other Symantec technologies. Data is collected in more than 86 countries around the globe. Over 8 billion email messages, as well as over 1 billion Web requests are processed per day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the Symantec ISTR XVI, in which we observed five key threat landscape trends in 2010.

1. Targeted attacks continue to evolve

The year 2010 was book-ended by two significant targeted attacks, including Hydraq (a.k.a. Aurora) and Stuxnet. While there were some major differences observed in these attacks such as scale, motivations and

[2] *Symantec Internet Security Threat Report XVI, April 2011.* http://www.symantec.com/business/threatreport/index.jsp

backgrounds of alleged attackers, they had one thing in common – their victims were specifically targeted and compromised, even though many had implemented security measures.

Stuxnet was a game changer, exemplifying just how sophisticated and targeted threats are becoming. It demonstrated the vulnerability of critical national infrastructure industrial control systems to attack through widely used computer programs and technology. Stuxnet also served as a wake-up call to critical infrastructure owners and operators around the world. It was the first publicly known threat to target industrial control systems and grant hackers vital control of critical infrastructures such as power plants, dams and chemical facilities.

Another type of targeted attack is known as "spear-phishing." While the high-profile, targeted attacks that received a high degree of media attention such as Stuxnet and Hydraq attempted to steal intellectual property or cause physical damage on a major scale, spear-phishing attacks simply prey on individuals for their personal information. In 2010, for example, data breaches caused by hacking resulted in an average of over 260,000 identities exposed per breach—far more than any other cause. Breaches such as these can be especially damaging for enterprises because they may contain sensitive data on customers as well as employees that even an average attacker can sell on the underground economy.

2. Hide and seek (zero-day vulnerabilities and rootkits)

Though not always necessary to carry out effective targeted attacks, zero-day vulnerabilities often play a role. A zero-day vulnerability is one for which there is sufficient public evidence to indicate the vulnerability has been exploited in the wild prior to being publicly known. In 2010, Symantec observed 14 new zero-day vulnerabilities, an increase from 12 in 2009. Stuxnet is a notorious example, as it used an unprecedented four of these zero-day vulnerabilities. Of course, all vulnerabilities can pose a risk. Symantec documented a total of 6,253 new vulnerabilities in 2010, a 30 percent increase over 2009 and more than in any previous reporting period. The number of new vendors affected by vulnerabilities also increased to 1,914, a 161 percent increase over 2009.

Attackers also leveraged rootkits to evade detection, allowing the threat to remain running on a compromised computer longer, and thereby increasing the potential harm it can do. A rootkit is a collection of tools that allow an attacker to hide traces of a computer compromise from the operating system and, by extension, the user. They use hooks into the operating system to prevent files and processes from being displayed and prevent events from being logged. For example, if a Trojan (malicious software programs that masquerade as benign applications or files), or a backdoor is detected on a computer, the victim may take steps to limit the damage, such as changing online banking passwords and canceling credit cards. However, if the threat goes undetected for an extended period, this not only increases the possibility of theft of confidential information, it also gives the attacker more time to capitalize on this information.

3. Social networking + social engineering = compromise

Social networks continue to be a security concern for organizations, as government agencies and companies struggle to find a satisfactory compromise between leveraging the advantages of social networking, and limiting the dangers posed by the increased exposure of potentially sensitive and exploitable information. Malicious code that uses social networking sites to propagate remains a significant concern. Dumpster diving for paper-based personally identifiable information has now given way to the riches of social networking sites where individuals and organizations readily post their most sensitive information.

Attackers can gather other information from social networking sites that can indirectly be used in attacks on an enterprise. For example, an employee may post details about changes to the company's internal software or hardware profile that may give an attacker insight into which technologies to target in an attack. All it takes is a single negligent user or unpatched computer in the employee's list of friends to give attackers a beachhead into the organization from which to mount additional attacks on the enterprise -- from within, often using the credentials of the compromised employee.

Another one of the chief concerns is the popularity of shortened URLs. Attackers are increasingly using shortened URLs because they can obscure the actual destination of the link from the user. Potential victims are unable to quickly determine where the URL will send them, leaving them more vulnerable to a phishing scam or malware infection. A favorite method used to spread an attack from a compromised social networking profile is to post links to malicious websites from that profile, so that the links appear in the news feeds of the victim's friends. During a three-month period in 2010, nearly two-thirds of malicious links in news feeds observed by Symantec used shortened URLs.

As more people join social networking sites and the sophistication of these sites grows, it is likely that increasingly complex attacks will be perpetrated through them. Users should ensure that they monitor the security settings of their profiles on these sites as often as possible, especially because many settings are automatically set to share extensive, potentially exploitable information.

4. Attack kits get a caffeine boost

While targeted attacks are focused on compromising specific organizations or individuals, attack toolkits attempt to exploit anyone unfortunate enough to visit a compromised website. In 2010, attack toolkits continued to see widespread use with the addition of new tactics. A typical toolkit today is built to allow the criminal to monetize infected machines in every way possible. Not only can it record everything a user types on a system (keystroke loggers are a simple way to capture any password a user types in), but it can also steal email addresses found on the machine (to sell to spammers or to attack other users) and add additional malware to the machine at any time (remote access allows the criminal to download and execute any file they want).

Web attack toolkits are similar to "off the shelf" products that automatically create obfuscated html code containing exploits. They are user-interface driven and can even collect stats on how many users have been infected by their "product." The organized nature of attack toolkits and their ability to self update over the Web, greatly increase the speed at which new vulnerabilities are exploited and spread.

One of the most significant attack kits , known as the Zeus Trojan, is a favorite of cybercriminals, due to its ease of use and low cost (about $400) in the underground economy. It takes little to no technical knowledge to launch this attack, and it can be extremely profitable for cybercriminals. Several gangs using Zeus have been charged with theft in the millions of dollars.

We are also seeing an increase in the prevalence of "shot gun attacks," whereby web attack kits make it easy to blast many different attack vectors at once. Today it is not unusual to see single attacks that target tens - if not hundreds - of different weaknesses in a user's defenses, increasing the chances for success.

Globally, the number of Web-based attacks per day increased by 93 percent in 2010 compared to 2009. Since two-thirds of all Web-based threat activity observed by Symantec is directly attributed to attack kits, these kits are likely responsible for a large part of this increase.

5. Mobile threats increase

As more users download and install third-party applications for mobile devices, the opportunity for installing malicious applications is also increasing. Most malicious codes now are designed to generate revenue. Hence, there will likely be more threats created for these devices as people increasingly use them for sensitive transactions such as online shopping and banking. Trojans that steal data from mobile devices, and phishing attacks, will likely be some of the first of these threats to arrive.

In a sign that the mobile space is starting to garner more attention from both security researchers and cybercriminals globally, there was a 42 percent increase in the number of reported new mobile operating system vulnerabilities, from 115 in 2009 to 163 in 2010.

Currently, the majority of malicious code for mobile devices is in the form of Trojans that pose as legitimate applications. These applications are uploaded to mobile application marketplaces where users download and install them. In some cases, attackers may take a popular legitimate application and add additional code to it. On the horizon, we also are seeing proofs of concept for stealing information off mobile memory cards and the running of botnets on mobile devices.

REAL-WORLD IMPACTS

Symantec has conducted a number of recent studies and surveys to look more closely at the real-world impacts that today's cyber threats have on critical infrastructures, corporate enterprises, small businesses and consumers. A number of these findings are highlighted below.

- **Norton Cybercrime Report 2010: Human Impact**

In 2010, Norton, the consumer division of Symantec, conducted a groundbreaking global study exposing the alarming extent of cybercrime and the feelings of powerlessness and lack of justice felt by its victims. The *Norton Cybercrime Report 2010: Human Impact*[3] study included more than 7,000 adults from 14 countries.

The study revealed that 65 percent of adults worldwide report being a victim of cybercrime, and most of those surveyed expect to be scammed or defrauded online at some point, with less than one in 10 people saying they feel 'very' safe online. In addition, 79 percent do not expect cybercriminals to be brought to justice, indicating a growing prevalence of fear and trepidation associated with Internet usage, along with a general theme of powerlessness. Further, the study showed that most victims take an average of 28 days, at an average cost of $334 to resolve a cybercrime attack.

- **Symantec Consumerization of IT from the End User's Perspective Survey**

The *Symantec Consumerization of IT from the End User's Perspective Survey*[4] revealed that the number of employee-owned endpoints is growing. The growing uptake of smartphones and tablets, and their increasing connectivity and capability, has resulted in a rise in the number of users downloading and installing third-party applications for these devices. This in turn increases users' security risk exposure of installing malicious applications. In fact, the same study revealed that 52 percent of respondents felt that employee-owned endpoints somewhat compromise security and increase data loss threats. While employers are

[3] *Norton Cybercrime Report 2010: Human Impact.* www.norton.com/cybercrimereport
[4] *Symantec Consumerization of IT from the End User's Perspective Survey, May 2011.* http://www.symantec.com/connect/blogs/survey-results-consumerization-it-end-user-s-perspective-2

communicating mobile device security policies and/or best practices, they are primarily dealing with the loss or theft of devices, with malicious apps still taking a backseat, leaving the employer's and the employee's information vulnerable.

Companies must not underestimate the impact of data breach as a result of the consumerization of IT and mobility of employees. This creates security gaps in business processes, increasing the likelihood and extent of data loss threats. Accordingly, there is an urgent need for companies to address these issues and take action to reduce the level of security and data loss risks to which they are exposed. Enterprises need to understand what and how endpoints are being used in their organizations, identify where and how their sensitive data is being stored and accessed, and establish criteria and data security policies to manage, govern and enforce compliance across the corporation.

- **Symantec 2011 Small & Mid-sized Business Disaster Preparedness Survey**

The global threat landscape underscores the need for small and mid-sized businesses (SMBs) to evaluate their current security policies to ensure they are prepared for today's risks. In January 2011, Symantec released the *Small and Mid-sized Business Disaster Preparedness Survey*[5] in which we found that SMBs are still not taking disaster preparedness seriously when it comes to their IT systems. Half of the SMBs we surveyed said they do not have a plan, 52 percent do not think that computer systems are critical to their business, and 40 percent say data protection is not a priority.

According to the study, 65 percent live in areas prone to disasters, and in the past year, SMBs experienced an average of six IT outages. If SMBs aren't prepared for that risk, the impact of a potential disaster, whether natural or manmade, can be expensive. An IT outage costs SMBs an average of $12,500 per day if their computers are down, not including its effect on their customers (which averaged $10,000 per day). In fact, 54 percent of SMB customers switched SMB vendors due to unreliable computing systems, and 29 percent of customers indicated that they lost "some" or "a lot" of important data such as credit card information, patient records, or other financial information.

- **Symantec 2010 Critical Infrastructure Protection Survey**

Our nation's critical information infrastructure is characterized as including businesses and industries whose importance is such that if their cyber networks were successfully breached and disabled, it could result in a threat to national security. The vast majority of the nation's critical infrastructure is owned and operated by the private sector. In August 2010, Symantec commissioned a Critical Infrastructure Protection (CIP) Survey to assess the level of attacks against and the readiness of owners and operators. The survey included 1,580 enterprises in 15 countries worldwide, with companies ranging from 10 employees to more than 10,000. The median company size was between 1,000 and 2,499 employees. We focused on six key critical infrastructure segments: Energy, Banking and Finance, Communications, Information Technology, Healthcare, and Emergency Services.

We discovered that the threat of such attacks is real and organizations will continue to be at risk of being targeted by specific attacks. *Symantec's 2010 CIP Survey*[6] included the following highlights:

---

[5] *Symantec Small & Mid-sized Business Disaster Preparedness Survey*, January 2011.
http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=dpsurvey&om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpsurvey

[6] *Symantec Critical Infrastructure Protection Survey*, September 2010.
http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf

- Critical infrastructure providers are being attacked. Fifty-three percent of companies suspected experiencing an attack waged with a specific goal in mind. Of those hit, the typical company reported being attacked 10 times in the past five years. Forty-eight percent expect attacks in the next year and 80 percent believe the frequency of such attacks is increasing.

- Attacks are effective and costly. Respondents estimated that three in five attacks were somewhat to extremely effective. The average cost of these attacks was $850,000.

- Industry is willing to partner with government on CIP. Nearly all of the companies (90 percent) said they have engaged with their government's CIP program, with 56 percent being significantly or completely engaged. In addition, two-thirds have positive attitudes about programs and are somewhat to completely willing to cooperate with their government on CIP.

- Room for readiness improvement. Only one-third of critical infrastructure providers feel extremely prepared against all types of attacks and 31 percent felt less than somewhat prepared. Respondents cited security training, awareness and comprehension of threats by executive management, endpoint security measures, security response, and security audits as the safeguards that needed the most improvement.

NEW TECHNOLOGIES = NEW RISKS & REWARDS

Virtualization and cloud computing promise the next wave of technological evolution in the way we manage desktops as well as data centers. However, with rapid adoption of new technologies come new risks. As highlighted in the Symantec ISTR XVI, the increased use and relative simplicity and effectiveness of attack kits has contributed to their increased use in cybercrimes — these kits are now being used in the majority of malicious Internet attacks. This new trend has attracted traditional criminals who would otherwise lack the technical expertise in cybercrime, fuelling a self-sustaining, profitable, and increasingly organized global underground economy. Cybercriminals who are financially motivated are now able to easily launch malware anytime and anywhere, stealing confidential information such as customer credit card information or intellectual property, from enterprises or end-users. Existing technological solutions suggest that detection capability of these targeted attacks would be a lot more effective on the cloud than on the desktop.

With 80 percent of respondents globally planning to use cloud computing much more intensively two years from now, (according to a survey conducted by the Ponemon Institute for Symantec[7]), the cloud's growing popularity will increase the risk of being targeted by cybercriminals. However, despite widespread interest and benefits in adopting cloud computing technologies, many organizations are still 'flying blind' with respect to making them secure, potentially putting their business operations, company data and customer information at risk. Most organizations lack the procedures, policies and tools to ensure that sensitive information they put in the cloud remains secure. In fact, the same study revealed that only 27 percent of respondents said their organizations have procedures for approving cloud applications that use sensitive or confidential information.

[7] Ponemon Institute, *Flying Blind in the Cloud: The State of Information Governance*, April 2010. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-ponemon_institute_flying_blind_in_the_cloud_WP.en-us.pdf

These findings indicate the need for IT managers to be more involved in the deployment of cloud computing services within their organizations. At Symantec, we believe the success of the cloud computing model hinges on the level of trust and confidence between service providers and service consumers. Vendors and service providers that can successfully address the security, compliance and privacy challenges will be the winners in the era of cloud computing.

If cloud security is appropriately implemented, there is an array of benefits to be gained, from efficiency to improved and more rapid protections. Security benefits include:

- Increased visibility because it is possible to more easily identify attacks and suspicious behavior where data from multiple sources is aggregated together.
- Scaling advantages as large cloud providers can invest in sophisticated monitoring and dedicated security personnel that are shared across a customer base where any single customer may not be able justify the cost. The same advantages exist for a cloud provider investing in multiple data centers and connectivity for redundancy.
- Should an issue be detected in a cloud environment that affects one single customer, the issue can be fixed once and the protection is shared across the entire customer base, even if they are not (yet) exposed to the new threat.
- The existence of a cloud layer provides for an additional layer of defense, thereby increasing the strategic depth of the defender and the layers of security that the attacker needs to successfully penetrate.

However, over and above providing hosted security services, it is critical for organizations to view and manage their security environment in a holistic manner – both on-premises and in the cloud. Interoperability between on-premise security tools and cloud-based tools is critical. These entities must work together to maximize the security benefits that they both bring.

To ensure the security and success of cloud computing, Symantec sees the critical need for security to evolve in the following areas:

- Ensure that policies and procedures clearly state the importance of protecting sensitive information stored in the cloud. The policy should outline what information is considered sensitive and proprietary.
- Organizations should adopt an information governance approach that includes tools and procedures for classifying their information and understanding risk so that policies can be put in place that specify which cloud-based services and applications are appropriate and which are not.
- Evaluate the security posture of third parties before sharing confidential or sensitive information. As part of the process, corporate IT and/or information security experts should conduct a thorough review and audit of the vendor's security qualifications.
- Prior to deploying cloud technology, organizations should formally train employees on how to mitigate the security risks specific to the new technology to make sure sensitive and confidential information is protected.

In other words, when discussing threat protection, especially technological threats, one needs to remember that the world is changing rapidly, therefore the technology and security has to keep up. The strive for security is very much a moving target and we must continue to stay ahead of the curve to protect our data and our networks.

PROTECTING NETWORKS AGAINST THREATS & PREVENTING DATA LOSS

Deployment and management of an anti-malware solution is the first step in network protection. But this solution alone does not provision the entire security landscape. You must also be constantly watching out for and monitoring vendor security notifications and alerts, and apply needed patches or workarounds as soon as possible. Ensuring that users are kept up to date through a security education and awareness program is vital to keeping networks secure. Last, but not least, know your assets, identify your perimeter of secure operations, and maintain a high level of situational awareness to ensure you are aware of, and can respond to, incidents in a timely manner for the sake of operational survival.

In light of the current key threat trends, and recent high-profile cases such as WikiLeaks and other data breaches, it has also become critical for all organizations to establish and implement a sustainable data loss prevention (DLP) program that effectively addresses evolving risk factors. A comprehensive, long- term, sustainable DLP program is based on the following principles:

- **Threat coverage:** Information must be protected wherever it resides, whether at-rest, in-motion or in-use. This requires control points at multiple tiers (i.e. endpoint, gateway, network, back-end databases). Further enhanced compatibility with a cloud environment and Web 2.0 sites provides a more transparent Web experience for end-users that seamlessly prevents data exposure.
- **Data Insight:** DLP should help enterprises identify their most critical information and enable simplified data clean-up and remediation through automated data owner identification. Besides continuous monitoring and auditing of data usage DLP needs to ensure adherence with corporate policies and regulatory compliance.
- **Business Process Integration:** DLP must be incorporated into an organization's overall business process so that it is viewed as a business necessity, aligned with strategic goals, compliance requirements and risk management.
- **Risk Reduction Measurement:** Enterprises should define achievable and measurable goals and then regularly review progress against them and hold business leaders accountable for meeting them.
- **Identify critical information and simplify remediation:** Effective DLP solutions should include a unified platform that allows customers to create policies once, and enforce them everywhere to prevent confidential data loss across endpoint, network and storage systems. Integrated DLP technology helps enterprises align their information assets to business goals by simplifying the remediation of exposed critical data.

To reduce the risk of data breaches, organizations require a clear understanding about where their sensitive data resides and how it is being used. With this insight, organizations will be better placed to identify gaps in their strategy, better equipped to define their requirements, and better prepared to implement a data governance plan that will reduce their risk posture.

ENSURING RESILIENCY AGAINST CYBER ATTACKS

We have learned many lessons from Stuxnet and other recent attacks. While the sophistication level of attacks is increasing, as is the potential and real damage caused by such attacks, we must turn these lessons into action. Symantec recommends the following steps be taken in order to better protect critical systems from cyber attack:

- **Develop and enforce IT policies** and automate compliance processes. By prioritizing risks and defining policies that span across all locations, organizations can enforce policies through built-in automation and

workflow and not only identify threats but remediate incidents as they occur or anticipate them before they happen.

- **Protect information** proactively by taking an information-centric approach. Taking a content-aware approach to protecting information is key in knowing who owns the information, where sensitive information resides, who has access, and how to protect it as it is coming in or leaving your organization. Utilize encryption to secure sensitive information and prohibit access by unauthorized individuals.
- **Authenticate identities** by leveraging solutions that allow businesses to ensure only authorized personnel have access to systems. Authentication also enables organizations to protect public facing assets by ensuring the true identity of a device, system, or application is authentic. This prevents individuals from accidentally disclosing credentials to an attack site and from attaching unauthorized devices to the infrastructure.
- **Manage systems** by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.
- **Protect the infrastructure** by securing endpoints, messaging and Web environments. In addition, defending critical internal servers and implementing the ability to back up and recover data should be priorities. Organizations also need the visibility and security intelligence to respond to threats rapidly.
- **Ensure 24x7 availability.** Organizations should implement testing methods that are non-disruptive and they can reduce complexity by automating failover. Virtual environments should be treated the same as a physical environment, showing the need for organizations to adopt more cross-platform and cross-environment tools, or standardize on fewer platforms.
- **Develop an information management strategy** that includes an information retention plan and policies. Organizations need to stop using backup for archiving, implement de-duplication everywhere to free up resources, use a full-featured archive system and deploy data loss prevention technologies.

Cybercrime is an ever-evolving threat, and there is no single solution to prevent attacks. Bad actors are getting smarter and more resourceful every day and we must continue to be vigilant to protect our economy, our national security, and our way of life. Symantec applauds Congress and the Administration for focusing much needed attention on this serious issue and making it a high priority, and we look forward to continuing the important dialog around cybersecurity legislation.

Symantec would like to thank the Committee for the opportunity to testify today. We remain committed to continuing to work in coordination with Congress, the Administration, our industry partners and customers, and the public to secure the nation's infrastructure from cyber attack.

Mr. CHAFFETZ. Thank you.

We will now start the questioning. I am going to recognize myself for 5 minutes—maybe even a little bit longer than that.

I appreciate all the expertise and routinely what we hear is the threat, the threat, the threat, it is happening and we are quantifying something at $86 billion and perhaps beyond. I do think there are probably a number of companies that would be embarrassed to allow it out there that there was some sort of security breach.

We are constantly told that it is consumers and shoppers, that it is safe and secure to type in our critical information, our personal information just because it has that little lock on there. What should the average person in Topeka, Kansas be thinking about when they go type in, how do you really tell if it is secure or not and can you ever? Do you want to take a stab at that, Mr. Bond.

Mr. BOND. I will take a first stab at it, Mr. Chairman. I think I would urge consumers to do what a national education campaign has urged which is stop, think and connect. Many of these newly designed threats that come in and pose as something they are not, trying to get you to either give information or simply click on a bogus connection which very often can be understood, gleaned or perceived as a threat by simply stopping and thinking through, wait a minute, is this really coming from the company or an entity that it purports to be.

This links to issues about short address names and other things that are part of the challenge right now, but I do think that a public education campaign that tells people to stop and think before they connect can have measurable impact. That is a beginning point.

Mr. Chaffetz. Certainly the success of Twitter and Facebook and particular networks has become immense globally. Mr. Lewis, what sort of threat or danger to young people, old people, people who participate on those types of social networks exists? How secure, if at all, is the information that is provided?

Mr. BOND. The intent with information is to be public, so it is easily collected. We know there have been many problems in the past. One of them, my favorite in some ways, is the fact that people will often use their pet's name or birthplace as their password and then they will list it on the Web site, so we have seen many, many incidences where guessing the password on these sites isn't that difficult.

We are a treasure trove for cyber criminals because you can harvest all kinds of data that will give you hints on passwords, employment, where you bank is, so they have become kind of unmanageable problems. There is little the companies can do about that. I don't want to blame Twitter or Facebook or any of them. People choose to put their information up there and they haven't thought enough, as you heard from Phil, about what the implications are. If you are going to have a Facebook account, don't use your dog's name as the password.

Mr. Chaffetz. Mr. McGurk, I would like to learn a bit more about the differences or perhaps the similarities between cyber attacks from domestic and international sources. Are there distinguishable differences or motives between the domestic and the international actors?

Mr. MCGURK. In the Department, as I mentioned earlier during my testimony, we are focused more on the risk mitigation strategy, so when we look in the national infrastructure protection plan, at the definition of risk, we identified as threat, vulnerability and consequence. The Department takes an all hazards approach.

The challenge there is identifying where the threat actors are originating. That is a part of it but from our standpoint, from the mitigation standpoint, in protecting the networks, restoring services and recovery, the actual source is not as important as the vulnerability and the consequence of those vulnerabilities. That is really where the Department focuses most of its attention and how to provide actionable intelligence to the asset owners and operators to prevent further escalation of the consequences of the breach.

Mr. CHAFFETZ. How far and wide are you doing that? You are doing that, I would assume, with the national interest, the Federal assets that we have. What about the private sector? How involved do you get with them? There is obviously Microsoft, Goggle and Yahoo in the world, but there are also your medium level guys. How interactive are you, can you possibly be where there will be virtually every single entity you could possibly think of?

Mr. MCGURK. One of the areas we focus on in NCCIC is our assist and assess mission where we actually send incident response teams and assessment teams out into the field. We have gone to companies of only seven employees that were experiencing cyber intrusion to Fortune 10 companies, working with them to not only identify what the risk is but to mitigate that risk in their cyber environments.

On average, a week does not go by where I do not have a team in the field working with the private sector to address those cyber vulnerabilities and to mitigate those risks.

Mr. CHAFFETZ. What percentage of the companies can you possibly get to?

Mr. MCGURK. Again, to date, we have been able to conduct 75 risk assessments over this past year. We have not had the opportunity or the requirement to turn anyone away. It is completely voluntary. Part of the challenge is when a risk, threat or intrusion is identified to the Department, we will respond in kind with a team of cybersecurity experts to assist in restoring services. Again, that is a matter of the request coming from industry.

Mr. CHAFFETZ. Yes, Mr. Bond?

Mr. BOND. I want to observe here that this is where the power of the network can be tremendously valuable. DHS does not to physically go out and talk to every company. We do need timely, actionable sharing of information so that the network, led by great vendors like Symantec and others, and then proliferate and spread that word to address whatever the vulnerability is at the earliest possible stage as soon as we know about the threat.

You will uncover, through the committee's efforts and hearings, that there are information sharing challenges between the government and private sector, between the private sector and the private sector.

Mr. CHAFFETZ. Thank you. My time has expired. I will now recognize Mr. Tierney for 5 minutes or whatever he would like.

Mr. TIERNEY. I am trying to work out something in my mind that Mr. Bond got me thinking about as he was talking, about who is responsible for what, liability protections, incentives and all of that.

I understand with respect to our national security concerns and homeland protection, being a part of that, that the government systems, we have the responsibility, we have to take care of it and move on from that, but in terms of the private sector, when you are not doing business with the government, why isn't that on you? Why isn't it on you to make sure that your systems are protected?

I see Mr. McGurk has teams running all over the place doing what I would have thought was your job, making sure you are safe, making sure nobody can get into your system, making sure consumer information is protected. If you don't do a good job of that, I suspect people aren't going to buy your product or utilize your services. I don't know why we have to give you incentives and I don't know why you wouldn't be held liable if you make a mess of it.

Mr. BOND. It is an important observation because we believe market forces are primary to shaping good behavior and we see that time and again. However, let me try to give you an example.

If a small community is targeted, say the bank in that community is targeted because they want to get personal information or financial information because there may be a lot of DOD workers in that community, the Federal Government says, gee, that small community bank has somehow been breached and we need you to go off line for a minute to help figure this out and because it is a serious threat.

Mr. TIERNEY. Let me back up. The government didn't supply that system to that bank?

Mr. BOND. No.

Mr. TIERNEY. If it is breached, let's say there aren't any government workers in that area?

Mr. BOND. That is not the point of liability. For their inability to provide a secure system, there are going to be questions about a community bank in the future, but while they are down because of a government request or demand and Farmer McDonald doesn't get his loan or loses the farm, is the bank liable because they went down at the government request?

Mr. TIERNEY. Forget the bank, the bank didn't put the system in, they bought it from somebody and paid for the service of installing it. If it goes down, whether it goes down because somebody breached it, the government suggests they go down or whatever, it is still their fault and their problem. Why wouldn't all the responsibility and obligation lie with them, not lie with the government in protecting national security? We don't assess the government every time they come in and protect us, but the people who go out and sell to a bank in a community, that they are going to give them a system that is safe and secure, why doesn't the buck stop there?

Mr. BOND. I am trying to make a distinction that I think is legitimate. When the government says, based on what we know, you should do this or we require you to do this and you do that, any liability that stems from that step should be protected because you are doing something in accord with policy or government request.

Mr. TIERNEY. You wouldn't do it on your own is what you are saying, look and see what happened, figure you have to put in those safeguards of your own volition?

Mr. BOND. You would and I am failing to communicate.

Mr. TIERNEY. No, you are not. I am just failing to accept your premise. It is not that you are failing to communicate. For whatever reason you have to do something, it seems a customer would want you to do and expect you to do, I don't understand the shifting of responsibility and obligation.

Mr. BOND. If it is an action taken at government requirement or policy, I don't think it is the government's intent to make a company liable for obeying the law.

Mr. TIERNEY. Let us take your example, which I thought was the most favorable position you could take for yourself. A lot of people work in the government, Department of Defense or something, living in a particular neighborhood doing business with a credit union or a bank and the system someone in private industry installed was secure, goes down and there is a breach, you are telling me if the government tells you to shut it down, or the government tells you how to bring it up safely, you wouldn't come across that on your own and if you didn't come across that, the government had to take action, therefore you shouldn't be responsible for anything that results from you taking those steps.

One of two things can happen. You are going to try to resolve it yourself or somebody is going to have to suggest to protect the consumers and the community that it is going to be done, then you say if I do it the way they say do it, because I wouldn't do it on my own, then I am going to be shielded the responsibility or liability. Is that your position?

Mr. BOND. No, but I appreciate your framing it for me. What I am trying to underscore is that when there is a policy or something in place that has a requirement to it that there not be liability attached to it being the requirement. I could think of a lot of different examples but if you are adhering to the rules and best practices, and something about that policy causes harm as a response, that is something you are obeying policy on and you should not be liable.

Mr. TIERNEY. How do we ever get best policies to keep getting better if you never have an incentive to do it because you are covered—the threshold thing that is in place at a given time?

Mr. BOND. I could reverse it and say why would you ever obey the government rule if you also not protected when obeying that rule?

Mr. TIERNEY. Maybe we don't have a government rule. Maybe we just leave you out there to the market, so when you go down and that community goes down or whatever, then you are on your own. Would that be something you want, no consumer protections, no government regulations, would that make you happier?

Mr. BOND. I am taking your earlier point that market forces really do matter, but I am trying to make the point that if we pass rules and companies obey those rules, that should not usher in some liability because you obeyed the rule.

Mr. TIERNEY. I am not trying to be contentious with you, I am trying to get to the bottom. I think it is an interesting question to

ask, but there be no government regulations in this area. Mr. Bond, go ahead.

Mr. BOND. I am not advocating that. I think there are already some regulations in place, certainly around the government systems and how they interact with private sector systems, contractors and others.

Mr. TIERNEY. Other than that, should there be any government regulations on your provision of systems to private entities at all or should it just be totally unregulated?

Mr. BOND. I think that is a good question we should look at, what is the use of standards, what is the use of industry best practices and other things that government and the private sector are coming up with together and that any regulatory steps should be taken very carefully with all the expertise of the different players in the room.

I am not here to draw any kind of line in the sand, I am here to say that you need technical experts like Mr. Turner and others in the room to understand what the implications in an interconnected world.

Mr. TURNER. Just to add to that, I think it is important when we are discussing liability, we acknowledge the fact that it is incredibly difficult to pin where that liability sets. There is no such thing as a 100 percent secure, fool proof piece of software. It doesn't exist out there, I am sorry to say. Vulnerabilities are a fact of life.

Mr. TIERNEY. But there was never a 100 percent secure train either, but at some point liability went to the locomotive company because technology had advanced to the point where they were the ones to be held responsible for anything.

Mr. TURNER. I understand but when you are asking to assess liability on a particular focal point, whether that be the Federal Government, the private sector or the vendor, we have to deal with something called the law of unintended consequences. It is virtually impossible for us, as an industry or anybody, to be able to test with 100 percent certainty how that particular product, software or service is going to be used in that situation.

Mr. TIERNEY. A product liability system has never gone on 100 percent certainty, who is responsible and then people make a decision about what is reasonable. I was trying to figure out whether it is reasonable to leave it all to the industry to set the standards and suffer whatever consequences or obligations there might be or is there some advocacy here that the government should, on behalf of the consumer, whoever that might be, a business or an individual, set some standards for compliance and I haven't figured out whether you are for or against yet.

Mr. TURNER. I suspect you will find that the answer lies somewhere in the middle, that it is again the public/private partnership.

Mr. LEWIS. Can I add something, Mr. Chairman, because it is an interesting line of questioning. There is a point we might want to put out in the open and I think if you would use your experience and the experience of other committee members with the intelligence community, you would be able to confirm this, but there is no such thing as a secure, unclassified system. I have been told by senior intelligence officials that they have never seen an unclassi-

fied system that has not been penetrated. We are dealing with a problem where anyone can get in. The solution to that is not a technological solution.

Yes, over time, our technologies will get better and that will squeeze out the low end threat, so the high school kid who used to be able to break in in a couple of hours now he might have to spend a little more time. I think that is why a lot of us are in favor of a comprehensive approach. You need to have law enforcement cooperation with other countries. You need to have strong military forces to deter potential opponents. You need to work with the service providers to get them to help consumers and you do need some kind of what we are calling now risk-based standards run through the government that would impose some requirements on at least critical infrastructure companies.

If we can get a package together, we can deal with the problem, but no single part will solve this very damaging situation.

Mr. TIERNEY. I guess what I am taking from that is you don't feel you can do your optimum job without the assistance of the government in some respect, is that fair to say? You are all talking about partnerships. I am guessing what the industry is saying is we can't do this right without government assistance at some level.

Mr. BOND. I think I would say that we absolutely need and welcome government involvement around the critical infrastructure and as they do that, we want to make sure experts are in the room because these are very complicated and interconnected issues. That is simply it.

Mr. CHAFFETZ. Mr. McGurk, as we talk about the threat, where do you see the biggest threats outside of the domestic United States? What are the biggest threats? Where do you see them coming from?

Mr. MCGURK. Again, focusing on the total consequence and vulnerability aspect, the threat actors range in sophistication and capability from nation state-sponsored through criminal activity down to a hactivist, entirely into what we call the script kiddie environment.

Mr. CHAFFETZ. How many nations are attacking this country on the cybersecurity front, how many nation actors?

Mr. MCGURK. The challenge with that was the point made earlier by some of the members of attribution. It is very difficult to positively attribute known activity. Even if I were to say an IP address or the source address originated in a particular country or a particular area, that may not be actual actor, so the attribution piece is very difficult.

Mr. CHAFFETZ. I recognize that it is difficult, but you have some number that you have assessed, at least I hope you do. What is that number, how many countries?

Mr. MCGURK. I would actually defer that to the intelligence community representatives in another forum. I wouldn't be able to comment on that here today.

Mr. CHAFFETZ. What is the consequence for somebody who is attacking us on the cybersecurity front? Is there anything we can do or have done? Is there any instance where we have actually said, Country X, you have been doing this and this is the consequence? Is there any consequence to that?

Mr. MCGURK. To my knowledge, I am not familiar with any official demarche that has ever been issued or ever been delivered to a particular nation state associated with malicious cyber activity.

Mr. CHAFFETZ. How often are we getting attacked from nation states—daily, hourly?

Mr. MCGURK. There are hourly cyber attacks. Whether they originate and are state-sponsored or if they just originate from IP addresses that are being spoofed as far as the location, if they are criminal activity or if they are independent activists that are operating under the protection of a nation state.

Mr. CHAFFETZ. Let us pretend we have a nation state that says yes, what is the consequence? What do we do?

Mr. MCGURK. Not necessarily dealing in hypotheticals, but looking at the consequence analysis that the Department conducts associated with cyber physical systems, one of the demonstrations we conducted in 2007 was known as the Aurora Experiment where we demonstrated the capability of taking digital protective circuits and physically destroying large pieces of rotating equipment. This type of equipment has years to repair or replace.

Mr. CHAFFETZ. That is cool, I like hearing that. What else can we do?

Mr. MCGURK. Subsequently, we recognize we have to apply a defense in-depth strategy.

Mr. CHAFFETZ. I hope we are doing that.

Mr. MCGURK. Yes, sir. In many of these cases, these legacy-based systems are 10, 20 or 30 years old, so subsequently we can't bolt on a new application so we either need to enclave these pieces of equipment in a secure environment or mitigate the risk associated with operating those systems in a connected world.

The comment was made earlier about separating networks and never finding a secure network. In our experience, in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the Enterprise network. On average, we see 11 direct connections between those networks and in some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise environment. That is one of the challenges we have, as I mentioned earlier, in actually securing these networks and understanding the consequences associated with the vulnerabilities and not just the threat actors.

Mr. CHAFFETZ. That doesn't give us much confidence, but it is reality. That is what we are after here.

If I went down the row here, what do you all see as the singlemost, significant weakness in the system right now? I will start with you, Mr. Bond, and then we will loop around and get to you, Mr. McGurk.

Mr. BOND. I would probably identify better information sharing coming between the government and the private sector. I don't think we are sometimes free to discuss the threats we see so that we can respond quickly.

Mr. CHAFFETZ. Mr. Lewis.

Mr. LEWIS. I would go back to your point about consequences. If nobody is ever punished for doing something bad or even chastised,

they are just going to do more of it, so I think our failure to have any consequence for any sort of cyber action is really damaging.

Mr. CHAFFETZ. Mr. Turner.

Mr. TURNER. I would have a tendency to agree with Mr. Bond that information sharing is the key component, but I would also add and rank just as highly that we need to start moving away from the mindset in which we currently find ourselves which is detection and remediation. This is the cycle we are in, we detect and remediate, detect and remediate. We are always behind the curve. We need to get a little more predictive and a little more proactive in terms of reaching out which sort of dovetails into Mr. Lewis' comment about the consequences for actions.

Mr. CHAFFETZ. Mr. McGurk.

Mr. MCGURK. Thank you for the opportunity to last because I would say all of the above.

Mr. CHAFFETZ. I agree with you.

Mr. MCGURK. If I may add on the information sharing piece, arguably we have been sharing information for years between the government and the private sector. We need to focus on collaboratively developing knowledge so that we can provide actionable intelligence to mitigate the risk.

The great example of that was in November of last year, there was a particularly malicious piece of code known as the "Here You Have" virus. It was actually identified through the intelligence community as being a known malicious piece of software and within hours, the Department was able to identify that particular piece of code and provide actionable intelligence to the community through a series of declassification measures using the private sector's expertise to provide information to the private sector so they could take the necessary steps to mitigate the risk.

That is the step we need to do to actually have an effect on cyber risk at that speed and not just simply put together another information sharing body.

Mr. CHAFFETZ. I want to go quickly here to the cloud. There is a lot of movement within the industry to encourage people to store their information on the cloud which creates questions about security and do I trust some major provider more than I trust my own local server, do I think it is more safe than my individual computer.

What are the vulnerabilities there? Should be feel more secure, more safe with cloud and movement to the cloud or less? Let us start with Mr. Lewis this time.

Mr. LEWIS. You caught me off guard, Mr. Chairman. Right now, I would say there is probably a slight advantage to having your stuff in the cloud because some of the companies, some of the service providers can devote more attention, particularly for small and medium size enterprises. They may actually benefit from having a big company—a Google or a Microsoft or an IBM—manage their data. There are other drawbacks to it.

For large enterprises, I am not sure they benefit and a lot depends on how well the cloud service providers actually do. On the whole, small companies are better off. Big companies may be a wash.

Mr. CHAFFETZ. Mr. Turner.

Mr. TURNER. I agree with Mr. Lewis in a sense. I do think, however, enterprises do benefit because a lot of what we are seeing in the move to the cloud is driven by total cost of ownership and reduction of costs, and so forth. From a security perspective, it is going to be contextual because you are going to have to ask yourself those very important questions about with whom do I trust my data. That is going to come down to reputation and past behavior.

It is not meant to be a pitch but that is certainly the case in the questions that have to be asked. If they don't, there will be a lot people, as we move to the cloud, that will be able to make these services available whether they be onshore in the United States or offshore and these other places. What is the track record going to be? We have to make a very clear and very careful assessment of the information we are willing to share because not all information could be protected.

Mr. CHAFFETZ. Let me shift here a little, if I could. Mr. McGurk, let us talk about data bases. The Federal Government has over 2,000 data bases. On one hand, you can say maybe that diversified portfolio provides a degree of safety and security, so the Bureau of Indian Affairs is separate from the Department of Justice. I can understand the security component at the Department of Justice is probably a little bit higher than the Bureau of Indian Affairs.

What are the weak links associated with that? Do we want to consolidate those and have five really good data warehouses or data bases or is this diversified portfolio advisable? I worry that so many agencies are trying to create so many things, we are duplicating efforts and consequently, they are all probably not nearly as secure as we want them to be. What is your perception of that?

Mr. MCGURK. I believe it is actually a capabilities versus a requirements discussion. When you talk about the disbursed nature of the data base as in the infrastructure, it goes to the cloud discussion we were just having.

One of the benefits of that secure environment is that you can have a disparate approach to data storage so that not all the keys to the kingdom are in one location. That provides an obscurity model for data in motion and data at rest. By being able to do that, we can better allow for a distributed approach for data security.

That being said, one of the initiatives the Department has been executing for quite some time now is a trusted Internet connection program. That was part of the Comprehensive National Cybersecurity Initiative. Instead of trying to instrument or monitor each of the separate departments and agencies, but we roll that up to an aggregation point so that we can understand flow and control the information access points at an aggregated standpoint and still allow for the diversity of the independent departments and agencies.

Mr. BOND. Just quickly, I want to make sure to offer to brief the committee and its members. Our TechAmerica Foundation actually has 73 companies and academics involved in commission right now to advise the government on the cloud and the leadership opportunity for the US and the cloud. One of the questions they are going to be addressing is the security profile of the cloud. There are leading thinkers who would challenge Jim's assertion and maybe even say the cloud would be more secure for all enterprises.

Mr. CHAFFETZ. Mr. Tierney.

Mr. TIERNEY. Mr. Bond, in your testimony you emphasized the public/private relationship, particularly with respect to education and information sharing. Do you think education and information sharing are sufficient to protect the critical infrastructure from cyber attacks? Do you think that is where we should leave it?

Mr. BOND. No, I think we presume there are going to be special rules, regulations and requirements around the critical infrastructure. We think education jointly identifying where the government should invest R&D dollars in cybersecurity, all will be a part of that ultimate solution. We certainly advocate for clear distinction of what the critical infrastructure, a good definition of it and special requirements for it.

Mr. TIERNEY. In that vein—and I ask this of all of you—the present CEO of the North American Electrical Reliability Corp., a fellow named Gerry Cauley, that you are all probably familiar with, testified before the Armed Services Committee on this topic. He said he didn't think there was clarity of responsibility. He thinks collaboration and consultation have been good but should be based on an ad hoc relationship with clear lines of responsibility and authority. Are you all pretty much in agreement with that or do you disagree?

Mr. LEWIS. In some ways, the electrical grid is the most attractive target we have for some of our opponents. It is not secure, so if the statement he made was that we have been relying on an ad hoc process, I think that is right and there is a lot of room for improvement.

Mr. TIERNEY. Do you know why there isn't a clear line of responsibility? What is the impediment to deciding who will be in charge of this overall, overriding plan we have?

Mr. TURNER. I think part of the issue too is the responsibility in sharing the data itself. What data can you share? There are a whole host of impediments and barriers to sharing what is arguably confidential information in some areas. That is part of the issue I think gets in the way of trying to formalize relationships and put them in a hierarchical order to say this is who is doing this and this is who is doing that. I think that has primarily been holding back even the larger information sharing relationship that goes on between the public and private sector, not limited to that particular sector itself.

Mr. TIERNEY. Can I assume that some countries share this problem and some countries don't depending on the nature of the government in a given country?

Mr. TURNER. I am not so sure it actually comes down to a country by country level, to be perfectly honest with you. I think it is the nature of the issue itself that you are talking about the sharing of that information. This is merely to illustrate a problem with the information sharing network that sometimes when information goes from the private sector to the public sector, it is a one way street. Part of the whole education thing is we have to come to agreement on how we share that information to ensure that there is valuable information that can come back the other way as well.

Mr. LEWIS. On that note, I talked with one of the larger European countries. They have set up something like our Cyber Com-

mand. They were telling me what they had done with their electrical grid and requiring their grid operators to be more secure. I said, that is amazing, how did you guys get away with that? We could never do that. They said, when they privatize, they made sure to keep two board seats.

Where you are seeing a difference emerge is in the countries that still have a small number of service providers, where the government has a more directive role, they are pulling ahead a little bit. Right now, I would say we are all sort of in equally bad shape and one of the trends to watch is whether that changes in a way that disadvantages us.

Mr. TIERNEY. Let me ask one last question of each of you. What do each of you as individuals think the government role ought to be in protecting the infrastructure for private companies? Mr. McGurk.

Mr. MCGURK. I believe the current role we are executing as a coordinator and integrator to provide understanding and awareness across the 18 critical infrastructures is a key role and a service that we provide. As many of my distinguished panel members have said, information may come from one sector and may be germane to another but there is no direct connection to share that information.

By aggregating that at the Department, we are able to take alerts, warnings or indications coming from the electric sector, anonimize that information or identify the vulnerability and provide that to the water sector, the chemical sector or the petroleum sectors. That is a service and capability we provide because we do have broad exposure into each of those 18 critical infrastructures.

Mr. TIERNEY. Mr. Bond.

Mr. BOND. Certainly I would underscore the notion that there needs to be a key role in defining the critical infrastructure and having special requirements for that. The farther out you move on the network and the closer to consumer applications and so forth, I think we need this roundtable of real experts to understand what it means in a networked world because they are all connected and difficult to determine regulatory schemes.

Mr. TIERNEY. Mr. Lewis.

Mr. LEWIS. Three things—some kind of flexible, standard-based approach that I would think DHS and the other regulatory agencies would oversee for critical infrastructure; better information sharing as you have heard; and finally, steps that would make the international environment more secure, steps that would deter criminals and other potential hackers.

Mr. TIERNEY. Mr. Turner.

Mr. TURNER. I would agree with everything that has been said on the panel. Going last, it is easier to do that.

I would add in addition to facilitating information sharing and making it easier, keeping an eye toward that liability. We have to keep in mind that most of the attacks that we see today, the attacks themselves are international in nature, so we are not just dealing with threat actors or threat intelligence that comes from the five I's or the United States alone.

We are also dealing with issues that come from other jurisdictions, other western jurisdictions where the sharing of that infor-

mation is considered, to put it bluntly, very difficult to do and can put you in a lot of hot water. Those issues have to be addressed if we are going to get down to the role where we talk about how do we make it easier for governments to protect the private sector especially when we are talking about critical infrastructure. Those are some of the hurdles we have to address. If we don't address them at the higher level, sharing the information formally at a lower level is difficult. It happens informally now.

I wouldn't want to leave the panel with the impression that we do not share information because that is certainly not the case. I personally have worked with all the levels of the U.S. Government on sharing information about current threats to critical infrastructure but it is in an unofficial capacity because there doesn't exist an official capacity in which we can do that.

Mr. TIERNEY. Thank you.

Thank you, Mr. Chairman.

Mr. CHAFFETZ. I want to thank all the panel members for their participation today and your expertise. If there are additional comments or information you would like to share with us, I would appreciate it.

Mr. McGurk, if you would commit to this committee to help us conduct that confidential briefing, a classified briefing, I should say, we would certainly appreciate that. Is that something you could commit to?

Mr. MCGURK. Yes, Mr. Chairman, it would be my pleasure to help facilitate that.

Mr. CHAFFETZ. That would be great.

Thank you again for your expertise. This is a fast moving industry, it changes every moment and we appreciate your participation. Thank you again for your expertise and your comments.

The committee now stands adjourned.

[Whereupon, at 4:15 p.m., the subcommittee was adjourned.]