AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBERSECURITY: AN OVERVIEW OF RISKS TO CRITICAL INFRASTRUCTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JULY 26, 2011

Serial No. 112–80

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

73–391 PDF WASHINGTON : 2012

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 ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chairman
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

CLIFF STEARNS, Florida
Chairman

LEE TERRY, Nebraska
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
CORY GARDNER, Colorado
H. MORGAN GRIFFITH, Virginia
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

DIANA DEGETTE, Colorado
Ranking Member
JANICE D. SCHAKOWSKY, Illinois
MIKE ROSS, Arkansas
KATHY CASTOR, Florida
EDWARD J. MARKEY, Massachusetts
GENE GREEN, Texas
DONNA M. CHRISTENSEN, Virgin Islands
JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

	Page
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement	1
Prepared statement	4
Hon. Diana DeGette, a Representative in Congress from the State of Colorado, opening statement	7
Prepared statement	9
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, opening statement	11
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement	11
Prepared statement	13
Hon. Donna M. Christensen, a Representative in Congress from the Virgin Islands, opening statement	14
Hon. Henry A. Waxman, a Representative in Congress from the State of California, prepared statement	75
Hon. Fred Upton, a Representative in Congress from the State of Michigan, prepared statement	77

WITNESSES

Roberta Stempfley, Acting Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, Department of Homeland Security	15
Prepared statement [1]	
Sean P. McGurk, Director, National Cybersecurity and Communications Integration Center, Office of Cybersecurity and Communications, National Protection and Programs Directorate, Department of Homeland Security	16
Prepared statement	19
Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office	31
Prepared statement	33

[1] Ms. Stempfley issued a joint statement with Mr. McGurk for the record.

CYBERSECURITY: AN OVERVIEW OF RISKS TO CRITICAL INFRASTRUCTURE

TUESDAY, JULY 26, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 11:00 a.m., in room 2322 of the Rayburn House Office Building, Hon. Cliff Stearns (chairman of the subcommittee) presiding.

Members present: Representatives Stearns, Murphy, Burgess, Blackburn, Scalise, Griffith, DeGette, Schakowsky, Castor, Green, Christensen, and Waxman (ex officio).

Staff present: Carl Anderson, Counsel, Oversight and Investigations; Todd Harrison, Chief Counsel, Oversight and Investigations; Karen Christian, Counsel, Oversight and Investigations; Alan Slobodin, Deputy Chief Counsel, Oversight and Investigations; Peter Spencer, Professional Staff Member, Oversight and Investigations; Carly McWilliams, Legislative Clerk; Andrew Powaleny, Press Assistant; Sean Bonyun, Deputy Communications Director; Kristin Amerling, Democratic Chief Counsel and Oversight Staff Director; Tiffany Benjamin, Democratic Investigative Counsel; Karen Lightfoot; Democratic Communications Director and Senior Policy Advisor; and Ali Neubauer, Democratic Investigator.

Mr. STEARNS. Good morning, everybody. And the subcommittee will come to order. And I will start with my opening statement.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

I have called to order this subcommittee's first hearing on cybersecurity and critical infrastructure protection. Over the last 15 years, our Federal Government has wrestled with the question of how best to protect our Nation's critical infrastructures from cyber attacks. Since September 11, our infrastructure systems have become even more automated and more reliant on information systems and computer networks to operate. This has allowed our systems to become more efficient, but it has also opened the door to cyber threats and cyber attacks.

Recent reports and news articles have highlighted how threats and risks to cybersecurity have created vulnerabilities in our Nation's critical infrastructures and information systems. For example, just last week, the Department of Homeland Security sent out a bulletin about potential insider threats to utilities. That bulletin stated that outsiders have attempted to obtain information about

the utilities' infrastructure to use in coordinating and conducting a cyber attack.

In March 2011, the computer systems of RSA were breached. RSA manufactures tokens for secure access to computer networks. Sensitive information about these tokens was stolen and later used to hack into the network of Lockheed Martin, a Department of Defense contractor.

Last summer, the Stuxnet attack was identified. Stuxnet targets vulnerabilities in industrial control systems such as nuclear and energy to gain access to the systems and then manipulate the control process. This kind of attack has the potential to bring down or severely interrupt the functions of an electricity or even a nuclear plant.

The issues surrounding critical infrastructure protection and security are complex. Our systems are interconnected and depend on one other to operate. A vulnerability in one critical infrastructure naturally exposes other critical infrastructures to the same threats and risks, either because they are linked together through information systems or because one infrastructure depends on another to operate. In addition, much of the country's critical infrastructures are privately owned, as much as 80 or 90 percent. They therefore have different operations, components, control systems, and computer networks—as well as vastly different resources available to address problems like cybersecurity and infrastructure protection.

My colleagues, we must identify and protect the very systems that make our country run: energy, water, healthcare, manufacturing, and communications. Pursuant to the Homeland Security Act of 2002, DHS has led the coordination of infrastructure protection efforts with the private and public sectors and numerous federal agencies. One way DHS does this is to coordinate working groups and information sharing and analysis centers or ISACs in the individual critical infrastructure sectors and in cross-sector working groups.

DHS is primarily responsible for conducting threat analysis and issuing warnings about cyber threats so that other federal agencies and the owners and operators of critical infrastructure can simply protect their systems. DHS' efforts to protect our critical infrastructure have been the subject of some criticism.

Since 2003, the Government Accountability Office has designated "protecting the Federal Government's information systems and the Nation's cyber critical infrastructures" as a "high risk" area. In particular, in a report issued last July, GAO found that public- and private-sector owners and operators of critical infrastructure were not satisfied with the kind of cyber threat information they were getting from DHS. GAO has also expressed some concern that the sector-specific plans for dealing with cybersecurity need to be updated. In light of growing and more sophisticated cyber attacks, this is obviously a critical issue.

As I mentioned previously, this is the subcommittee's first hearing in this Congress on critical infrastructure protection and cybersecurity. The purpose of this hearing in particular is to get an overview of DHS' role and responsibilities and how it coordinates with the sector-specific federal departments and agencies, many of which are subject to this committee's jurisdiction. Once we have a

better understanding of DHS' role, it is my intention to call additional hearings to understand the issues that are presented in protecting the individual sectors, such as energy and information systems and communications.

Many ideas have been presented about how to improve critical infrastructure protection and cybersecurity. I believe the Oversight and Investigations Subcommittee has an important role to play in examining and bringing to light what is working now, and what can be done better.

I should note that this subcommittee's inquiry into this matter began with a bipartisan letter to the Department of Homeland Security asking for a briefing about its efforts to protect critical infrastructure. I appreciate the support of Ranking Member, Ms. DeGette, and the minority in this investigation. As Members of Congress, one of our foremost responsibilities is protecting our Nation's security and the safety of its citizens.

With that I yield opening statement to the ranking member, Ms. DeGette.

[The prepared statement of Mr. Stearns follows:]

Statement of the Honorable Cliff Stearns
Committee on Energy and Commerce
Chairman, Subcommittee on Oversight and Investigations hearing on Cybersecurity: An Overview of Threats to Critical Infrastructure
July 26, 2011

(843 words)

I call to order this Subcommittee's first hearing on cybersecurity and critical infrastructure protection.

Over the last 15 years, our federal government has wrestled with the question of how best to protect our nation's critical infrastructures from cyber attacks. Since September 11, our infrastructure systems have become even more automated and more reliant on information systems and computer networks to operate. This has allowed our systems to become more efficient, but it has also opened the door to cyber threats and cyber attacks.

Recent reports and news articles have highlighted how threats and risks to cybersecurity have created vulnerabilities in our nations critical infrastructures and information systems. For example:

- Just last week, the Department of Homeland Security sent out a bulletin about potential insider threats to utilities. That bulletin stated that outsiders have attempted to obtain information about the utility's infrastructure to use in coordinating and conducting a cyber attack.

- In March 2011, the computer systems of RSA were breached. RSA manufactures tokens for secure access to computer networks. Sensitive information about these tokens was stolen, and later used to hack into the network of Lockheed Martin, a Department of Defense contractor.

- Last summer, the Stuxnet attack was identified. Stuxnet targets vulnerabilities in industrial control systems, such as nuclear and energy, to gain access to the systems and manipulate the controls processes. This kind of attack has the potential to bring down or severely interrupt the functions of an electricity or nuclear plant.

The issues surrounding critical infrastructure protection and security are complex. Our systems are interconnected and depend on one other to operate. A vulnerability in one critical infrastructure naturally exposes other critical infrastructures to the same threats and risks, either because they are linked together through information systems or because one infrastructure depends on another to operate. In addition, much of the country's critical infrastructures are privately owned, as much as 80 or 90 percent. They therefore have different operations, components, control systems, and computer networks — as well as vastly different resources available to address problems like cybersecurity and infrastructure protection.

We must identify and protect the very systems that make our country run: energy, water, healthcare, manufacturing, and communications. Pursuant to the Homeland Security Act of 2002, DHS has lead the coordination of infrastructure protection efforts with the private and public sectors and numerous federal agencies. One way DHS does this is to coordinate working groups and information sharing and analysis centers or "ISACS" (I-sacks) in the individual critical infrastructure sectors and in cross-sector working groups. DHS is primarily responsible for conducting threat analysis and issuing warnings about cyber threats so that other federal agencies and the owners and operators of critical infrastructure can protect their systems.

DHS' efforts to protect our critical infrastructure have been the subject of some criticism. Since 2003, the Government Accountability Office has designated "protecting the Federal government's information systems and the nation's cyber critical infrastructures" as a "high risk" area. In particular, in a report issued last July, GAO found that public and private sector owners and operators of critical infrastructure were not satisfied with the kind of cyber threat information they were getting from DHS. GAO has also expressed some concern that the sector-specific plans for dealing with cybersecurity need to be updated. In light of growing and more sophisticated cyber attacks, this is obviously a critical issue.

Today, we will hear testimony from two witnesses from DHS: Ms. Bobbie Stempfley, Acting Assistant Secretary at DHS for the Office of Cybersecurity and Communications, and Mr. Sean McGurk, Director of the National Cybersecurity and Communications Integration Network at DHS. I look forward to their testimony, and getting a better understanding of the status of

DHS' work. I also welcome Mr. Gregory Wilshusen of the Government Accountability Office, which has done extensive work relating to DHS' cybersecurity efforts.

As I mentioned previously, this is the Subcommittee's first hearing in this Congress on critical infrastructure protection and cybersecurity. The purpose of this hearing, in particular, is to get an overview of DHS' roles and responsibilities, and how it coordinates with the sector-specific federal departments and agencies, many of which are subject to this Committee's jurisdiction. Once we have a better understanding of DHS' role, it is my intention to call additional hearings to understand the issues that are presented in protecting the individual sectors, such as energy and information systems and communications. Many ideas have been presented about how to improve critical infrastructure protection and cybersecurity. I believe the Oversight and Investigations Subcommittee, in particular, has an important role to play in examining and bringing to light what is working now, and what can be done better.

I should note that this Subcommittee's inquiry into this matter began with a bipartisan letter to the Department of Homeland Security, asking for a briefing about its efforts to protect critical infrastructure. I appreciate the support of Ranking Member DeGette and the Minority in this investigation. As Members of Congress, one of our foremost responsibilities is protecting our nation's security and the safety of its citizens.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. DEGETTE. Thank you very much, Mr. Chairman. And like you, this is a matter of great urgency. I am glad we are having this overview hearing and I am also happy to work with the majority on additional hearings in the particular issues of cybersecurity.

Just today, in the Washington Post it talked about a GAO report on significant breaches of classified computer networks in the Department of Defense. And while that is not in the jurisdiction of this committee, it just points out how vulnerable this country can be and why it is so important to keep our information systems safe.

The chairman referred to the cyber attack on RSA, which compromises the Department of Energy systems that necessitated shutting down internet connectivity for several days and breaches of Citibank data belonging to hundreds of thousands of customers. Anecdotally, at least, it seems like these breaches are becoming more and more frequent. The incidents remind us of the need for vigilance regarding efforts to prevent cybersecurity breaches and respond effectively when they occur and the importance of congressional oversight in these areas.

As the chairman mentioned, I asked him earlier this Congress to look into these issues, and I am really glad that we are going to have a rigorous review of all of the cybersecurity issues. As the chairman mentioned, we have jurisdiction over a number of key components of our Nation's critical infrastructure, including the electrical grid, drinking water system, chemical plants, healthcare system, and telecommunications activities. In the last Congress, we saw progress in this committee regarding addressing cybersecurity issues in a number of these areas. The committee developed and passed on a bipartisan basis legislation to promote security and resiliency in the electrical power grid by providing the Federal Energy Regulatory Commission new authorities and providing for Department of Energy assistance to industry to protect the grid against cyber threats and other vulnerabilities. The committee also developed and passed legislation regarding chemical and drinking water facilities to meet the risk-based cybersecurity performance standards.

Cybersecurity issues are complex and evolving and deserve continuing and focused attention. One major question is how to best ensure an effective public-private partnership to address cybersecurity threats. The majority of our Nation's critical infrastructure is owned or operated by the private sector. While there are incentives for private-sector entities to protect the security of their information networks, national security priorities may not always align with priorities and capabilities of the private sector.

I know that the Department of Homeland Security witnesses before us today are helping lead the administration's efforts to foster private- and public-sector cooperation in promoting cybersecurity and I look forward to hearing their insights on progress that is being made and obstacles that may still exist.

Another question we have to ask is how to best ensure that the Federal Government is drawing on its own expertise and experience to ensure cybersecurity measures are appropriately tailored to

address specific needs in different critical infrastructure sectors. I look forward to hearing from GAO about these challenges. But even with a maximally effective partnership of federal agencies, state and local governments, and the private sectors in our country on cybersecurity protection, we must still address issues raised by the fact that information networks do not have national boundaries. Many reports suggested that the cyber attacks have started outside of American borders, raising serious questions about how we ensure international cooperation to protect against threats that cross borders. And in this DOD example, in the GAO report today, apparently the cyber attack came from a portable computer, a laptop computer that was somehow tapped into.

And so I look forward to the insights of today's witnesses on these and other issues. I hope that we will build on this hearing with additional hearings on cybersecurity. It is one of the few bastions of bipartisanship left around here this week and I am happy to be part of it.

I yield back.

[The prepared statement of Ms. DeGette follows:]

Opening Statement of Rep. Diana DeGette
Ranking Member, Subcommittee on Oversight and Investigations
"Cybersecurity: An Overview of Risks to Critical Infrastructure"
Subcommittee on Oversight and Investigations
July 26, 2011

Today's hearing on cybersecurity for our nation's critical infrastructure is important and timely. We have recently seen a steady stream of publicly reported security breaches that underscore vulnerabilities in information systems key to our national economy and security. In just the past few months, we learned of a cyberattack on RSA, the company that provides technology used by government agencies and private sector companies to access secure information networks, compromises to Department of Energy systems that necessitated shutting down Internet connectivity for several days and breaches of Citibank data belonging to hundreds of thousands of customers. Anecdotally at least, it seems that these breaches are becoming more frequent.

These incidents remind us of the need for vigilance regarding efforts to prevent cybersecurity breaches and respond effectively when they occur, and the importance of congressional oversight in these areas. Earlier this Congress, I asked Chairman Stearns to look into these issues and I am pleased that we will have the opportunity today to hear an overview of federal cybersecurity issues from our witnesses. I hope this hearing marks the starting point for rigorous review of cybersecurity in this Subcommittee.

Our Committee has jurisdiction over a number of key components of the nation's critical infrastructure, including our electrical grid, drinking water system, chemical plants, health care system, and telecommunications activities. In the last Congress, we saw progress in this Committee regarding addressing cybersecurity issues in a number of these areas. The Committee developed and passed on a bipartisan basis legislation to promote security and resiliency in the electric power grid by providing the Federal Energy Regulatory Commission new authorities and providing for Department of Energy assistance to industry to protect the grid against cyber threats and other vulnerabilities.
The Committee also developed and passed legislation requiring chemical and drinking water facilities to meet risk-based cybersecurity performance standards.

Cybersecurity issues are complex and evolving, and deserve continuing and focused attention.

One major question is how to best ensure an effective public-private partnership to address cybersecurity threats. The majority of our nation's critical infrastructure is owned or operated by the private sector. While there are incentives for private sector entities to protect the security of their information networks, national security priorities may not always align with priorities and capabilities of the private sector. I know that the Department of Homeland Security witnesses before us today are helping lead the Administration's efforts to foster private and public sector cooperation in promoting cybersecurity. I look forward to their insights on progress that is being made and obstacles that may exist.

Another question is how to best ensure that the federal government is drawing on its own expertise and experience to ensure cybersecurity measures are appropriately tailored to address specific needs in the different critical infrastructure sectors. I look forward to hearing more from GAO about these challenges.

But even with a maximally effective partnership among federal agencies, state and local governments, and the private sector in our country on cybersecurity protection, we must still address issues raised by the fact that information networks do not have national boundaries. Many recent reports suggest that cyber-attacks have started outside of American borders, raising serious questions about how we ensure international cooperation to protect against threats that cross borders.

I look forward to the insights of today's witnesses on these and other issues, and hope the Subcommittee builds on this hearing with additional hearings on cybersecurity issues under our jurisdiction.

Mr. STEARNS. I thank the gentlelady and recognize the gentleman from Texas, Dr. Burgess, for 2 minutes.

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. I thank the chair.

To say that this committee has been working diligently for years is kind of an oxymoron but it does seem through several terms on this subcommittee we have indeed delved into this issue. I am anxious that we bring this to a legislative conclusion and institute those things that will provide the protection that I think we all feel that we need. There are critical urgent things that need to be done to protect our transmission grid, our power plants from attacks from those who wish to do us harm. The threats are real. It is time to move the legislation forward.

We do have to be careful that we don't unduly shift the balance of responsibility that has been properly maintained between the government and the private sector for decades. It is important that we be careful; it is important that we be prudent in providing the Federal Government any additional authority. If indeed any is necessary, it must be done in a way that cannot be abused and will not result in significantly higher cost to consumers and businesses at a time when the economy is so fragile. And it must not result in the loss of any personal freedoms that people now have.

The testimony we will hear today will help this committee in perfecting legislation that was considered last year. I certainly look forward to working with members on both sides of the dais to ensure that the legislation is mindful of both the real threats that we face and the burdens that granting new powers to the Federal Government can create. Ensuring this balance can and should be done.

Thank you, Mr. Chairman, for the recognition. I will yield back my time.

Mr. STEARNS. The gentleman yields back and the gentlelady from Tennessee, Ms. Blackburn, is recognized for 2 minutes.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. Thank you, Mr. Chairman. And I want to welcome our witnesses. We appreciate that you would take the time and come over here to the Hill. We all do know and do agree that cybersecurity is an important issue and we know that there are those who are, as we speak, waging war if you will on our vital infrastructure.

Last month, Wall Street Journal reported that the IMF was investigating a recent cyber attack. Not surprisingly, this attack came just 1 month after a group called Anonymous indicated its hackers would target the IMF Web site in response to the strict austerity measures in its financial package of Greece.

Closer to home, in my State of Tennessee, presides our Nation's largest public power utility, the Tennessee Valley Authority. TVA's power networks stretch across 80,000 square miles in the Southeastern U.S. and provide electricity to more than 8.7 million Americans. Under Homeland Security Presidential Directive number 7,

TVA is considered a National Critical Infrastructure and must take great steps to protect and to safeguard its essential cyber assets. A power grid disruption or other threat on TVA operations or any other public utility in our country would cause a cascading effect impacting our economy, safety, and daily lives.

In fact, this concern was reaffirmed last month as former CIA director and current Secretary of Defense Panetta appeared before the Senate Armed Services Committee and declared that the next Pearl Harbor our Nation confronts could very well be a cyber attack that cripples our power systems, the grid, our security systems, our financial systems, and our governmental systems.

With all that in mind, I thank the chairman for the hearing. I thank you all for your participation as we discuss what steps DHS is taking to avoid what would be the unimaginable, a Pearl Harbor attack on our Nation's vital infrastructure.

And I yield back.

[The prepared statement of Mrs. Blackburn follows:]

Opening Statement
The Honorable Marsha Blackburn
Oversight and Investigations
Cybersecurity: An Overview of Risks to Critical Infrastructure
July 26, 2011

Cybersecurity is a serious threat to our nation's vital infrastructure and is a war that is being waged at an escalating pace.

Just last month the Wall Street Journal reported that the International Monetary Fund was investigating a recent cyber attack. Not surprisingly, this attack came just one month after a group called "Anonymous" indicated its hackers would target the IMF web site in response to the strict austerity measures in its financial package for Greece.

Closer to home, in my state of Tennessee resides our nation's largest public power utility, the Tennessee Valley Authority. TVA's power networks stretch across 80,000 square miles in the southeastern United States, and provides electricity to more than 8.7 million Americans. Under Homeland Security Presidential Directive-7, TVA is considered a "National Critical Infrastructure" and must take great steps to protect and safeguard its essential cyber assets.

A power-grid disruption or other threat on TVA operations or any other public utility in our country could cause a cascading effect impacting our economy, our safety, and our daily lives.

In fact, this concern was reaffirmed last month as former CIA Director and current Secretary of Defense, Leon Panetta, appeared before the Senate Armed Services Committee and declared that the next Pearl Harbor our nation confronts could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, and our governmental systems.

With that in mind I thank the Chairman for calling for this hearing today so that we can discuss what steps DHS is taking to avoid the imaginable- a Pearl Harbor attack on nation's vital infrastructure.

I yield back.

Mr. STEARNS. The gentlelady yields back and I recognize Ms. Christensen from the Virgin Islands for 5 minutes.

OPENING STATEMENT OF HON. DONNA CHRISTENSEN, A REPRESENTATIVE IN CONGRESS FROM THE VIRGIN ISLANDS

Mrs. CHRISTENSEN. Thank you, Chairman Stearns, and thank you, Ranking Member DeGette, for holding this hearing to discuss cybersecurity risks, threats, and challenges to our Nation's critical infrastructure. Many of today's battles are in cyberspace where terrorism and hackers help attack our cell phones, computer grids, and have the potential to destroy sensitive information in 18 of our Nation's most critical sectors.

Since 9/11, we have known to expect that we would experience terrorist attacks that would be cyber attacks. As a former member of the Homeland Security Committee, I have taken part in many hearings and worked on legislation addressing this issue. As our witnesses who we welcome here today will testify, a lot has been done to create entities to coordinate and oversee efforts to address and prevent cybersecurity threats. But there are still challenges to protecting our Nation's infrastructure from these threats and we must continue to examine how we can overcome these challenges.

In doing so, it is important that we pass legislation to protect our Nation's electric grid. All of these long-term initiatives require a national electric grid that is reliable and secure. The electrical grid serves more than 143 million American customers, has to operate without interruption, and is a key foundation of our national security. Designing and operating an electrical system that prevents cybersecurity events from having a catastrophic impact is a challenge we must all address. And I want to add that the healthcare sector is not immune to these attacks either.

So I would like to thank DHS and GAO and commend both Agencies for their efforts to address imminent cybersecurity threats. And with that, I will yield back the balance of my time.

Mr. STEARNS. The gentlelady yields back.

And at this time, we will move to our first panel, our witnesses. Let me address you folks.

You are aware that the committee is holding an investigative hearing and when doing so has had the practice of taking testimony under oath. Do you have any objections to taking testimony under oath? All right. No.

The chair then advises you that under the rules of the House and the rules of the committee you are entitled to be advised by counsel. Do you desire to be advised by counsel during your testimony today? All right.

In that case, if you will please rise and raise your right hand, I will swear you in.

[Witnesses sworn.]

Mr. STEARNS. You are now under oath and subject to the penalties set forth in Title XVIII, Section 1001, of the United States Code.

We welcome the three of you for your 5-minute summary statement. And we have Ms. Bobbie Stempfley, Acting Secretary of the DHS Office of Cybersecurity and Communications, welcome; and Mr. Sean P. McGurk, Director, National Cybersecurity and Com-

munications Integration Center in the Office of Cybersecurity and Communications at DHS; and lastly, Mr. Gregory Wilshusen, Government Accountability Office Director of Information Security Issues. Thank you.

And Ms. Stempfley, we welcome your opening statement. Just turn the mike on if you don't mind. Just move it close to you so we can hear you. That would be super. Thanks.

STATEMENTS OF ROBERTA STEMPFLEY, ACTING ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY; SEAN P. MCGURK, DIRECTOR, NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY; AND GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

STATEMENT OF ROBERTA STEMPFLEY

Ms. STEMPFLEY. OK. Thank you very much. So thank you very much, Chairman Stearns, Ranking Member DeGette, and other members of the subcommittee.

As you heard, my name is Bobbie Stempfley, and I am the Acting Assistant Secretary in the Office of Cybersecurity and Communications at the Department of Homeland Security, and it is definitely my privilege to be here to speak to you today with my colleagues from across government to talk about cybersecurity, which is an area of great passion for all of us.

The opening comments did such a wonderful job describing the threat landscape that we operate in today. It certainly is one we have increasing sophistication, increasing severity, and an environment where no one is immune from individuals to private-sector companies, and one where we see it slightly untenable where the threat actors have to make one right choice in an environment where only a single wrong implementation in the networks that are being defended enables access. And so it is an environment where we spend a great deal of time bringing together private-sector partners and others.

We have identified 38,000 vulnerabilities over a period of time in critical infrastructures and provide warning notification and awareness products around those vulnerabilities to private-sector individuals. It is an environment, as the chairman pointed out, of significant interdependence, both between critical infrastructure sectors, between corporations, between environments. Several examples that you provided do a wonderful job illuminating that interdependence across the board. And that means that it requires an interdependent and integrative approach in order to provide protective, preventative, and restoral and defensive measures both across government and within the private sector.

It is the job of the National Protection and Programs Directorate; it is our mission responsibility to secure the federal executive civilian branch—that is the federal departments and agencies—to pro-

vide technical support to private-sector individuals, owners, and operators to help them with risk assessment, with mitigation, with restoral and response activities. It is also our mission to provide general awareness to the broad public. And finally, as Mr. McGurk will discuss, to provide national coordination and response across the board.

It is, as I said, not an environment where a single solution works or a single organization provides all of the answers. It is an environment where much progress has been made and it is a team sport for us all. Cooperation between law enforcement, between intelligence agencies, between the Homeland Security, between, as I said, government and private sector is a significant part of how we need to move forward of the successes we have had to date.

Examples such as you pointed out, the compromise in RSA really helps demonstrate the progress that has been made in government. The response that we had in that worked across a set of responsibilities defined in the National Cybersecurity Instant Response Plan where law enforcement has responsibility for pursuit and for investigation, where intelligence has warning responsibilities and attribution responsibilities, and where Homeland Security's responsibilities are in protection, prevention, restoral, and response. And that partnership across government is so important for us as we work through each of the events that occur.

We have in a proactive manner responded to 100 requests from critical infrastructure partnerships, largely across water, oil, and gas and power to help identify vulnerabilities in their environment and help them improve the capabilities that they have for protection and for response. It is through that partnership that we continue to work to enhance our prevention activities because, as we said, we are in that untenable environment today.

What we have also put a great deal of effort in is to increase visibility and information sharing across environments. Again, I look forward to the comments of Mr. McGurk in our operations center. But it is information sharing not only in operations and in response, but information sharing at large that is important across the board.

And so in conclusion, I look forward to further questions from the committee to discuss what we have done. And it, again, is my pleasure to be here today.

[The joint prepared statement of Ms. Stempfley and Mr. McGurk appears after Mr. McGurk's testimony.]

Mr. STEARNS. Thank you.

Mr. McGurk, you are welcome for your opening statement.

STATEMENT OF SEAN P. MCGURK

Mr. MCGURK. Thank you, Chairman Stearns, Ranking Member DeGette, and distinguished members of the subcommittee. My name is Sean McGurk. I am the director of the National Cybersecurity and Communications Integration Center, also known as the NCCIC. Thank you for inviting me here today along with my distinguished colleagues to discuss the overall cyber-risk to critical infrastructure. The Department greatly appreciates the committee's support for our central mission and looks forward to working with the committee to establish the necessary plans and pro-

grams moving forward to address risks to the critical infrastructure.

The cyber environment is not homogenous under a single department or agency nor under the private sector. Each of the 18 critical infrastructure and key resource sectors are completely different—energy, water, nuclear, transportation, they all have their unique challenges and their unique environments. In fact, within a particular company, two plants may not have the same operating environment. We rely on this continuous availability of a vast, interconnected, critical infrastructure to sustain our way of life. A successful cyber attack could potentially result in physical damage and even loss of life. We face a significant challenge moving forward—strong and rapidly expanding adversary capabilities and a lack of comprehensive threat and vulnerability awareness.

Support of these efforts from our private-sector partners is key to securing these critical infrastructures. The government does not have all the answers, so we must work with the private sector to establish those guidelines. There is no one-size-fits-all solution in a cyber environment. There is no cyber Maginot Line. We must leverage our expertise and our access to information, along with industry-specific needs, capabilities and timelines. Each partner has a role and a unique capability, as demonstrated by the diversity of this panel.

Two-factor authentication was mentioned earlier, the RSA example. In that particular example, within a 24-hour period, the Department, working along with law enforcement and with the intelligence community, responded to a request from the private industry partner to provide a mitigation, identification, and assessment team in support of their mitigation efforts. The Department continuously works with our private-sector partners and the financial-services sector, energy sector, communications, IT, and others to prepare, prevent, respond, recover, and restore.

Coordinating the national response of domestic cyber emergencies is the focus of the National Cyber Incident Response Plan and indeed the NCCIC. The what and the how on the cyber attack is the focus and the intent of our mitigation activities. The who and the why usually come later.

The NCCIC works closely with the government at all levels and private sector to coordinate and integrate a unified cyber response. Sponsoring security clearances for our partners enable them to participate fully in our watch-center environment. To date, we have physical representation from the communications sector and its Information Sharing and Analysis Center and also with companies such as AT&T, Verizon, and Sprint. The information technology sector is represented physically on the watch floor along with the financial-services sector, NERC, representing the North American Energy Reliability Corporation; representing the energy sector, Information Sharing and Analysis Center; and most recently, we have begun to coordination and share information with the National Electric Sector Cybersecurity Organization, or NESCO.

We have virtual connections as well as physical connections with these organizations and we share data in near-real time. Additionally, we have a physical representative from the Multi-State ISAC, enabling us to provide actionable intelligence to state, local, tribal,

and territorial governments and their representatives. Each of these partners bring a unique perspective and a unique capability to the watch environment.

Currently, within our legal authorities, we continue to engage, collaborate with our partners and provide analysis, 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 and to respond, recover, and restore to cyber impacts.

Finally, we work closely with the private sector and our interagency partners and law enforcement and intelligence to provide the full complement of capabilities from the federal standpoint in preparation for and response to significant cyber incidents.

Chairman Stearns, Ranking Member DeGette, and distinguished members of the subcommittee, let me conclude by reiterating that I look forward to exploring opportunities to advance the mission and collaboration with the subcommittee and my colleagues in the public and private sector. Thank you again for this opportunity to testify and would be happy to answer your questions.

[The joint prepared statement of Ms. Stempfley and Mr. McGurk follows:]

Statement for the Record
of

Roberta Stempfley
Acting Assistant Secretary
Office of Cyber Security and Communications
National Protection and Programs Directorate
Department of Homeland Security

and

Sean P. McGurk
Director, National Cybersecurity and Communications Integration Center
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
Washington, DC

July 26, 2011

Introduction
Chairman Stearns, Ranking Member DeGette and distinguished Members of the Subcommittee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission. Specifically, I will discuss the Department's cybersecurity mission as it relates to critical infrastructure and our coordination of this mission with the private sector.

I would like to express the Department's desire to work more with you to convey the relevance of cybersecurity to average Americans. Increasingly, the services we rely on in our 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 faces 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 and the sharing of information. As bad as the loss of precious national intellectual capital is, we increasingly face threats that are even greater. We face threats that could significantly compromise the accessibility and reliability of our information infrastructure.

Malicious actors in cyberspace, including nation states, terrorist networks, organized criminal groups, and individuals located here in the United States, 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, 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.

Malicious cyber activity can instantaneously result in virtual or physical consequences that threaten national and economic security, critical infrastructure, public health and welfare. 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 across the public and private sectors.

We need to support the efforts of our private sector partners to secure themselves against malicious activity in cyberspace. Collaboratively, public and private sector partners must use our knowledge of information technology systems and their interdependencies to prepare to respond should 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.

Cybersecurity Mission

No single technology—or single government entity—alone can overcome the cybersecurity challenges our nation faces. Consequently, the public and private sectors must work collaboratively. Cybersecurity must start with informed users taking necessary precautions and extend through a coordinated effort among the private sector, including critical infrastructure owners and operators, and the extensive expertise that lies across coordinated government entities. In addition to leading the effort to secure Federal Executive Branch civilian departments and agencies' unclassified networks, the National Protection and Programs Directorate (NPPD) within DHS is responsible for the following key cybersecurity missions:

- Providing technical expertise to the private sector and critical infrastructure and key resources (CIKR) owners and operators—whether private sector, state or municipality-owned—to bolster their cybersecurity preparedness, risk assessment, mitigation and incident response capabilities;
- Raising cybersecurity awareness among the general public; and
- Coordinating the national response to domestic cyber emergencies.

In a reflection of the bipartisan nature with which the federal government continues to approach cybersecurity, President Obama determined that the Comprehensive National Cybersecurity Initiative (CNCI) and its associated activities should continue to evolve as 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 NPPD. The Office of Cybersecurity and Communications (CS&C), a component of NPPD, focuses on reducing risk to the 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. It also houses the National Cybersecurity and Communications Integration Center (NCCIC)—DHS' 24-hour cyber and communications watch and warning center. Within NCSD, the United States Computer Emergency Readiness Team (US-CERT) is working more closely than ever with our public and private sector partners to share what we learn from EINSTEIN 2, a federal executive agency computer network intrusion detection system, to deepen our collective understanding, identify threats collaboratively, and develop effective security responses. EINSTEIN enables us to respond to warnings and other indicators of operational cyber attacks, and we have many examples showing that this program investment has paid for itself several times over.

Teamwork—ranging from intra-agency to international collaboration—is essential to securing cyberspace. Together, we can leverage resources, personnel, and skill sets that are needed to achieve a more secure and reliable cyberspace. Although DHS leads significant cybersecurity mission activities in the public sector, I will focus the rest of my testimony on private sector coordination.

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, are collocated in 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. Currently, representatives from the Information Technology and Communications Sectors and the Multi-State Information Sharing and Analysis Center are located on the NCCIC watch floor. We are also finalizing steps to add representatives from the Banking and Finance Sector, as well as the Energy Sector .

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 reported 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.

NCSD collaborates with private sector stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of private sector critical infrastructures. NCSD also provides cyber threat and vulnerability analysis, early warning, incident response assistance, and exercise opportunities for 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 (NCIRP). The NCIRP 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 NCIRP 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 NCCIC and the federal government's full suite of cybersecurity response capabilities.

Providing Technical Operational Expertise to the Private Sector

DHS has significant cybersecurity capabilities, and we are using those capabilities to great effect as we work collaboratively with the private sector to protect the nation's CIKR. We engage with

the private sector on a voluntary basis to provide onsite analysis, mitigation support, and assessment assistance. Over the past year, we have repeatedly demonstrated our ability to materially and expeditiously assist companies with cyber intrusion mitigation and incident response. We are able to do so through our trusted and close relationships with private sector companies as well as federal departments and agencies. Finally, our success in assisting the private sector is due in no small part to our dedication to properly and fully addressing privacy, civil rights and civil liberties in all that we do. Initiating technical assistance with a private company to provide analysis and mitigation advice is a sensitive endeavor—one that requires trust and strict confidentiality. Within our analysis and warning mission space, DHS has a proven ability to provide that level of trust and confidence in the engagement. Our efforts are unique among federal agencies' capabilities in that DHS focuses on civilian computer network defense and protection rather than law enforcement, military, or intelligence functions. DHS engages to mitigate the threat to the network to reduce future risks.

Our approach requires vigilance and a voluntary public/private partnership. We are continuing to build our capabilities and relationships because the cyber threat trends are more sophisticated and frequent.

Over the past year, we established the NCCIC and are adding staff to that center, both from existing DHS personnel and from partner organizations in the public and private sectors. More broadly, we are continuing to hire more cybersecurity professionals and increasing training availability to our employees. The NCIRP is operational, and we continue to update and improve it with input from senior cybersecurity leaders. We will be releasing the NCIRP publicly in the near future. We are executing within our current mission and authorities now, receiving and responding to substantial netflow data from our intrusion detection technologies deployed to our federal partners, and leveraging that data to provide early warnings and indicators across government and industry. With our people, processes and technology, we stand ready to execute the responsibilities of the future.

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, and the private sector. 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 sectors depend on the Energy Sector, and failure in one of these sectors could subsequently affect government and private sector operations.

US-CERT also collaborates, provides remote and onsite response support, and shares information with federal, state and local governments; critical infrastructure owners and operators; and international partners to address cyber threats and develop effective security responses.

DHS provides onsite and remote incident response assistance to its public and private sector partners. Upon notification of a cyber incident, ICS-CERT and/or US-CERT can perform a preliminary diagnosis to determine the extent of the compromise. At the partner's request and when appropriate, either ICS-CERT or US-CERT can deploy a team to meet with the affected organization to review network topology, identify infected systems, create image files of hard drives for analysis, and collect other data as needed to perform thorough follow-on analysis. Both ICS-CERT and US-CERT can provide mitigation strategies, advise asset owners and operators on their efforts to restore service, and provide recommendations for improving overall network and control systems security.

An incident in early 2010 illustrates the incident response support that DHS provides. In this case, an employee of a company had attended an industry event and used an instructor's flash drive to download presentation materials to the company's laptop. The flash drive was infected with the Mariposa botnet, unbeknownst to the event organizer. When the employee returned to the work location and used the laptop, the virus quickly spread to nearly 100 systems. US-CERT and ICS-CERT had already been tracking a trend of removable media involved in malware infections, and, on request, deployed a team to the company's location to help diagnose the malware and identify those infected systems.

The team spent two days with the company reviewing the incident details, network topology, and the company's control systems architecture to identify systems of interest. The company was ultimately able to leverage all of the information to contain the infection and remove the malware from the infected systems. ICS-CERT and US-CERT provided follow-on reporting, mitigation measures, and access to additional resources through the US-CERT secure portal.

US-CERT'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, 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 many related initiatives and 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.

An additional 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 sophisticated malware of this type potentially 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, our goal is to balance the need for public information sharing while protecting the information that malicious actors may exploit. DHS provided the alerts in accordance with its responsible disclosure processes.

The purpose and function for responsible disclosure is to ensure that DHS executes its mission of mitigating risk to critical infrastructure, not necessarily to be the first to publish on a given threat. For example, ICS-CERT's purpose in conducting the Stuxnet analysis was to ensure that DHS understood the extent of the risks so that they could be mitigated. After conducting in-depth malware analysis and developing mitigation steps, we were able to release actionable information that benefited our private sector partners.

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.

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 solidified the priority the Administration places on improving cybersecurity.

No single agency has sole responsibility for securing cyberspace, and the success of our cybersecurity mission relies on effective communication and critical partnerships. Many government players have complementary roles as well as unique capabilities —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.

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. DHS, through the National Infrastructure Protection Plan partnership framework, has many years of experience in private sector collaboration, leveraging our relationships in both the physical and cybersecurity protection areas. For example, the Office of Infrastructure Protection and the National Cyber Security Division partnered with the chemical industry to publish the *Roadmap to Secure Industrial Control Systems in the Chemical Sector* in 2009, available at www.us-cert.gov. To meet the first set of milestones set forth in this 10-year plan, industry, in partnership with DHS, developed a suite of control systems security awareness materials that will be shared widely within the Chemical Sector this summer.

DHS engages with the private sector on a voluntary basis in accordance with our responsibilities under the Homeland Security Act. We stand by to assist our private sector partners upon their request, and thus far have been able to do so successfully due to our technical capabilities, existing private sector relationships, and expertise in matters relating to privacy and civil rights and civil liberties.

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. Based on lessons learned from the pilot, DHS is developing comprehensive information-sharing and incident response coordination processes with CIKR sectors, leveraging capabilities from within DHS and across the response community, through the NCCIC.

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 major urban area 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 the 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 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. The final strategy is set to be released in the near future, fulfilling 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 rights 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.

In September 2010, Secretary Napolitano and Secretary Gates co-signed a Memorandum of Agreement between DHS and DoD regarding cybersecurity. The MOA established a Joint Coordination Element (JCE) led by a DHS senior official at DoD's National Security Agency. The intent of the MOA was to enable DHS and DoD to leverage each other's capabilities, and more readily share cybersecurity information on significant cyber incidents. The JCE has been in place and building to fully operational capability since October 2010.

In December 2010, the DHS Science and Technology Directorate 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 test beds for specific use cases that strengthen the resiliency, security, integrity, and usability of financial services and other critical infrastructures.

Collaborative Risk Management Forums

The increased pace of collaborative cybersecurity operations between DHS and the private sector is due, in part, to standing public-private forums that support ongoing process improvements across the partnership. A few of these forums -- the Cross-Sector Cyber Security Working Group, the IT CIKR Sector, and the Industrial Control Systems Joint Working Group -- meet under the auspices of the Critical Infrastructure Partnership Advisory Council and conduct their activities consistent with the National Infrastructure Protection Plan (NIPP) partnership framework.

The Cross-Sector Cyber Security Working Group was established to address cross-sector cyber risk and explore interdependencies between and among various sectors. The working group serves as a forum to bring government and the private sector together to address common cybersecurity elements across the 18 CIKR sectors. They share information and provide input to key policy and planning documents including the NCIRP, the President's *Cyberspace Policy Review*, and the *National Strategy for Trusted Identities in Cyberspace*.

The IT CIKR Sector security partnership is comprised of DHS as the IT Sector Specific Agency, public sector partners in the IT Government Coordination Council, and private sector partners in the IT Sector Coordinating Council. This partnership forms to execute the IT Sector's risk

management framework: to identify and prioritize risks to IT Sector critical functions, to develop and implement corresponding risk management strategies, and to report on progress of risk management activities and adjustments to the IT Sector's risk profile. IT Sector public-private partners worked collaboratively to produce the 2009 IT Sector Baseline Risk Assessment (ITSRA), prioritizing risks to the sector's critical functions, and have subsequently been working to finalize corresponding risk management strategies outlining a portfolio of sector risk management activities to reduce the evaluated risks from the ITSRA across the functions. Progress reporting on implementation of these risk management strategies will be provided in the IT Sector Annual Report (as required by the NIPP).

In partnership with the Department of Energy, which is the Sector Specific Agency responsible for the Energy Sector under the NIPP, the Industrial Control Systems Joint Working Group provides a vehicle for stakeholders to communicate and partner across all critical infrastructure sectors to better secure industrial control systems and manage risk. The Industrial Control Systems Joint Working Group is a representative group comprising owners and operators, international stakeholders, government, academia, system integrators, and the vendor community. The purpose of the ICSJWG is to facilitate the collaboration of control systems stakeholders to accelerate the design, development, deployment and secure operations of industrial control systems. Based on public and private sector partner input, CSSP uses the Industrial Control Systems Joint Working Group to inform its mission activities and deliver needed products and services.

As you are aware, cybersecurity training is essential to increasing awareness of threats and the ability to combat them. To that end, CSSP conducts multi-tiered training through web-based and instructor-led classes across the country. In addition, a week-long training course is conducted at CSSP's state-of-the-art advanced training facility at the Idaho National Laboratory to provide hands-on instruction and demonstration. This training course includes a red team/blue team exercise in which the blue team attempts to defend a functional mockup control system while the red team attempts to penetrate the network and disrupt operations. The positive response to this week-long course has been overwhelming, and the classes are filled within a few days of announcement. To date, more than 16,000 public and private sector professionals have participated in some form of CSSP training through classroom venues and web-based instruction.

CSSP also provides leadership and guidance on efforts related to the development of cybersecurity standards for industrial control systems. CSSP uses these industry standards in a variety of products and tools to achieve its mission.

First, CSSP uses and promotes the requirements of multiple federal, commercial and international standards in its Cyber Security Evaluation Tool (CSET), which has been requested by and distributed to hundreds of asset owners across each of the 18 CIKR sectors. Tool users are evaluated against these standards based on answers to a series of standard-specific questions. CSET is also used by CSSP assessment teams to train and bolster an asset owner's control system and cybersecurity posture in onsite assessments. In fiscal year 2010, the program conducted more than 50 onsite assessments in 15 different states and two U.S. territories, including several remote locations where the control systems represent potential single points of

failure for the community. The program is planning for 75 onsite assessments in fiscal year 2011.

Second, CSSP developed the *Catalog of Control Systems Security: Recommendations for Standards Developers*, which brings together pertinent elements from the most comprehensive and current standards related to control systems. This tool is designed as a superset of control systems cybersecurity requirements and is available in the CSET and on the website for standards developers and asset owners.

Lastly, the CSSP provides resources, including time and expertise, to standards development organizations including NIST, the International Society of Automation, and the American Public Transportation Association. Experts provide content, participate in topic discussions, and review text being considered by the standards body.

The General Public

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, 7 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.*, 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 program is part of the NIST National Initiative for Cyber Education.

DHS is committed to safeguarding 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 dangerous 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 broad collaboration. DHS 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. Cybersecurity is critical to ensure that government, business and the public can continue to use the information technology and communications infrastructure on which they depend.

DHS continues to engage, collaborate and provide analysis, vulnerability, and mitigation assistance to its private sector CIKR partners. Our continued dedication to privacy and civil rights and civil liberties ensures a positive, sustainable model for cybersecurity engagement in the future. Finally, we work closely with our interagency partners in law enforcement, military, and intelligence, providing the full complement of federal capabilities in preparation for, and in response to, significant cyber incidents.

Chairman Stearns, Ranking Member DeGette, and distinguished Members of the Subcommittee, 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 sectors. Thank you again for this opportunity to testify. I would be happy to answer your questions.

Mr. STEARNS. Thank you. Mr. Wilshusen?

STATEMENT OF GREGORY C. WILSHUSEN

Mr. WILSHUSEN. Chairman Stearns, Ranking Member DeGette, and members of the subcommittee, thank you for the opportunity to testify in today's hearing on the cybersecurity risks to the Nation's critical infrastructure. But before I begin, if I may, Mr. Chairman, I would like to recognize Mike Gilmore, Tammy Carvette, and Lee McCracken, who is sitting behind me, and also Brad Becker from our Denver office, who are responsible for the significant contributions in reviewing this area and helping me prepare this testimony today.

Mr. STEARNS. I am glad you did. Thank you.

Mr. WILSHUSEN. Critical infrastructures are systems and assets, whether physical or virtual, so vital to our Nation that their incapacity or destruction would have a debilitating effect on our national security, economic wellbeing and public health and safety. They include, among other things, banking and financial institutions, telecommunications networks, and energy production transmission facilities, most of which are owned by the private sector. These infrastructures have become increasingly interconnected and dependent on interconnected networks and systems. And while the benefits of this interconnectivity have been enormous, they can also pose significant risk to the networks and systems, and more importantly, to the critical operations and services they support.

In my testimony today, I will describe the cyber threats confronting critical infrastructures, recent actions by the Federal Government to identify and protect these infrastructures and ongoing challenges to protecting them.

Mr. Chairman, our Nation's critical infrastructures face a proliferation of cyber threats. These threats can be intentional or unintentional. Unintentional threats can be caused by equipment failures, software upgrades, or maintenance procedures that inadvertently disrupt the systems. Intentional threats include both targeted and non-targeted attacks from a variety of sources, including criminal groups, hackers, insiders, and foreign nations engaged in intelligence gathering and espionage.

First, recent reports of cyber attacks incidents involving cyber-reliant critical infrastructure underscore the risks and illustrate that they can be used to disrupt industrial control systems and operations, commit fraud, steal intellectual property and personally identifiable information, and gather intelligence for future attacks. Over the past 2 years, the Federal Government has taken a number of steps aimed at addressing cyber threats and better protecting critical infrastructures.

For example, a cyberspace policy review identified 24 recommendations to address the organizational and policy changes needed to approve the current U.S. approach to cybersecurity. DHS updated the National Infrastructure Protection Plan in part to provide a greater focus on cyber issues and issued an interim version of the National Cyber Incident Response Plan. It also conducted Cyber Storm III, a cyber attack simulation exercise intended to test elements of the National Response Plan.

In addition, DHS, as you know, created the National Cybersecurity and Communications Integration Center, or NCCIC, to coordinate national response efforts, as well as work directly with other private- and public-sector partners.

Despite these threats, more needs to be done to address a number of remaining challenges. For example, implementing the recommendations made by the President's Cybersecurity Policy Review, updating the national strategy for securing the information and communications infrastructure, strengthening the public-private partnerships for securing cyber-reliant critical infrastructures, enhancing cyber analysis and warning capabilities, and securing the modernized electricity grid.

In summary, the threats to information systems are evolving and growing and systems supporting our Nation's critical infrastructures are not yet sufficiently protected to consistently thwart the threats. While actions have been taken, federal agencies and partnership with the private sector need to act to improve our Nation's cybersecurity posture, including enhancing cyber analysis and warning capabilities and strengthening the public-private partnerships. Until these actions are taken, our Nation's critical infrastructure will remain vulnerable.

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

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 11:00 a.m. EDT
July, 26, 2011

CYBERSECURITY

Continued Attention Needed to Protect Our Nation's Critical Infrastructure

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

U.S. Government Accountability Office
GAO 90 YEARS 1921-2011
ACCOUNTABILITY * INTEGRITY * RELIABILITY

GAO-11-865T

July 26, 2011

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-11-865T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

CYBERSECURITY

Continued Attention Needed to Protect Our Nation's Critical Infrastructure

Why GAO Did This Study

Increasing computer interconnectivity, such as the growth of the Internet, has revolutionized the way our government, our nation, and much of the world communicate and conduct business. However, this widespread interconnectivity poses significant risks to the government's and the nation's computer systems, and to the critical infrastructures they support. These critical infrastructures include systems and assets—both physical and virtual—that are essential to the nation's security, economic prosperity, and public health, such as financial institutions, telecommunications networks, and energy production and transmission facilities. Because most of these infrastructures are owned by the private sector, establishing effective public-private partnerships is essential to securing them from pervasive cyber-based threats. Federal law and policy call for federal entities, such as the Department of Homeland Security (DHS), to work with private-sector partners to enhance the physical and cyber security of these critical infrastructures.

GAO is providing a statement describing (1) cyber threats facing cyber-reliant critical infrastructures; (2) recent actions the federal government has taken, in partnership with the private sector, to identify and protect cyber-reliant critical infrastructures; and (3) ongoing challenges to protecting these infrastructures. In preparing this statement, GAO relied on its previously published work in the area.

View GAO-11-865T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The threats to systems supporting critical infrastructures are evolving and growing. In a February 2011 testimony, the Director of National Intelligence noted that there has been a dramatic increase in cyber activity targeting U.S. computers and systems in the last year, including a more than tripling of the volume of malicious software since 2009. Varying types of threats from numerous sources can adversely affect computers, software, networks, organizations, entire industries, or the Internet itself. These include both unintentional and intentional threats, and may come in the form of targeted or untargeted attacks from criminal groups, hackers, disgruntled employees, hostile nations, or terrorists. The interconnectivity between information systems, the Internet, and other infrastructures can amplify the impact of these threats, potentially affecting the operations of critical infrastructure, the security of sensitive information, and the flow of commerce. Recent reported incidents include hackers accessing the personal information of hundreds of thousands of customers of a major U.S. bank and a sophisticated computer attack targeting control systems used to operate industrial processes in the energy, nuclear, and other critical sectors.

Over the past 2 years, the federal government, in partnership with the private sector, has taken a number of steps to address threats to cyber critical infrastructure. In early 2009, the White House conducted a review of the nation's cyberspace policy that addressed the missions and activities associated with the nation's information and communications infrastructure. The results of the review led, among other things, to the appointment of a national Cybersecurity Coordinator with responsibility for coordinating the nation's cybersecurity policies and activities. Also in 2009, DHS updated its National Infrastructure Protection Plan, which provides a framework for addressing threats to critical infrastructures and relies on a public-private partnership model for carrying out these efforts. DHS has also established a communications center to coordinate national response efforts to cyber attacks and work directly with other levels of government and the private sector and has conducted several cyber attack simulation exercises.

Despite recent actions taken, a number of significant challenges remain to enhancing the security of cyber-reliant critical infrastructures, such as

- implementing actions recommended by the president's cybersecurity policy review;
- updating the national strategy for securing the information and communications infrastructure;
- reassessing DHS's planning approach to critical infrastructure protection;
- strengthening public-private partnerships, particularly for information sharing;
- enhancing the national capability for cyber warning and analysis;
- addressing global aspects of cybersecurity and governance; and
- securing the modernized electricity grid, referred to as the "smart grid."

In prior reports, GAO has made many recommendations to address these challenges. GAO also continues to identify protecting the nation's cyber critical infrastructure as a governmentwide high-risk area.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on the cybersecurity risks to the nation's critical infrastructure.

Increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. From its origins in the 1960s as a research project sponsored by the U.S. government, the Internet has grown increasingly important to both American and foreign businesses and consumers, serving as the medium for hundreds of billions of dollars of commerce each year. The Internet has also become an extended information and communications infrastructure, supporting vital services such as power distribution, health care, law enforcement, and national defense.

While the benefits have been enormous, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, can allow unauthorized individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Recent cyber-based attacks have further underscored the need to manage and bolster the cybersecurity of our nation's critical infrastructures.

Mr. Chairman, in February, GAO issued its biennial high-risk list of government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges.[1] Once again, we identified protecting the federal government's information systems and the nation's cyber critical infrastructure as a governmentwide high-risk area. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure, referred to as cyber critical infrastructure protection or cyber CIP.

[1]GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

In my testimony today, I will describe (1) cyber threats facing cyber-reliant critical infrastructures; (2) recent actions the federal government has taken, in partnership with the private sector, to identify and protect cyber-reliant critical infrastructures; and (3) ongoing challenges to protecting cyber critical infrastructure. In preparing this statement in July 2011, we relied on our previous work in these areas (please see the related GAO products page at the end of this statement). These products contain detailed overviews of the scope of our reviews and the methodology we used. The work on which this statement is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Critical infrastructures are systems and assets, whether physical or virtual, so vital to our nation that their incapacity or destruction would have a debilitating impact on national security, economic well-being, pubic health or safety, or any combination of these. Critical infrastructure includes, among other things, banking and financial institutions, telecommunications networks, and energy production and transmission facilities, most of which are owned by the private sector. As these critical infrastructures have become increasingly dependent on computer systems and networks, the interconnectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt critical systems, with potentially harmful effects.

Because the private sector owns most of the nation's critical infrastructures, forming effective partnerships between the public and private sectors is vital to successfully protect cyber-reliant critical assets from a multitude of threats, including terrorists, criminals, and hostile nations. Federal law and policy have established roles and responsibilities for federal agencies to work with the private sector and other entities in enhancing the cyber and physical security of critical public and private infrastructures. These policies stress the importance of coordination between the government and the private sector to protect the nation's computer-reliant critical infrastructure. In addition, they establish the Department of Homeland Security (DHS) as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation efforts, and recovery efforts for public and private critical infrastructure and information systems. Federal

policy also establishes critical infrastructure sectors, assigns federal agencies to each sector (known as sector lead agencies), and encourages private sector involvement. Table 1 shows the 18 critical infrastructure sectors and the lead agencies assigned to each sector.

Table 1: Critical Infrastructure Sectors and Lead Agencies

Critical infrastructure sector	Description	Lead agency or agencies
Agriculture and food	Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.	Department of Agriculture Department of Health and Human Services (Food and Drug Administration)
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.	Department of the Treasury
Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical sector produces products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	DHS
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	DHS
Communications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.	DHS
Critical manufacturing	Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.	DHS
Dams	Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	DHS
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	DHS
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Government facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the U.S. and abroad.	DHS

Critical infrastructure sector	Description	Lead agency or agencies
Health care and public health	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.	DHS
National monuments and icons	Maintains monuments, physical structures, objects, or geographical sites that are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance.	Department of the Interior
Nuclear reactors, materials, and waste	Provides nuclear power. The sector includes commercial nuclear reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste.	DHS
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector	DHS
Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	DHS
Water	Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.	Environmental Protection Agency

Source: GAO-08-1075R, GAO-11-537R.

In May 1998, Presidential Decision Directive 63 (PDD-63) established critical infrastructure protection as a national goal and presented a strategy for cooperative efforts by the government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government.[2] Among other things, this directive encouraged the development of information sharing and analysis centers (ISAC) to serve as mechanisms for gathering, analyzing, and disseminating information on cyber infrastructure threats and vulnerabilities to and from owners and operators of the sectors and the federal government. For example, the Financial Services, Electricity Sector, IT, and Communications ISACs represent sectors or subcomponents of sectors.

[2]The White House, *Presidential Decision Directive/NSC 63* (Washington, D.C.: May 22, 1998).

The Homeland Security Act of 2002 created the Department of Homeland Security.[3] Among other things, DHS was assigned with the following critical infrastructure protection responsibilities: (1) developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States, (2) recommending measures to protect those key resources and critical infrastructures in coordination with other groups, and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of or response to terrorist attacks.

In 2003, the *National Strategy to Secure Cyberspace* was issued, which assigned DHS multiple leadership roles and responsibilities in protecting the nation's cyber critical infrastructure.[4] These include (1) developing a comprehensive national plan for critical infrastructure protection; (2) developing and enhancing national cyber analysis and warning capabilities; (3) providing and coordinating incident response and recovery planning, including conducting incident response exercises; (4) identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems; and (5) strengthening international cyberspace security.

PDD-63 was superseded in December 2003 when Homeland Security Presidential Directive 7 (HSPD-7) was issued.[5] HSPD-7 defined additional responsibilities for DHS, sector-specific agencies, and other departments and agencies. The directive instructs sector-specific agencies to identify, prioritize, and coordinate the protection of critical infrastructures to prevent, deter, and mitigate the effects of attacks. It also makes DHS responsible for, among other things, coordinating national critical infrastructure protection efforts and establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors.

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

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

[5]The White House, *Homeland Security Presidential Directive 7* (Washington, D.C.: December 17, 2003).

As part of its implementation of the cyberspace strategy and other requirements to establish cyber analysis and warning capabilities for the nation, DHS established the United States Computer Emergency Readiness Team (US-CERT) to help protect the nation's information infrastructure. US-CERT is the focal point for the government's interaction with federal and private-sector entities 24 hours a day, 7 days a week, and provides cyber-related analysis, warning, information-sharing, major incident response, and national-level recovery efforts.

Cyber-Reliant Critical Infrastructures Face a Proliferation of Threats

Threats to systems supporting critical infrastructure are evolving and growing. In February 2011, the Director of National Intelligence testified that, in the past year, there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009.[6] Different types of cyber threats from numerous sources may adversely affect computers, software, networks, organizations, entire industries, or the Internet itself. Cyber threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.

The potential impact of these threats is amplified by the connectivity between information systems, the Internet, and other infrastructures, creating opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. For example, in May 2008, we reported that the Tennessee Valley Authority's (TVA) corporate network contained security weaknesses that could lead to the disruption of control systems networks and devices connected to that network.[7] We made 19 recommendations to improve the implementation of information security program activities for the control systems governing TVA's critical

[6]Director of National Intelligence, Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community, statement before the Senate Select Committee on Intelligence (Feb. 16, 2011).

[7]GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

infrastructures and 73 recommendations to address specific weaknesses in security controls. TVA concurred with the recommendations and has taken steps to implement them. As government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

Recent reports of cyber attacks illustrate that the cyber-based attacks on cyber-reliant critical infrastructures could have a debilitating impact on national and economic security.

- In June 2011, a major bank reported that hackers broke into its systems and gained access to the personal information of hundreds of thousands of customers. Through the bank's online banking system, the attackers were able to view certain private customer information.
- In March 2011, according to the Deputy Secretary of Defense, a cyber attack on a defense company's network captured 24,000 files containing Defense Department information. He added that nations typically launch such attacks, but there is a growing risk of terrorist groups and rogue states developing similar capabilities.
- In March 2011, a security company reported that it had suffered a sophisticated cyber attack that removed information about its two-factor authentication tool.[8] According to the company, the extracted information did not enable successful direct attacks on any of its customers; however, the information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack.
- In February 2011, media reports stated that computer hackers broke into and stole proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.
- In July 2010, a sophisticated computer attack, known as Stuxnet, was discovered. It targeted control systems used to operate industrial processes in the energy, nuclear, and other critical sectors. It is

[8]Two-factor authentication is a way of verifying someone's identity by using two of the following: something the user knows (password), something the user has (token), or something unique to the user (fingerprint).

designed to exploit a combination of vulnerabilities to gain access to its target and modify code to change the process.

- In January 2010, it was reported that at least 30 technology companies—most in Silicon Valley, California—were victims of intrusions. The cyber attackers infected computers with hidden programs allowing unauthorized access to files that may have included the companies' computer security systems, crucial corporate data, and software source code.

The Federal Government Has Taken Steps to Address Cyber Threats to Cyber Critical Infrastructure

Over the past 2 years, the federal government has taken a number of steps aimed at addressing cyber threats to critical infrastructure.

In early 2009, the President initiated a review of the nation's cyberspace policy that specifically assessed the missions and activities associated with the nation's information and communication infrastructure and issued the results in May of that year.[9] The review resulted in 24 near- and mid-term recommendations to address organizational and policy changes to improve the current U.S. approach to cybersecurity. These included, among other things, that the President appoint a cybersecurity policy official for coordinating the nation's cybersecurity policies and activities. In December 2009, the President appointed a Special Assistant to the President and Cybersecurity Coordinator to serve in this role and act as the central coordinator for the nation's cybersecurity policies and activities. Among other things, this official is to chair the primary policy coordination body within the Executive Office of the President responsible for directing and overseeing issues related to achieving a reliable global information and communications infrastructure.

Also in 2009, DHS issued an updated version of its National Infrastructure Protection Plan (NIPP). The NIPP is intended to provide the framework for a coordinated national approach to addressing the full range of physical, cyber, and human threats and vulnerabilities that pose risks to the nation's critical infrastructures. The NIPP relies on a sector partnership model as the primary means of coordinating government and private-sector critical infrastructure protection efforts. Under this model, each sector has both a government council and a private sector council to

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

address sector-specific planning and coordination. The government and private-sector councils are to work in tandem to create the context, framework, and support for the coordination and information-sharing activities required to implement and sustain each sector's infrastructure protection efforts. The council framework allows for the involvement of representatives from all levels of government and the private sector, to facilitate collaboration and information-sharing in order to assess events accurately, formulate risk assessments, and determine appropriate protective measures. The establishment of private-sector councils is encouraged under the NIPP model, and these councils are to be the principal entities for coordinating with the government on a wide range of CIP activities and issues. Using the NIPP partnership model, the private and public sectors coordinate to manage the risks related to cyber CIP by, among other things, sharing information, providing resources, and conducting exercises.

In October 2009, DHS established its National Cybersecurity and Communications Integration Center (NCCIC) to coordinate national response efforts and work directly with federal, state, local, tribal, and territorial governments and private-sector partners. The NCCIC integrates the functions of the National Cyber Security Center, US-CERT, the National Coordinating Center for Telecommunications, and the Industrial Control Systems CERT into a single coordination and integration center and co-locates other essential public and private sector cybersecurity partners.

In September 2010, DHS issued an interim version of its national cyber incident response plan. The purpose of the plan is to establish the strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident. It aims to tie various policies and doctrine together into a single tailored, strategic, cyber-specific plan designed to assist with operational execution, planning, and preparedness activities and to guide short-term recovery efforts.

DHS has also coordinated several cyber attack simulation exercises to strengthen public and private incident response capabilities. In September 2010, DHS conducted the third of its Cyber Storm exercises, which are large-scale simulations of multiple concurrent cyber attacks. (DHS previously conducted Cyber Storm exercises in 2006 and 2008.) The third Cyber Storm exercise was undertaken to test the National Cyber Incident Response Plan, and its participants included

representatives from federal departments and agencies, states, ISACs, foreign countries, and the private sector.

Challenges in Protecting Cyber Critical Infrastructure Persist

Despite the actions taken by several successive administrations and the executive branch agencies, significant challenges remain to enhancing the protection of cyber-reliant critical infrastructures.

- *Implementing actions recommended by the president's cybersecurity policy review.* In October 2010, we reported that of the 24 near- and mid-term recommendations made by the presidentially initiated policy review to improve the current U.S. approach to cybersecurity, only 2 had been implemented and 22 were partially implemented.[10] Officials from key agencies involved in these efforts (e.g., DHS, the Department of Defense, and the Office of Management and Budget) stated that progress had been slower than expected because agencies lacked assigned roles and responsibilities and because several of the mid-term recommendations would require action over multiple years. We recommended that the national Cybersecurity Coordinator designate roles and responsibilities for each recommendation and develop milestones and plans, including measures, to show agencies' progress and performance.

- *Updating the national strategy for securing the information and communications infrastructure.* In March 2009, we testified on the needed improvements to the nation's cybersecurity strategy.[11] In preparation for that testimony, we convened a panel of experts that included former federal officials, academics, and private-sector executives. The panel highlighted 12 key improvements that, in its view, were essential to improving the strategy and our national cybersecurity postures, including (1) the development of a national strategy that clearly articulates objectives, goals, and priorities; (2) focusing more actions on prioritizing assets and functions, assessing vulnerabilities, and reducing vulnerabilities than on developing plans;

[10]GAO, *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, GAO-11-24 (Washington, D.C.: Oct. 6, 2010).

[11]GAO, *National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: Mar. 10, 2009).

and (3) bolstering public-private partnerships though an improved value proposition and use of incentives.

- *Reassessing the cyber sector-specific planning approach to critical infrastructure protection.* In September 2009, we reported that, among other things, sector-specific agencies had yet to update their respective sector-specific plans to fully address key DHS cyber security criteria.[12] In addition, most agencies had not updated the actions and reported progress in implementing them as called for by DHS guidance. We noted that these shortfalls were evidence that the sector planning process has not been effective and thus leaves the nation in the position of not knowing precisely where it stands in securing cyber critical infrastructures. We recommended that DHS (1) assess whether existing sector-specific planning processes should continue to be the nation's approach to securing cyber and other critical infrastructure and consider whether other options would provide more effective results and (2) collaborate with the sectors to develop plans that fully address cyber security requirements. DHS concurred with the recommendations and has taken action to address them. For example, the department reported that it undertook a study in 2009 that determined that the existing sector-specific planning process, in conjunction with other related efforts planned and underway, should continue to be the nation's approach. In addition, at about this time, the department met and worked with sector officials to update sector plans with the goal of fully addressing cyber-related requirements.

- *Strengthening the public-private partnerships for securing cyber-critical infrastructure.* The expectations of private sector stakeholders are not being met by their federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. In July 2010, we reported that federal partners, such as DHS, were taking steps that may address the key expectations of the private sector, including developing new information-sharing arrangements.[13] We also reported that public sector stakeholders believed that improvements could be made to the partnership, including improving

[12]GAO, *Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment*, GAO-09-969 (Washington, D.C.: September 24, 2009).

[13]GAO, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*, GAO-10-628 (Washington, D.C.: July 15, 2010).

private sector sharing of sensitive information. We recommended, among other things, that the national Cybersecurity Coordinator and DHS work with their federal and private-sector partners to enhance information-sharing efforts, including leveraging a central focal point for sharing information among the private sector, civilian government, law enforcement, the military, and the intelligence community. DHS concurred with this recommendation and officials stated that they have made progress in addressing the recommendation. We will be determining the extent of that progress as part of our audit follow-up efforts.

- *Enhancing cyber analysis and warning capabilities.* DHS's US-CERT has not fully addressed 15 key attributes of cyber analysis and warning capabilities that we identified.[14] As a result, we recommended in July 2008 that the department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability as envisioned in the national strategy. DHS agreed in large part with our recommendations and has reported that it is taking steps to implement them. We are currently working with DHS officials to determine the status of their efforts to address these recommendations.

- *Addressing global cybersecurity and governance.* Based on our review, the U.S. government faces a number of challenges in formulating and implementing a coherent approach to global aspects of cyberspace, including, among other things, providing top-level leadership, developing a comprehensive strategy, and ensuring cyberspace-related technical standards and policies do not pose unnecessary barriers to U.S. trade.[15] Specifically, we determined that the national Cybersecurity Coordinator's authority and capacity to effectively coordinate and forge a coherent national approach to cybersecurity were still under development. In addition, the U.S. government had not documented a clear vision of how the international efforts of federal entities, taken together, support overarching national goals. Further, we learned that some countries had attempted to mandate compliance with their indigenously

[14]GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: July 31, 2008).

[15]GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010).

developed cybersecurity standards in a manner that risked discriminating against U.S. companies. We recommended that, among other things, the Cybersecurity Coordinator develop with other relevant entities a comprehensive U.S. global cyberspace strategy that, among other things, addresses technical standards and policies while taking into consideration U.S. trade. In May 2011, the White House released the *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. We will be determining the extent that this strategy addresses our recommendation as part of our audit follow-up efforts.

- *Securing the modernized electricity grid.* In January 2011, we reported on progress and challenges in developing, adopting, and monitoring cybersecurity guidelines for the modernized, IT-reliant electricity grid (referred to as the "smart grid").[16] Among other things, we identified six key challenges to securing smart grid systems. These included, among others,

  - a lack of security features being built into certain smart grid systems,
  - a lack of an effective mechanism for sharing information on cybersecurity within the electric industry, and
  - a lack of electricity industry metrics for evaluating cybersecurity.

  We also reported that the Department of Commerce's National Institute for Standards and Technology (NIST) had developed and issued a first version of its smart grid cybersecurity guidelines. While NIST largely addressed key cybersecurity elements that it had planned to include in the guidelines, it did not address an important element essential to securing smart grid systems that it had planned to include—addressing the risk of attacks that use both cyber and physical means. NIST officials said that they intend to update the guidelines to address the missing elements, and have drafted a plan to do so. While a positive step, the plan and schedule were still in draft form. We recommended that NIST finalize its plan and schedule

[16]GAO, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to Be Addressed*, GAO-11-117 (Washington, D.C.: January 12, 2011).

for updating its cybersecurity guidelines to incorporate missing elements; NIST agreed with this recommendation.

In addition to the challenges we have previously identified, we have ongoing work in two key areas related to the protection of cyber critical infrastructures. The first is to identify the extent to which cybersecurity guidance has been specified within selected critical infrastructure sectors and to identify areas of commonality and difference between sector-specific guidance and guidance applicable to federal agencies. The second is a study of risks associated with the supply chains used by federal agencies to procure IT equipment, software, or services, along with the extent to which national security-related agencies are taking risk-based approaches to supply-chain management. We plan to issue the results of this work in November 2011 and early 2012, respectively.

In summary, the threats to information systems are evolving and growing, and systems supporting our nation's critical infrastructure are not sufficiently protected to consistently thwart the threats. While actions have been taken, the administration and executive branch agencies need to address the challenges in this area to improve our nation's cybersecurity posture, including enhancing cyber analysis and warning capabilities and strengthening the public-private partnerships for securing cyber-critical infrastructure. Until these actions are taken, our nation's cyber critical infrastructure will remain vulnerable. Mr. Chairman, this completes my statement. I would be happy to answer any questions you or other members of the Subcommittee have at this time.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Michael Gilmore (Assistant Director), Bradley Becker, Kami Corbett, and Lee McCracken.

Related GAO Products

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems. GAO-11-463T. Washington, D.C.: March 16, 2011.

High-Risk Series: An Update. GAO-11-278. Washington, D.C.: February 2011.

Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed. GAO-11-117. Washington, D.C.: January 12, 2011.

Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk. GAO-11-43. Washington, D.C.: November 30, 2010.

Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed. GAO-11-24. Washington, D.C.: October 6, 2010.

Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems. GAO-10-916. Washington, D.C.: September 15, 2010.

Information Management: Challenges in Federal Agencies' Use of Web 2.0 Technologies. GAO-10-872T. Washington, D.C.: July 22, 2010.

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. GAO-10-628. Washington, D.C.: July 15, 2010.

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606. Washington, D.C.: July 2, 2010.

Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats. GAO-10-834T. Washington, D.C.: June 16, 2010.

Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development. GAO-10-466. Washington, D.C.: June 3, 2010.

Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing. GAO-10-513. Washington, D.C.: May 27, 2010.

Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. GAO-10-338. Washington, D.C.: March 5, 2010.

Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise. GAO-08-825. Washington, D.C.: September 9, 2008.

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. GAO-08-526. Washington, D.C.: May 21, 2008.

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

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper

Mr. STEARNS. I thank the gentleman.

Let me ask you a question. I have your opening statement here in which you mention various cybersecurity attacks. They are putting software viruses into the network. Is that primarily what it is?

Mr. WILSHUSEN. It could be a number of different attacks. In terms of one to include computer intrusions in which individuals are able to gain access through the installation of malicious software. For example, if a user inadvertently plugged a USB into his computer that was corrupted, it could install some malicious software, which might facilitate an attack.

Mr. STEARNS. Now, when an attack occurs——

Mr. WILSHUSEN. Um-hum.

Mr. STEARNS [continuing]. Generally, what does that attack look like? They are coming in to steal information, or are they coming to put in a replicating software that will destroy it, or is it just putting in there to observe? What of those three?

Mr. WILSHUSEN. It could be any of the combinations.

Mr. STEARNS. Any of those three combinations?

Mr. WILSHUSEN. Right. One, in terms of either to sabotage his particular system or gain information for future attacks perhaps or as well to——

Mr. STEARNS. Depending upon their motivation.

Mr. WILSHUSEN. Depending upon their motivation.

Mr. STEARNS. Mr. McGurk, what do you think?

Mr. MCGURK. Yes, sir. I would also echo my colleague's statements that the vast array of capability we see demonstrated with the malicious code is such that it encompasses all of those things.

Mr. Chairman, you had mentioned Stuxnet earlier. That is a great example of a particular piece of malicious code that demonstrated very unique capabilities. It not only exploited what we call zero-day vulnerabilities, which are vulnerabilities that are not known in the public environment, but also it used advanced communication capability. It did advanced reconnaissance, so it was gathering information. And subsequently, it left behind that malicious code that was able to have a physical impact.

Mr. STEARNS. Now, are we in the United States, you know, we have jurisdiction over energy, water, information technology, communication, nuclear plants—are we vulnerable to Stuxnet in your opinion?

Mr. MCGURK. Sir, because of the ubiquitous nature of information technology in the critical infrastructure, the exploitation may occur in one sector and it could actually migrate into another sector.

Mr. STEARNS. So yes or no? Do you think we are vulnerable?

Mr. MCGURK. I would say the vulnerabilities exist and the capability to exploit those vulnerabilities exist.

Mr. STEARNS. OK. So the big question is that the American people want to know what has the United States Government done about that to make sure we don't have that attack?

Mr. MCGURK. Much of the Department's focus over the past several years has been on mitigating the vulnerabilities associated with those critical infrastructure systems.

Mr. STEARNS. Do you do it by having innocuous or something that inoculates us from this software or do you do it to make sure you don't put the USB port or how are you doing this?

Mr. MCGURK. So it is a multifaceted approach, sir. Much of it is through an education program, so we work with the private sector to develop standards required to educate the community on good practices and uses of equipment and technology. We actually conduct——

Mr. STEARNS. You think education alone would do it?

Mr. MCGURK. No, sir. We also conduct vulnerability analyses of products in our laboratories in conjunction with the national laboratory community where we actually take vendors products and do a complete vulnerability assessment of those products. We also develop practices for owners and operators because in some cases, especially in the power companies, it is not a matter of replacing the technology, so you have to be able to put practices in place that mitigate the risk. And they are also working with the security communities to actually provide an enclaving capability so that we can secure the environments around which they operate.

So by taking this multifaceted approach, we can identify not necessarily the threat actors and focus on the threats which are coming from many areas, but the vulnerabilities themselves and mitigating the risks associated with those vulnerabilities.

Mr. STEARNS. Let me ask you a question but with this Stuxnet. What have we done to protect those specific vulnerabilities in Seimens' product? In other words, has DHS issued a guidance on this?

Mr. MCGURK. Yes, sir. The Department, when we started analyzing Stuxnet back in July of last year, we identified the capabilities of the particular piece of mal code. We understood its capabilities and subsequently we put mitigation plans in place working with the specific sectors to identify the mitigation strategies associated with that. But since that particular piece of mal code was looking for a very unique combination of hardware and software, it was easy to identify what the mitigation strategies would be.

Mr. STEARNS. OK. Ms. Stempfley, just last Friday, the head of US–CERT resigned. US–CERT is the group charged with collaborating with state and local governments and private industry on cyber attacks. There have been a number of recent attacks on government systems, the Senate, FBI, CIA, and even a Gmail hacking aimed at top government officials. Have all of these recent attacks caused any change in the direction or change in the operation in US–CERT?

Ms. STEMPFLEY. No, sir. The US–CERT's set of responsibilities stays the same. And as we commented in the opening statements and your opening statements as well, this is a very sophisticated environment and it is constantly evolving. And as a part of that evolution, we understand that we have to have a bench and a mechanism for growth of individuals as we go forward. And so Randy's departure was a decision that he made and we have a continued direction and focus in prevention, preparedness, and restoral responsibilities across the board.

Mr. STEARNS. What were the vulnerabilities that allowed these systems to be infiltrated, and do these same kind of vulnerabilities exist in the private sector and on control systems?

Ms. STEMPFLEY. I am sorry, sir. Could you repeat the question?

Mr. STEARNS. With regard to the Senate, FBI, and CIA and even the Gmail hacking aimed at top government officials, what were the vulnerabilities that allowed these systems to be infiltrated?

Ms. STEMPFLEY. There were a number of vulnerabilities that were associated with these kinds of events that occurred, and to respond to where are other members of the private sector potentially vulnerable, I believe that is a true statement. As we commented earlier, there are a great deal of vulnerabilities that exist in the environment, and you will see that through the production of warning products and awareness notifications, we provide mitigations and indicators for private-sector owners and operators to put in place in their infrastructure. It is a shared responsibility between us and the private sector in order to implement the restorative and preventative measures.

Mr. STEARNS. Thank you. My time has expired. The gentlelady from Colorado.

Ms. DEGETTE. Thank you very much, Mr. Chairman.

I want to go a little bit more in depth into some of the issues that we face trying to work on interoperability between our governmental agencies and privately owned endeavors. In particular with our communications infrastructure, which is of course an essential part of our critical infrastructure, one of the things I am concerned about 90 percent of our communications networks are privately owned by commercial carriers. So traditionally, the FCC has worked with commercial carriers to ensure the reliability of the communications networks, and under current FCC rules, carriers have to report regarding outages on legacy telecommunications system. Now, the FCC in turn uses this data to help industry standards groups to improve on the best practices.

So I am wondering, Ms. Stempfley and Mr. McGurk, if you can talk to me a minute given FCC's historical involvement with the communications infrastructure and the relationship with commercial carriers, don't you think that they can take an important role in helping drive greater awareness of cyber threats?

Ms. STEMPFLEY. So reporting is always good and the ability to get information about what is going on is an important part of how we can frame that national picture of what is happening and the response activities. So we have a history of working both with private industry directly and with other members of government in order to increase the awareness and the response actions that are necessary. I think the same would be true here.

Ms. DEGETTE. Mr. McGurk?

Mr. MCGURK. In addition, ma'am, what I would like to add is that in response to the reporting that is conducted, part of the capability that exists within the NCCIC is our National Center for Coordination for Communications. And they receive those direct reports. So from a situational-awareness standpoint, the watch center receives real-time reporting from not only the telecommunication industry itself but also from other federal departments and agencies so that we get a better understanding from a holistic view on

the impacts to communications because as we recognize that many of the critical infrastructures are relying on communications for controlling issues, for communications issues, and for flowing of data.

In addition, we have the physical carriers themselves located within the watch environment so that they can provide up-to-date and actionable intelligence so that we can take the necessary steps and make proper recommendations.

Ms. DEGETTE. Now, the office of Homeland Security coordinates those efforts on cyber threats. And so I guess my question to you following up is if there is a breach in the communications network, then how do DHS and FCC respond? How do they interact together to respond?

Mr. MCGURK. Part of the National Cyber Incident Response Plan includes the development and coordination of a cyber-unified coordination group or cyber UCG. This is a steady state body of emergency response and incident handlers at working level, at the operational level, and then also at the senior decision-making level. For our cyber UCG seniors, it encompasses individuals from the departments and agencies that are at the assistant secretarial level or higher. So these are the actual decision-makers in the Federal Government. And then we have a staff which encompasses not only private sector but representatives from the federal departments and agencies that coordinate on a daily basis and share real-time information whether it comes from the communications sector, the energy sector, or one of the other 18 critical infrastructures. So that enables us to have that constant flow of data and provide that actionable intelligence so that private-sector companies can take the necessary steps to mitigate risk.

Ms. DEGETTE. OK. Now, as I understand it, the FCC has proposed to rule this spring to extend reporting requirements about network shortages to the broadband network and they are taking public comments on that issue. And so, Mr. Wilshusen, I was going to ask you do you think that collecting data on broadband outages would help gain a better understanding of when hackers have gotten into our systems?

Mr. WILSHUSEN. We haven't examined that issue, but I would imagine collecting information can only be helpful in making such a determination.

Ms. DEGETTE. OK. And for the other two witnesses, do you have any thoughts on the potential for reporting broadband network outages to contribute to situational awareness like after there is a major emergency, something like that?

Mr. MCGURK. Yes, ma'am. I believe as Ms. Stempfley had mentioned earlier, reporting is good and more reporting is even better. So the more information that enables us to develop that common operation picture that takes all of the data that we are receiving and then fuses that together. So the more information we receive in the NCCIC the better situational awareness we can provide not only to the secretary of Homeland Security and the other executive secretaries, but also to the President for decision-making capability.

Ms. DEGETTE. And just one last question relating to my opening statement about our communications networks is there is a lot of

issues around supply chains for equipment and components that have been manufactured abroad for use in the U.S. So I am wondering if these two witnesses on the end, Ms. Stempfley and Mr. McGurk, can talk about this publicly. Can you talk about how DHS is working with other federal agencies to address that issue of supply chain that part of it is foreign?

Ms. STEMPFLEY. So as you pointed out, the telecommunications supply chain activities are an interagency response within the Federal Government. It would be more than happy to bring another agency body back to discuss that in detail?

Ms. DEGETTE. Thank you.

Thank you very much, Mr. Chairman.

Mr. STEARNS. I thank the gentlelady.

The gentleman from Texas, Dr. Burgess, recognized for 5 minutes.

Mr. BURGESS. Thank you, Mr. Chairman.

Now, if I understand things correctly, there is an authority that exists within the executive branch to take some control of transmission grid operations in the event of a national emergency, is that correct? Either of DHS witnesses.

Mr. MCGURK. Yes, sir. The Secretary for the Department of Energy has that authority.

Mr. BURGESS. And is it necessary to place any limits on that authority?

Mr. MCGURK. Sir, I have the luxury of being a simple sailor and an operator and I don't normally identify or make recommendations on policy or operational requirements. I can say that within the guidelines that we currently have and the authorities that we currently have, we are able to execute our mission both efficiently and effectively. So I will leave that to other members of the Department to comment as far as additional requirements.

Mr. BURGESS. Ms. Stempfley, do you have any thoughts on that?

Ms. STEMPFLEY. Respectfully, sir, I believe that would be most appropriate for DHS not to comment on the legal authorities of another department.

Mr. BURGESS. Well, let me ask you this. Should such an authority be necessary? Should such an occurrence happen that the authority was necessary? How long would you expect that presidential emergency authority to be exercised over a continuous time period?

Ms. STEMPFLEY. Regrettably, sir, I am not in the position to answer that question.

Mr. BURGESS. Well, let me ask you this. It seems like—and I think it was referenced by either the chairman or the ranking member in their opening statements—is that we are hearing more and more about this. Does this just reflect the situational awareness that these types of threats and these types of attacks can occur or is, in fact, this a real phenomenon with the rapidity with which these attacks are coming is increasing?

Ms. STEMPFLEY. So I believe it is all of those things, sir. There is certainly more awareness within the community of the importance of cybersecurity and the overall activity. That is increasing both the detection actions that are occurring and the reporting ac-

tions that exist. Based on that awareness and what we are seeing is that increase across the board.

We are also, as we all indicated in our opening statement, seeing an increase in sophistication of the attacks as they occurred as well. So I believe it is a phenomenon of all things, sir.

Mr. BURGESS. Mr. McGurk, do you have any thoughts on that?

Mr. MCGURK. Not in addition, sir. The only thing I would add was that because of the adoption of information technology capabilities into the critical infrastructure, we are also exposing a greater landscape of vulnerabilities to areas that were in the past specifically closed off and proprietary in nature. So by adopting that technology, we also advance the vulnerability landscape associated with those critical infrastructure operations.

Mr. BURGESS. Well, one of the hazards in this is you are always fighting the last attack. What sort of forward-looking policies and procedures are being implemented by DHS? Are you looking into for wherever the perpetrator is, what is the value that they are deriving from these and are there ways that we can perhaps preempt some of these attacks before they happen rather than just simply reacting to them?

Mr. MCGURK. Sir, part of what the National Cyber Incident Response Plan focuses on is moving from the left end of the continuum where we are primarily focusing on response and recovery, which to your point, sir, is accurate. We are always fighting that last event or that last battle.

What we are looking forward to working with the private sector is moving to the right and putting the preparedness, the protective, and the preventative measures in place. And we are taking, again, a multifaceted approach through advanced technology, working with the owners and operators, and also with the vendor community to establish criteria for new systems and new operational parameters.

The Department produces a procurement guideline for owners and operators which talks about security requirements for new systems and new operating procedures. And we also work closely with the integration community so that we are identifying how to install and how to manage these systems as they are being updated in the critical infrastructure. So we are looking at it as a continuum shifting more from the left, the responsive part, over to the right where we are being preventative and predictive.

Mr. BURGESS. Now, a vast majority of this critical infrastructure is in private hands, is that correct?

Mr. MCGURK. That is correct, sir.

Mr. BURGESS. So is there any type of analysis as to the cost that may be incurred by the private sector to keep up with what you just articulated.

Mr. MCGURK. Yes, sir. In fact, the Department identifies and describes risk as an equation of threats, vulnerabilities, and consequences. When we work with the private sector, we understand that the denominator there is also cost. So the procurement standards that I had mentioned earlier takes that into account. Not everything can be a gold standard. We are not saying that you have to have absolute security across the board. It is a risk-based approach so we take that same levelized approach and build the busi-

ness case to identify what we need to implement in what areas. So if we are going to spend a dollar to mitigate risk, should we focus on the threats or should we focus on mitigating the risks and the vulnerabilities? And then what are the subsequent consequences associated with that? That is really one of the approaches that we are taking in addressing this issue.

Mr. BURGESS. And do you solicit and accept input from the private sector, the owners of the critical infrastructure as to that pricing consideration?

Mr. MCGURK. Yes, sir. In fact, as the chairman had mentioned earlier, one of the things that we focus on is a number of working groups. And in the industrial control systems area, we actually sponsor a joint public-private working group, the Industrial Controls System Joint Working Group, ICSJWG, which looks at not only mitigating risks but also product development, implementation, education, and a whole host of issues. And that is a complete joint environment with both public and private members represented.

Mr. BURGESS. Thank you, Mr. Chairman. I will yield back.

Mr. STEARNS. I thank the gentleman.

Dr. Christensen is recognized for 5 minutes.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

Again, welcome to our panel.

Under Homeland Security Presidential Directive 7, healthcare and public health are identified as critical infrastructure sectors, and of course the healthcare sector plays a significant role in response and recovery in the event of a disaster. So I would like to talk with all of our witnesses about the efforts to protect this sector against cyber threats.

Beginning with Ms. Stempfley and Mr. McGurk, what do you see as the major challenges to ensuring cybersecurity in the healthcare sector?

Ms. STEMPFLEY. Ma'am, I will begin with some of the kinds of policy challenges we have been working through in the Federal Government associated with this. And so, for example, we are working to deploy technological solutions that enable detection and prevention measures in place. Those technological solutions oftentimes require a very detailed analysis of the kinds of privacy and protection requirements that need to be put in place that we all feel so strongly about as well and we need to work through some of those key policy nexuses between the two so that we can provide that kind of support and prevention support while still being very true to the protection measures that we feel so strongly about in terms of privacy and other areas.

Those kinds of infrastructure systems are very important to us and we agree with that. Once we get past the policy questions, it is a matter of how we employ those solutions, best practices across the board and handle the equally important integrative systems that exist in healthcare and have that nexus between IT and embedded systems as well.

Mr. MCGURK. Yes, ma'am. I would also mention that one of the Department's focuses is also on not just protecting the information in accordance with a number of regulations and requirements but also the equipment itself. When we look at the vulnerabilities asso-

ciated with the other sectors, the healthcare industry also has an equal number of vulnerabilities associated with embedded medical devices or with advanced technology that could potentially be exploited because of the inherent communications capability of those devices.

So again, the Department is taking not just a data-in-motion, data-at-rest approach, but a holistic approach to the healthcare industry, working with the private sector, working with the manufacturers of these pieces of equipment, and also with the necessarily federal departments and agencies so that we understand the risks associated with healthcare industry and provide actionable steps that will better improve not only the quality of service but the quality of life.

Mrs. CHRISTENSEN. Thank you. And those focuses estimates are great. I am assuming you are working with the Department of Health and Human Services as well as with the private sector.

Ms. STEMPFLEY. With any of the particular sectors, ma'am, we work very strongly with the sector-specific agency in helping Human Services specifically in the situation.

Mr. MCGURK. In fact, ma'am, we have the National Health Information Sharing and Analysis Center coming to visit and tour the NCCIC tomorrow and part of our development process to get them physically located on board. So they will be actually visiting us tomorrow so that we can identify those connections.

Mrs. CHRISTENSEN. Great. Great.

Mr. Wilshusen, I am also interested in hearing more about GAO's work on cybersecurity issues that affect health and public health. As providers use more computer-based mechanisms and programs to help them treat patients, and I guess this sort of follows up on what you were saying, Mr. McGurk, do you agree that it poses additional risk to the personal health information could be released to the public?

Mr. WILSHUSEN. Certainly. In fact, we have a couple of engagements that we have ongoing or will start soon. One was mandated by the High-Tech Act in which GAO is responsible for reviewing the security and privacy protections over information that is transferred and exchanged through the Electronic Prescription System or E–Prescribing.

Mrs. CHRISTENSEN. Um-hum.

Mr. WILSHUSEN. We anticipate starting that engagement in September with the report release date on September 2012.

In addition, we have another engagement that we are currently working on to look at the security controls and risks associated with embedded or implantable medical devices such as insulin pumps, pacemakers and that that can be accessed through wireless technologies and may have chips in place. So we are also examining the report of security risk associated with that, as well as FDA's premarket and post-market review processes to address those particular risks.

Mrs. CHRISTENSEN. Well, thank you. My time is running out. I appreciate the information because the ever-increasing use of technology in our healthcare system obviously holds a lot of promise and many benefits. But also as we increase our reliance on tech-

nology, there is also—as you have pointed out very clearly—the opportunity to hack in and interfere with that.

So thank you, Mr. Chairman. I am out of time.

Mr. STEARNS. I thank the gentlelady. Gentlelady from Tennessee, Mrs. Blackburn, recognized for 5 minutes.

Mrs. BLACKBURN. Thank you, Mr. Chairman.

Ms. Stempfley, I wanted to come with you. I was just meeting with one of my airports, and I wanted to know—TSA. What does the DHS and TSA do with the body images that they collect from the scanners at the airports? How long are they stored and do you protect these images? Do you share them with any other agency? And what action would you take in case you had a breach?

Ms. STEMPFLEY. Ma'am, the Office of Cybersecurity and Communications is responsible for setting standards that the Federal Government has to comply with to include TSA. I am not familiar with their specific——

Mrs. BLACKBURN. Would you get back to me on this?

Ms. STEMPFLEY. I certainly would.

Mrs. BLACKBURN. OK. I know that it is a part of what we are talking about and it also pertains to the privacy work that we are doing in our CMT Committee. And I think as we work with some of the issues we are having with TSA, I would love to have the answer if you could do that.

I have got another question. This would be for you and Mr. McGurk. And I mentioned TVA in my opening comments and the amount of coverage that we have with the power security. I want to see what your interface is with the state and local governments and the infrastructure by facilitating the information sharing of the cyber threats and the incidents and through the ISACs. So there are 16 of those ISACs, right? OK. And very briefly if you would just go through how it works, what kind of information that is shared, what is your process how you protect the data that you get and what your expectation is, the state and local governments, that they are going to protect that data and then what your response would be if you had a breach?

Mr. MCGURK. Thank you, ma'am. I would just like to start off by saying that we have a very close working relationship with the Tennessee Valley Authority. In fact, we visited many times and we share real-time information through a number of sensor programs that we operate so that we have a better understanding of the actual threats and impacts and associated with those operational environments.

What we do and how we share that information from the standpoint at the national level is much of the data that is voluntarily submitted through the NCCIC comes from either the ISACs themselves—the Information Sharing and Analysis Centers, including the Multi-State—or it comes from the private-sector companies themselves. Much of that data is submitted under the secretary's authority for the protection of critical infrastructure information or PCII. That protects that information from being released even to a regulator, for instance if it is a power company and they submit the information to us.

We then take that and we work directly with that company to develop a mitigation strategy that is a) company-specific and then

b) we anonymize it to the point where it becomes a sector-specific mitigation strategy. The RSA data breach was a great example of how, within a short period of time, less than 24 hours of notification of the breach, we had more than 50 companies and federal departments and agencies represented under the Cyber Unified Coordination Group developing sector-specific mitigation plans. So those individuals—not only from a physical environment but also a data-sharing environment—collaborate to generate those mitigation plans.

Mrs. BLACKBURN. OK. And at what point do you pull state or local government into that to participate?

Mr. MCGURK. Continuously. So they actually have a representative on the floor of the Multi-State ISAC.

Mrs. BLACKBURN. OK. OK.

Mr. MCGURK. So they are there in real time.

Mrs. BLACKBURN. All right.

Ms. STEMPFLEY. And ma'am, to continue on in that discussion, we have worked with the 50 states to provide clearances to the chief security officers in each of the states and then share classified information through their fusion centers so that that provides not just their representation on floor in real time around an event but also gives us an ability post-date it to them in their states as well.

Mrs. BLACKBURN. And then do you do any coeducation and training with local law enforcement back into your protocols?

Ms. STEMPFLEY. The training activity that we provide—all of our training is provided on an open basis so that state representatives can come and participate. I can't speak to which states have chosen to come in with particular law enforcement individuals, but we make it available to them in order for them to take it up.

Mrs. BLACKBURN. Excellent. Thank you, Mr. Chairman. Yield back.

Mr. STEARNS. The gentlelady from Florida, Ms. Castor, is recognized for 5 minutes.

Ms. CASTOR. Thank you, Mr. Chairman. Thank you to the witnesses for your insight today.

It is apparent that an effective partnership between the Federal Government and the private sector is necessary to ensure the security of all of our networks, whether those networks manage critical infrastructure or simply handle the day-to-day data of the Federal Government and communications.

Mr. Wilshusen, in your testimony you noted that the private sector has expressed concerns that DHS is not meeting their expectations in terms of information sharing. What concerns does private industry have about DHS' willingness to provide information?

Mr. WILSHUSEN. Yes, ma'am. We did a review in which we surveyed 56 individuals from the private sector from five private-sector councils. And we found that they identified a number of key activities that they thought were critical or important for the public-private partnership to include the provision of timely and actionable threat and alert information, having a secure mechanism for collecting information or sharing information with the public sector. And they indicated only 27 percent of those respondents indicated that they felt that their public-sector partners were actually meeting those expectations to a great or moderate extent. And so

there are a number of concerns about being able, on the part of the private sector, to collect timely information from the public-sector partners.

Ms. CASTOR. Were there any particular sectors that stood out that appeared to be problematic?

Mr. WILSHUSEN. Well, from the private-sector side, it was pretty much across the board. The five sectors that were included in our study included the banking and finance sector, the IT sector, the communications, energy, and the defense industrial base sectors. And it was pretty much across the board. As I mentioned, only 27 percent out of the 56 respondents actually felt that they were receiving support to a great or moderate extent.

Ms. CASTOR. So Mr. McGurk, what is DHS doing to address these concerns and to ensure that you all are working collaboratively with the private sector?

Mr. MCGURK. Ma'am, I would like to start off by saying, you know, can we do better? Absolutely. We have modified much of the structures by actually standing up and creating the NCCIC that met some of the requirements moving forward, by actually having the private sector participate and not only receiving the information but developing the information. By having them physically present in the environment really assists us in putting the information in a language that is necessary to reach our constituents.

A great example is in the past when we would produce information, we would produce it in a language that we understood, and then we would send that out and that may or may not meet the needs of our private-sector partners. By having power engineers and financial services specialists and IT specialists physically sitting there working with us and collaboratively developing the knowledge necessary to distribute, we are able to provide actionable intelligence.

Just last year we received a report in an intelligence communication of a particularly malicious piece of mal code that had a subject line on an email called "here you have." Within a few hours of that appearing in a classified report, the US–CERT produced an early warning and notice that went out to the broad private sector because we took that data, declassified it, and provided actionable intelligence for our private-sector partners. But by having them there and participating really enables us to provide better products for our partners and also speeds up the time necessary to generate that product.

Ms. CASTOR. Well, how about the flip side? I am also curious about how well the private sector is communicating with DHS when they suffer a cyber attack or a breach, Mr. McGurk, are private companies required to report cyber attacks or coordinate their responses to those attacks with DHS?

Mr. MCGURK. So there is no requirement to report the information directly to the Department, but I think what has happened over the development of the partnership over the past several years is the stigma associated with cyber breaches has started to be removed and companies are volunteering the information because they understand that it not only benefits their ability to maintain goods and services but it will also assist the broader community because they recognize that when they share with the Department,

we are not going to publish company-specific information. We are going to anonymize that and produce mitigation strategies and plans that help the broad sectors. And they have been working very closely with us in developing that.

Ms. CASTOR. Are there instances where DHS has become aware of a cyber attack or a breach in a particular company and then you contacted that company to assist and they declined your offers to work with them, declined assistance?

Mr. MCGURK. Yes, ma'am.

Ms. CASTOR. What can we do about that? How do we improve the collaboration in working together?

Mr. MCGURK. Part of that is an awareness and an understanding. From the private-sector standpoint, I understand that we have to demonstrate value and they have to see how working with DHS and partnering with DHS adds value to their capability. In some cases, those particular companies had a very advanced capability. We gave them the early-warning notice that they needed to take the necessary steps to protect their networks. So subsequently, additional response from DHS wasn't required. And in the extreme case, we received declination for support but recognition of the awareness or the alert.

Ms. CASTOR. Thank you very much.

Mr. MCGURK. Thank you, ma'am.

Mr. STEARNS. The gentleman from Virginia is recognized for 5 minutes, Mr. Griffith.

Mr. GRIFFITH. I am just curious, Mr. McGurk, under what circumstances, if any, would the DHS NCCIC withhold cyber threat information that it has encountered from owners or operators of critical infrastructure?

Mr. MCGURK. Sir, we do not withhold threat information, but subsequently, we don't develop threat information. Under the authorities of the Department, we focus primarily on mitigation of risk, and that is where we focus our activities. Threat information is really developed by the intelligence community and we rely on that partnership with the intelligence community to identify threat actors.

Mr. GRIFFITH. All right. Do you have any indication that they may be sometimes withholding information?

Mr. MCGURK. No, sir. In many cases, what is germane to mitigation is not necessarily associated with the actor. It is the activity. So it is the exploitation of the vulnerability which is necessary to share to protect the networks, not who is actually doing it.

Mr. GRIFFITH. Mr. Wilshusen, the GAO reported in October of 2010 that only 2 of 24 recommendations by the President Cybersecurity Policy Review had been implemented and the rest had only been partially implemented. What can you tell us about whether any additional progress has been made?

Mr. WILSHUSEN. Well, one of the reasons we found that the partial implementation occurred was because many of the agencies were not taking effect because they were not given specific roles and responsibilities to implement some of those recommendations, and that kind of delayed actions to implementing that. We will be following up as part of our annual review follow-up on our recommendations to see what extent those recommendations are now

being met. But since we just issued that in October, we have not gone back to follow up on our prior recommendations and to do a reassessment.

Mr. GRIFFITH. Should we expect an updated report this coming October?

Mr. WILSHUSEN. We will be updating the status of our recommendations, and if you request us to do it, we will certainly do it.

Mr. GRIFFITH. I would be curious since only 2 of the 24——

Mr. WILSHUSEN. Right.

Mr. GRIFFITH [continuing]. Were implemented as of last year, and I am just wondering should we be concerned that so few of the recommendations had been fully implemented at that time?

Mr. WILSHUSEN. Well, there are 10 near-term recommendations coming out of that policy review, 14 mid-term recommendations. Several of the mid-term recommendations are actions of such a nature that it is going to take multiple years to fully implement those. But the near-term recommendations are very important and they should be implemented as soon as possible.

Mr. GRIFFITH. All right. I thank you. Yield back my time.

Mr. STEARNS. The gentleman yields back.

Yes?

Mr. BURGESS. Would you yield to me for follow-up questions?

Mr. GRIFFITH. I yield for follow-up.

Mr. BURGESS. Dr. Christensen asked some very good questions on the healthcare aspects of the critical infrastructure and going along with what the gentleman was just asking as far as those forward-looking threats, it seems like we have created some problems for ourselves in the High-Tech Act and some of the things we have done with the information technology infrastructure as applied to health. Star Clause, for example, which prohibit hospitals from putting wire in a doctor's office if the doctor is not directly affiliated with the hospital. So pushing a lot of these vertically integrated systems to go on the internet in order to have the abilities or the ease of transfer of the data, which then renders them vulnerable to attacks on the internet. Have you looked at that, whether perhaps there is something that could be done on the policy side to lessen the impact of the vulnerability if we were to make some changes on the regulatory side? A closed loop if you would between the hospital and a group of doctors, even though they are not all part of the same business model might be one way to do that. Have you explored that at all?

Ms. STEMPFLEY. So your example is a wonderful example of furthering the independence between the infrastructures as they go forward.

Mr. BURGESS. No, it is an example of how we make things harder than they need to be in the first place and then we have got to do a whole bunch more stuff to make it workable in the real world. But continue.

Ms. STEMPFLEY. Thank you, sir. The specific reviews, technical reviews of proposals is not something that we certainly do. What we work towards are best practices for the kinds of separation and containment that might be necessary in order to understand the environment. Each of the owners and operators has a better under-

standing of the risks in their particular environment in the business models that best serve them in each of these cases. And so the set of best practices are an important part of how we do this.

Mr. BURGESS. But do we look at the regulations that we, the Federal Government, have put in place that make it harder for people to do the right thing in the real world?

Ms. STEMPFLEY. So I am not sure I can say that specific regulation was reviewed prior to in order to understand the potential implications across the board, but we do look at regulations and procedures as they come up.

Mr. BURGESS. I appreciate the gentleman for yielding. My time has expired. Let us look at that going forward. I yield back.

Mr. STEARNS. I thank the gentleman.

Ms. Schakowsky is recognized for 5 minutes.

Ms. SCHAKOWSKY. Thank you.

Have any of you, the three of you, read Stieg Larsson's book, the Girl with the Dragon Tattoo, et cetera?

Mr. WILSHUSEN. Yes.

Ms. SCHAKOWSKY. You have. If you haven't, people who are into cybersecurity would not only enjoy them but probably be a little worried about it. The pretty flawed heroine, Lisbeth Salander, there is no firewall too high or wide or low that she can't get through. And I think she is the heroine, sort of the good guy, but the notion of individual actors out there who have this tremendous capacity to infiltrate I think is a real concern. I sit also on the Intelligence Committee, and we think about that a lot.

So here is what I wanted to ask. Do we employ sort of old-school kinds of techniques like redundancy to make sure—I remember sitting in a hotel room watching a rolling blackout in Ohio a number of years ago, which turned out to be a failure of the grid and not some sort of attack—this was post-9/11—but felt like it might have been. So do we build in things like we do in aircraft or whatever, just redundancies so we are not as vulnerable? Can someone answer?

Mr. MCGURK. Yes, ma'am. I do agree that one of the salient points of the book was that they were focusing on perimeter defense as a method of ensuring their security, and as you quite adequately pointed out that there was no wall too high or too thick that she couldn't get through in the process, and subsequently, that is why the Department doesn't look at only a perimeter-defense strategy as part of enabling a sound cybersecurity profile. We look at a defense-in-depth strategy so that there is layers upon layers of security implemented. In addition, we want to focus on the practices and procedures to address the various risk associated with operating those networks. Whether it is from insider activity, whether it is from nation-state-sponsored, whether it is criminal activity, we treat the act separate from the actors so that we can understand what they are trying to exploit as far as the vulnerabilities. So that is the approach that the Department takes, and we do work very closely with the intelligence community, law enforcement community, and the private sector to develop those necessary strategies so that we can have a better and more secure defense posture.

Ms. SCHAKOWSKY. Let me ask another question. There is a lot of talk and even advertising about how we can centralize data management and storage and concentration and that you can access that without individual servers and all kinds of things to make business more efficient, et cetera. I am wondering if this creates a new layer, then, of vulnerability if everything is sort of outsourced to one place.

Ms. STEMPFLEY. The what I call re-architecting moments that are going on in the environment, things like the movement to cloud computing and mobility are intelligent and opportunity at the same time. So there certainly are vulnerabilities that exist in that environment that must be addressed as we architect to move things there. But it isn't generally a lump sum, just pick up and move. There are design considerations that must be taken into account as you move. And so they are these opportunities for individuals to look at how they both handle their data procedurally and how they protect it through this defense-in-depth approach across the board.

Mr. WILSHUSEN. And if I may add we did a review over the clouds computing security and identified a number of both positive as well as negative security implications of going to the cloud computing. Particularly of the negative sort is just agencies lose control over the access to their data, who has access to it, as well as the ability of agencies who are still responsible for the protection of that information to assure themselves through independent testing or other evaluations that the cloud service provider is actually implementing security effectively over their environment and the information. And those are still issues that are still being worked out. The Federal Government, through GSA—I am not sure if DHS is involved in this—OMB and others are studying up different procedures through FedRAMP and some other programs to try to address some of those areas.

Ms. SCHAKOWSKY. I started by talking about this rolling blackout that I saw. I wondered if we can talk about how secure our power grid really is. I don't know if you addressed that earlier. There was a project that showed the effect of hacking into a power plant's control station via computers and digital devices, so I am just wondering how that came out and if there are vulnerabilities that we are correcting?

Mr. MCGURK. Yes, ma'am. The purpose behind the Aurora evaluation and experiment that was conducted by the Department in conjunction with the Idaho National Lab back in 2007 was essentially identifying the interdependencies between the critical infrastructures. That is how it started out. We wanted to see if we could have a negative impact in an environment by attacking the capabilities or the equipment of another environment. For instance, if I destroyed the generation capability, could I then have an adverse impact on a data-storage center or an airport or some other physical infrastructure? So subsequently, we took a look at the interconnected nature of these devices and we conducted a series of experiments that identified the capability by modifying settings and accessing control networks to actually take a digital protective circuit and turn it into a digital destructive circuit.

A simple explanation of what we did with Aurora it is like you are driving down the road at 60 miles an hour and you throw your

transmission in reverse, it is going to have a negative impact on that car to operate.

Ms. SCHAKOWSKY. Yes.

Mr. MCGURK. So that is really what we were trying to demonstrate. And then subsequently, once we identify the vulnerabilities, how do we put those protective measures in place, whether it is through equipment design and modification or in many cases it is just through procedural changes? So we look at low-cost or no-cost approach. From that point forward, the Department has conducted numerous equipment vulnerability assessments to not only identify inherent vulnerabilities in devices but to work with industry to develop those mitigation strategies and in some cases working with the manufacturers to physically modify the equipment so it is more secure.

Ms. SCHAKOWSKY. Thank you. My time has well expired. Thank you.

Mr. STEARNS. The gentleman from Louisiana, Mr. Scalise, recognized for 5 minutes.

Mr. SCALISE. Thank you, Mr. Chairman. If I could ask all the panelists first, I just want to get your opinion on if our critical networks are more vulnerable today than they were 5 years ago?

Ms. STEMPFLEY. So my opinion is they are not necessarily more vulnerable than they were 5 years ago. A great deal has happened over the last 5 years in terms of coordination, collaboration across the board. What I believe is that we are much more aware now than we were 5 years ago both of the role that they play in the environment. We are certainly more dependent on cybersecurity solutions and interdependent today, more aware of that, and there is a higher sophistication in the threat that exists today than did some time ago.

Mr. SCALISE. Mr. McGurk?

Mr. MCGURK. Thank you, sir. I would also agree that I believe it has been an evolutionary period. Perhaps in the past we were focusing more on information assurance as a method of achieving cybersecurity, but since then, we have recognized that since the physical and the virtual are all interconnected, we are taking a more direct approach towards cybersecurity. So there may be more reporting but there is more awareness as well.

Mr. WILSHUSEN. And I would also say that the threats to cyber critical infrastructures are increasing. They are evolving and growing and becoming more sophisticated. So those two raise the overall risk to those infrastructures. Our reviews have shown that where we have evaluated the security over specific systems that they are vulnerable and that numerous vulnerabilities exist because appropriate information security controls, which are well known, have not been implemented on a consistent basis throughout. So while there is greater awareness, there is also a greater threat I believe and also the vulnerabilities still remain.

Mr. SCALISE. Mr. Wilshusen, in your testimony, the GAO—and you listed here some GAO recommendations to enhance the protection of cyber-reliant critical infrastructure. Regarding these recommendations that you laid out, do you see that other agencies are looking at these or open to these and specifically with members of DHS that are here and, you know, I would like to get their take,

too, but what has been the reaction you have seen from the GAO report of these specific recommendations?

Mr. WILSHUSEN. Well, for most of our reports in this area, we have received largely concurrences with our recommendations, particularly from DHS. They have taken a number of actions to implement our recommendations and we will be following up with them to ensure that they are effectively implemented over time. In some cases, even when DHS non-concurred for the purposes of our report with the recommendation, they ultimately reversed themselves and decided to implement the recommendations. So I think there is awareness and concurrence for the most part of the agencies to implement our recommendations.

Mr. SCALISE. I will ask the same, Mr. McGurk and Ms. Stempfley, just both of those recommendations but also other tools that you think should be available.

Mr. MCGURK. I would like to add that in addition to the recommendations of GAO—and we do evaluate them not only from a technical standpoint but also from an implementation standpoint, and that is part of the challenge that we identified. In the critical infrastructure, the networks are so—in some cases—unique that you can't apply a particular standard or requirement that is identified by a recommendation and you may actually cause an interoperability challenge. So we do look at that from a technical standpoint and then we work with other standards-settings bodies such as NIST to identify those best practices and those requirements and then work with the private sector to ensure that we can actually implement that without causing an adverse impact or additional cost.

Mr. SCALISE. Ms. Stempfley?

Ms. STEMPFLEY. So we agree that the recommendations in the GAO report are ones that we focus a great deal of attention on and recognize that cyber is one of the high-risk items that GAO executes. We have a regular interaction with them around this particular activity, particularly given the consequences. We talked a great deal about consequences of malicious activity in this particular environment. We watch very closely that. And as we work through issues both in terms of owners and operators, execution and implementation of practices in their environment and come out as we are requested to come out and provide voluntary review of information and infrastructures and the owner/operators we are also able to identify how they are doing in terms of implementation and get information about what is generally accepted practices across the board.

Mr. SCALISE. Real quickly one final question before my time runs out. The Department of Defense's director of intelligence and counterintelligence has talked about supply chain integrity and, you know, they suggest that some equipment that we buy, hardware that we buy could be corrupted both hardware and software. And there are some things that they are looking at in that regard, and I wanted to get your take from Homeland Security or if GAO wants to chime in. Is that something that you all have looked at as well? Have you seen any problems there?

Ms. STEMPFLEY. So I believe I made an offer earlier to bring back an interagency review around supply chain. We appreciate that it

is important for us to look across the entire lifecycle of both equipment and of software development as well so that we can make sure that we have good practices in each of the steps of the lifecycle.

Mr. WILSHUSEN. And if I may chime in, we are currently evaluating the supply chain risk process at several agencies including DOD, DHS, Justice, Energy as part of our review over the supply chain risks for IT. We are assessing also the agencies' efforts to employ a risk-based approach to assessing supply chain risks.

Mr. SCALISE. Thank you, Mr. Chairman. I yield back.

Mr. STEARNS. Thank you.

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

Mr. GREEN. Thank you, Mr. Chairman.

And following up our colleague from Tennessee, Ms. Blackburn, you know, our committee has jurisdiction both over cybersecurity and healthcare, and so when we go through those screenings, could we at least maybe in our jurisdiction have a radiologist look at those so we can do those full body scans and it maybe save us on our imaging cost.

But I want to welcome our panel here. It has been a long hearing for you all and I thought we ought to laugh a little bit.

The GAO has long identified protecting the Federal Government's information system and Nation's cyber-critical structures. And Mr. Wilshusen, when did the GAO first identify cybersecurity as part of our high-risk series?

Mr. WILSHUSEN. That was back in 2003.

Mr. GREEN. OK. And you did your first major review of DHS cybersecurity efforts in 2005?

Mr. WILSHUSEN. That is right. That is when we assessed the Department's performance and actually implementing some 13 roles and responsibilities that it was responsible for.

Mr. GREEN. Have you seen improvements in the way that the Federal Government prepares for and addresses cyber threats since you have been reviewing DHS' program?

Mr. WILSHUSEN. We have seen progress at DHS in the way that it is addressing some of these areas. We also recognize that there is more that needs to be done, particularly with some of the sector's specific planning efforts, its cyber analysis and warning capabilities, as well as just as I mentioned earlier related to its private-public partnerships.

Mr. GREEN. OK. I understand in 2009 DHS launched the 24-hour DHS-led coordinated watch and warning system known as the National Cybersecurity Communications Integrations System. Mr. McGurk, what private-sector entities have current access to the resources of this facility?

Mr. MCGURK. Certainly, sir. Currently, we have a direct partnership with each of the 18 critical infrastructure and key resource sectors. Physically located on the watch floor today we have representatives from the energy sector, the financial services sector, the communications sector, IT sector, Multi-State ISAC. We are also finalizing agreements with chemical and others so they can be physically present on the watch floor. In addition, we recognize the unique capabilities of some of our other partners in the manufac-

turing and antivirus environment. And we are working with them to develop cooperative research and development agreements so that they can be physically present so that we can share data in real time.

Mr. GREEN. Last week there were reports emerged about a Department of Homeland Security report insider threat to utilities, and when you mentioned utilities were involved in it, do you have pretty well unanimous support or working relationship with our utilities in our country from investor-owned, municipal-owned co-ops like the TVA even? Is that pretty well uniform throughout the country?

Mr. MCGURK. Yes, sir. We have very direct connections with many of our private-sector partners. We have spent a lot of time developing cooperative agreements with—for instance, there is an organization that is made up of the 18 largest utilities in the United States and they have a Chief Information Security Officer Panel, which we interface with directly. I have personally briefed them on a number of occasions and provided input into those organizations so that they have a better cyber awareness.

Mr. GREEN. OK. I know the report was not released to the public and in the news story we talked about, we have a high confidence in our judgment that insiders and their actions pose a significant threat to infrastructure and information systems of U.S. facilities, and I understand, like I said, the report is not made public. I would like to ask some questions about insider threats to our utilities.

Ms. Stempfley, could utility facilities be targets for terrorists on the cyber side? We know physical targets.

Ms. STEMPFLEY. So I think you will find that the vulnerabilities that exist and are possible to be exploited exist in many places to include utilities across the board. That is one of the reasons why, as we have reiterated, we try to look at this from a common approach across the environment.

Mr. GREEN. I am aware in Texas and Houston we have mostly investor-owned utilities, our service provider center point, and I know they are doing some really great things, but does access to these sensitive facilities—mostly owned by the private companies—need to be closer guarded and carefully monitored to protect these threats?

Ms. STEMPFLEY. So best practice activities in the cyber security systems are ones of multiple layers of defense, which would include not just perimeter defense but internal architecture approaches that separate sensitive data from each other, rely on identity and other services. Those kinds of best practices, which are widely available, should be employed across the board.

Mr. GREEN. I know a news story last week described an insider sabotage in April in a water treatment plant in Arizona where a disgruntled employee took control of the control room to create a methane gas explosion. What is DHS doing to ensure that these type of insider sabotage, again, whether they are just one person or a plan, what is DHS doing to try and limit some of these insider cyber sabotage?

Ms. STEMPFLEY. As we have identified, we continue to provide the kinds of warning products, indicators of activities that might be necessary and the kinds of best practice guides for owners and

operators to employ. In your example, it would be up to that particular owner and operator to employ those practices.

Mr. GREEN. And Mr. Chairman, I would just like to ask one last thing.

And do you get pretty good cooperation throughout the country with the utilities?

Mr. MCGURK. Yes, sir, absolutely. We get a very close working relationship with utilities.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. We will quickly go for a second round. We don't have votes and so I welcome my colleagues if they wish to have a second round.

I would like to return to the Stuxnet issue if you don't mind, Mr. McGurk. If you can, just answer yes or no.

Do you know how many operators in the industrial controls infrastructure actually implemented DHS guidance on Stuxnet?

Mr. MCGURK. No, sir.

Mr. STEARNS. OK. How many U.S. companies use a type of Siemens industrial-controlled products that were the target of Stuxnet attacks?

Mr. MCGURK. A total number of companies? It is very difficult to quantify, sir, because we don't have this ability into all of their networks, but there were approximately 300 companies that had some combination of hardware and software.

Mr. STEARNS. So 300 U.S. companies?

Mr. MCGURK. Yes, sir.

Mr. STEARNS. Approximately. Good. Do you believe that if the U.S. companies implemented the DHS guidance on Stuxnet, they will be able to fend off a future attack from this software?

Mr. MCGURK. Yes, sir, from this particular piece of mal code.

Mr. STEARNS. In addition to this software, we have heard that there are other vulnerabilities identified in industrial-controlled systems, including a Beresford vulnerability or exploit. Does that ring a bell?

Mr. MCGURK. Yes, sir.

Mr. STEARNS. Um-hum. Given that Stuxnet's impact and the other vulnerabilities that exist, are you comfortable that our country's industrial control systems are secure from cyber attacks?

Mr. MCGURK. I think it is an evolving threat, sir, so we have to continue to move forward and not focus on the previous attacks.

Mr. STEARNS. Wasn't the Beresford attack developed by one researcher in about 2–1/2 months? That is our background. And what does that say about the safety of our system if someone could work with his laptop computer in 2–1/2 months, develop something that is vulnerable, and be used? Would you care to comment?

Mr. MCGURK. Yes, sir. What that really highlights is the fact that it is not necessarily attributed to the actor itself but it is the action and the vulnerabilities that we need to focus on. Because as you had mentioned in your opening statement and again when focusing on Stuxnet, it is not the capability of the actor that necessarily brings about the consequence. It is the actual vulnerability associated that is being exploited, and that is really where the Department is focusing much of its efforts.

Mr. STEARNS. OK. What step has DHS taken to prepare and defend against a Beresford type of attack to industrial control system and has this guidance or other direction been issued to the industry of the private sector? And I will ask you later. Go ahead, Mr. McGurk.

Mr. MCGURK. Sir, the Department has produced a number of specific actions and guidance associated with various types of cyber risk and cyber threats but again, not focusing on the actor or the activity but focusing on the vulnerability and the necessary methods to secure the networks. We actually will not only address that issue but maybe the next-generation issue that could occur.

Mr. STEARNS. Do you actually talk to these U.S. companies to see how they are implementing and doing this?

Mr. MCGURK. Yes, sir. In many cases, we are invited to actually do an onsite assessment associated with the vulnerabilities to see how they implement the mitigation plans.

Mr. STEARNS. Well, just approximately how many do you think you have assessed?

Mr. MCGURK. We have assessed approximately—this past year we did 53. The year before we did about 40. These are voluntary assessments. The year prior to that, another 30. So we have done over 100 voluntary assessments and incident response activities over the past 3 years.

Mr. STEARNS. Now, was that oriented towards the Stuxnet or was it also involved with the Beresford?

Mr. MCGURK. It is involved with all types of vulnerabilities, not just those two particular instances.

Mr. STEARNS. Mr. Wilshusen, do you mind commenting?

Mr. WILSHUSEN. Well, in our reviews we often also focus on the vulnerabilities of systems because that is what the agencies or the operators can control. They can't always control the threats that come their way, but they can control how well they protect their systems and protect against known vulnerabilities. And so that is one thing that we often look at. And at the systems that we examine at a detailed level, we typically find that they are vulnerable.

Mr. STEARNS. Ms. Stempfley, you had indicated in a question 5 years ago are we more vulnerable today than we were 5 years indicate, you seemed to indicate you didn't think so. And I guess the question is based upon what I have just given you some examples how a man in just 2–1/2 months could come up with something that can make our system vulnerable, I guess the question for each panelist, can you explain how the cyber threats you are seeing now are different from 2 or 3 or 5 years ago? And I will start with you, Ms. Stempfley?

Ms. STEMPFLEY. So the cyber threats now are certainly more sophisticated than they were several years ago. The threats are focused more on individuals and very specific activities. An example I have used is spear fishing is very targeted to an individual. I received an email not too long ago that appeared to be from my husband as a situation and it was about a topic about college payment activities, and that was identified and sent to me. And had I clicked on it, it may have been something that was malicious. That is an example of increased sophistication and increased focus that exists.

The number of vulnerabilities that have existed and the kind of model that you presented where a researcher identified a vulnerability and something that is already in existence, that vulnerability had been there from the beginning. It was just recently identified. And so the specific vulnerabilities have not increased in that scenario. We are just more aware of it now and more able to respond.

Our protective measures and protective guidance are about building these infrastructures in a way that reduces the exposure of those vulnerabilities and makes it less likely for threat actors to be able to be successful.

Mr. STEARNS. And Mr. McGurk?

Mr. MCGURK. Yes, sir. I would also agree that, you know, it is a matter of awareness and understanding the interconnected nature of the——

Mr. STEARNS. But you don't see the cybersecurity increasing in the last 5 years?

Mr. MCGURK. Do I see cybersecurity risk?

Mr. STEARNS. Threats increasing.

Mr. MCGURK. Threats, yes, sir, as a result of exploiting those vulnerabilities because of the sophistication and also the targeted nature. In the past we were talking about just basic data ex-filtration from a very broad audience. Now, we are seeing—in the RSA example that was mentioned earlier—very specific, targeted attacks against these aggregation centers.

Mr. WILSHUSEN. And I agree, and I think you will continue to see more blended types of attacks that exploit a number of different vulnerabilities in order to gain access to its target.

Mr. STEARNS. So you would agree that the cyber threats are more now than they were 5 years ago?

Mr. WILSHUSEN. And more sophisticated.

Mr. STEARNS. Let me just close by this question. I am not quite clear myself what this Beresford software does or did. Can you describe, Mr. McGurk, what it does? Do you know anything about it?

Mr. MCGURK. I don't have those specific details of the analysis in front of me today, sir, so I couldn't really comment on that.

Mr. STEARNS. Anybody?

Mr. WILSHUSEN. No.

Mr. STEARNS. OK. All right. My time has expired.

The gentlelady from Colorado.

Ms. DEGETTE. Thank you very much, Mr. Chairman.

First of all, I would like to ask unanimous consent to put Mr. Waxman's opening statement in the record.

Mr. STEARNS. By unanimous consent, so ordered.

[The prepared statement of Mr. Waxman follows:]

Opening Statement of Rep. Henry A. Waxman
Ranking Member, Committee on Energy and Commerce
Hearing on Cybersecurity: An Overview of Risks to Critical Infrastructure
Subcommittee on Oversight and Investigations
July 26, 2011

Today we will hear testimony from the Department of Homeland Security and Government Accountability Office regarding the ability of the United States to prevent and respond to cyber attacks. Securing cyberspace is critical to our national security, and I am glad that we are starting a series of hearings on the issue in this Congress.

Information systems connected to the Internet are integral to the operation of major components of our critical infrastructure. While this interconnectedness is essential to our economy, the vulnerabilities it creates pose serious challenges. Every day the Internet is under attack by hackers and others with malicious intent. In just the last five years, cyber attacks on federal agencies have skyrocketed.

A series of presidential directives under Presidents Bush and Obama have tasked the Department of Homeland Security with a key role in ensuring coordination among federal, state, local, and private sector parties in preventing and responding to cyber attacks. Today, I hope we will assess whether we are making real, measurable progress in protecting our nation from cyber attacks.

Last Congress, Democrats and Republicans worked together to craft legislation to protect the security of our electric grid. The result was a strong bill, and it passed the Committee by a vote of 49 to zero before passing the House by voice vote.

The Senate was not able to act, so we need to renew our legislative efforts. Recently, our Committee held a hearing on this bipartisan bill. I look forward to working with my colleagues to pass this crucial legislation. The Defense community has made it clear that the changes made by this bill are critical to our national security.

We then need to examine other sectors under our broad jurisdiction, including the telecommunications and health care industries. We need to assess whether the authorities of the Department of Homeland Security, the FCC, and other agencies are sufficient to provide the protection from cyber attacks that our nation needs.

As we undertake this review, we must ensure we put our national interest ahead of special interests. We did this when we reported the grid security bill last Congress over objections from utility companies.

But we failed when we considered the chemical security bill earlier this year. GAO, federal officials, and outside experts told us that our current laws have loopholes that exempt from regulation public water systems, water treatment plants, and any facility subject to regulation by the Nuclear Regulatory Commission. We should have closed these loopholes and strengthened other parts of our chemical security laws.

Yet when oil companies and chemical companies objected, we listened to them – not the experts – and passed a bill that fails to address these security vulnerabilities.

We need to work together – on a bipartisan basis – to make sure we protect our nation from the cyber attacks launched by our adversaries and criminal elements.

I hope that today's hearing and future hearings on cybersecurity within this Subcommittee will help guide our efforts. Our shared goal should be to develop initiatives to promote cybersecurity for our nation's critical infrastructure.

Ms. DEGETTE. Thank you.

So this is the perfect segue actually to just one question I had of clarification. We are all throwing around the words threat, vulnerability, and risk quite a bit today. And Mr. Wilshusen, I am wondering as we prepare for our subsequent hearings on these topics, you can just basically describe for us whether there is a difference between those three words and what the technical descriptions are.

Mr. WILSHUSEN. Sure. Yes. And there is a difference. A threat is basically any circumstance or event that can potentially cause harm to an organization's operations, assets, personnel, or whatever. A vulnerability is a weakness in the security controls that are over a system or network. There is actually a fourth component here before we get to risk, and that is impact. What is the impact that could occur should a threat, either a threat actor or an event occur, exploit a vulnerability? What is the impact that it could have? And then those three of those kind of equate to what risk is.

Ms. DEGETTE. Thank you. And are they all three things we should be concerned about?

Mr. WILSHUSEN. Yes, indeed. Absolutely. Threats are what you try to guard against. The vulnerabilities are what you try to prevent and minimize by taking corrective actions and implementing appropriate security controls. And you do that in such a manner that you minimize the impact should such a security incident occur. And so, yes, it is important to think of all of them.

Ms. DEGETTE. So you have heard both me and the chairman and other members of this subcommittee talk about this committee's jurisdiction. I am wondering if there is any particular sectors of our jurisdiction that you think we should look more closely at in subsequent hearings?

Mr. WILSHUSEN. I think in terms of from a cyber perspective, I think probably the key sectors would be energy, electricity, both nuclear and other just because of the interdependencies that they have with other sectors, IT, finance and banking, and also communications would be I think the four that are the most important just because of the interdependencies that they have with the other critical sectors.

Ms. DEGETTE. Great. Thank you.

Thank you very much, Mr. Chairman. I yield back.

Mr. STEARNS. I thank the gentlelady. I want to thank the witnesses for their participation, their coming here this morning.

The committee rules provide that members have 10 days to submit additional questions for the record, the witnesses. And with that, the subcommittee is adjourned.

[Whereupon, at 12:41 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Opening Statement of the Honorable Fred Upton
Chairman, Committee on Energy and Commerce
Cybersecurity: Overview of Risks to Critical Infrastructure
Tuesday, July 26

Thank you, Mr. Chairman, for convening this subcommittee's first hearing on cybersecurity and critical infrastructure in this Congress.

Over the last year, there have been a number of cyber incidents that have raised questions about the security of our critical infrastructure. Just last week, the Department of Homeland Security released a bulletin about utility security. In particular, this bulletin discussed the threats insiders may pose to infrastructures and information systems at these facilities.

This Committee has a strong history of conducting cyber and critical infrastructure-related oversight. In this Congress, and the last, we have worked to develop the GRID Act to address concerns about the security of the bulk power system. I believe this Act is an important and necessary step to shore up the security of the electric grid. I also believe we have a responsibility to take a look at other infrastructure sectors to ensure they are protected.

The Committee's jurisdiction touches half of the 18 critical infrastructures identified in a 2003 presidential directive: chemical, commercial facilities, communications, critical manufacturing, energy, healthcare, information technology, nuclear reactors, materials, and waste, and water. In the face of cyber threats that are both more frequent and more sophisticated, this committee is well-positioned to play an important role in any comprehensive cybersecurity legislation that moves through the House. Before we can do that, I think it makes sense for the Committee to get a better understanding of what the government and the private sector are doing to protect critical infrastructure from cyber threats, and what is working and what is not.

Protecting critical infrastructure is a complicated issue. We are talking about facilities and frameworks owned by private companies, and by federal, state, and local governments. They are interconnected — electricity powers water systems that cool nuclear reactors, for example. They are vulnerable to threats from a number of different sources, including nation-states, criminals, and hackers.

I look forward to hearing the perspectives of our expert witnesses about the safety of our critical infrastructures, and whether we are taking the right steps to protect them from cyber risks and threats.

○