REVIEWING THE FEDERAL CYBERSECURITY MISSION

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MARCH 10, 2009

Serial No. 111–5

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

51–633 PDF WASHINGTON : 2010

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

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

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

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

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

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

YVETTE D. CLARKE, New York, *Chairwoman*

LORETTA SANCHEZ, California
LAURA RICHARDSON, California
BEN RAY LUJÁN, New Mexico
MARY JO KILROY, Ohio
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DANIEL E. LUNGREN, California
PAUL C. BROUN, Georgia
STEVE AUSTRIA, Ohio
PETER T. KING, New York *(Ex Officio)*

JACOB OLCOTT, *Staff Director*
DR. CHRIS BECK, *Senior Advisor for Science and Technology*
DANIEL M. WILKINS, *Clerk*
COLEY O'BRIEN, *Minority Subcommittee Lead*

CONTENTS

REVIEWING THE FEDERAL CYBERSECURITY MISSION

Tuesday, March 10, 2009

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:53 p.m., in Room 311, Cannon House Office Building, Hon. Yvette D. Clarke [Chairwoman of the subcommittee], presiding.

Present: Representatives Clarke, Richardson, Luján, Kilroy, Thompson [ex officio], Lungren, Broun, and Austria.

Ms. CLARKE. The subcommittee will come to order. The subcommittee is meeting today to receive testimony on reviewing the Federal Cybersecurity Mission. I will begin by recognizing myself for an opening statement.

Good afternoon, and thank you to all the witnesses for appearing before us today. I am pleased to chair today's hearing, my first as Chair of the Emerging Threats, Cybersecurity and Science Technology Subcommittee. While there may be a number of new faces here on the dais, I can assure everyone that this subcommittee will continue to address many of the same issues from the 110th Congress. Over the next 2 years, we will continue our oversight over nuclear detection programs, radiological threats, public health threats, cybersecurity and the Science and Technology Directorate. I also look forward to working in the same bipartisan spirit that the previous Chairman and Ranking Member carried on their work.

Mr. Lungren, I know that you take this responsibility as seriously as I do, and I look forward to partnering with you over the next 2 years to ensure the safety and security of the American people, American businesses, American infrastructure and the American way of life.

Today's hearing will be the first of three cybersecurity hearings that the subcommittee will hold this month. It is easy to understand why this issue dominates our agenda. We rely on information technology in every aspect of our lives, from our electric grid, banking systems, military and Government functions, to our e-mail, Web browsers, and iTunes.

Interconnected computers and networks have led to amazing developments in our society. Increased productivity, knowledge, services, and revenues are all benefits generated by our modern networked world. But in our rush to network everything, few

stopped to consider the security ramifications of this new world we were creating. So we find ourselves in an extremely dangerous situation today. Too many vulnerabilities exist on too many critical networks which are exposed to too many skilled attackers who can inflict too many damages to our systems. Unfortunately, to this day, too few people are even aware of these dangers and and fewer still are doing anything about it. This committee will continue to sound the alarm bells, raise awareness of the problems we face, and hold those in charge accountable for their inaction.

This hearing comes at a critical moment in our Nation's approach to their cyber threat. There is no more significant threat to our national and economic security than that which we face in cyberspace. We, the United States, must do everything equally significant to meet this challenge.

We are approximately halfway through the National Security Council's 60-day interagency review of the Federal Cybersecurity Mission which began on February 16. The review is being conducted by Melissa Hathaway, senior director of the NSC, on orders from President Obama and the National Security Adviser. The goal for the review is to develop a strategic framework to ensure the U.S. Government's cybersecurity initiatives are appropriately integrated, resourced, and coordinated with Congress and the private sector. I commend the President for his vision in making cybersecurity a priority for his administration and for requesting this review.

Given this committee's leadership role in cybersecurity policy development, we look forward to working with Ms. Hathaway and her team. Thankfully, their review does not have to start from scratch. I encourage the review team to rely upon the extensive hearing record of this committee in the 110th Congress, and from the work that our witnesses have already undertaken in that area.

The CSIS Commission report and the many GAO reports which Mr. Powner's team have produced over the years contain dozens of outstanding recommendations that, if actually implemented, will improve our national security posture. That message bears repeating. The previous 2 decades have seen countless reports from America's thought leaders in cybersecurity, containing hundreds of recommendations about how to improve America's posture in cyberspace. What has been lacking is the courage and leadership to actually implement these recommendations.

Now is the time to act. To ensure our national and economic security, now is the time we must act. The U.S. Government must chart a new course to secure cyberspace. Maintaining the status quo will not be enough to keep America secure. Now is the time for the Government to stop planning and start acting.

There are three key issues that I believe this review must address.

The 60-day review. First, this review must call for a national strategy for cyberspace. The previous administration drafted a high-level national security strategy in 2002 that presented problems and possible solutions to some of the same cybersecurity issues that we face today. Unfortunately, that strategy stopped short of mandating security changes. Without teeth, the strategy was never implemented. We need a strategy that uses all of the tools of the U.S. power in a coordinated fashion, but more impor-

tantly, we need to hold our agencies accountable for implementing that strategy.

That leads me to my second requirement, leadership. A lack of high-level leadership on cybersecurity has cost our country dearly over the last several years. The review must clearly delineate roles and responsibilities of each agency involved in the governance of cybersecurity at the Federal level, including DSA, NSA, and DOD; but most importantly, it must describe how the White House will coordinate policy and budgets for each of these different responsibilities. The CSIS Commission recommended, and I fully support, an assistant to the President of Cyberspace Security in the Executive Office of the President, along with support staff to coordinate this effort.

Third, the review must address the many policy and legal shortfalls that exist in protecting our critical infrastructure from cyber attack. Unfortunately, critical infrastructure systems remain the area of greatest vulnerability. While the previous administration relied on a voluntary protection system throughout many of the 18 credible infrastructure sectors, I believe this administration should seek to use a combination of regulations and incentives to ensure that our electricity grid, including the Smart Grid, water facilities, financial systems, and other key infrastructures are properly secured. The framework of this approach should be addressed in the review.

To the witnesses appearing before us today, I thank you for being here. I welcome your thoughts on the issues I have just discussed, as well as your opinions on what an effective national cybersecurity review should look like.

I intend for this subcommittee, as well as the full committee, to continue to play a role in shaping our national security posture.

I would like to just take a moment to acknowledge that we have been joined by the Chairman of this committee, the full committee, Chairman Bennie Thompson. I think this amplifies the importance of today's hearing.

The Chair now recognizes the Ranking Member of the subcommittee, the gentleman from California, Mr. Lungren, for an opening statement.

Mr. LUNGREN. Thank you very much, Chairwoman Clark. Thank you for the bipartisan manner in which you have approached the organization of this subcommittee and the informal meetings that we have had. I am looking forward to working with you and with our colleagues who are here present and the others who are Members of this subcommittee, particularly our Chairman, Mr. Thompson, and our Ranking Member of the full committee, Mr. King.

We need in this Congress to address the many threats and challenges that face us and that are under the jurisdiction of this subcommittee. Cybersecurity is certainly one of, if not the most paramount challenge that we have, and I support your decision to highlight the cyber threat with this, our first official hearing.

When I chaired the subcommittee in the 109th Congress that had cyber, the issue of cybersecurity within its jurisdiction, I realized that our first challenge was educating our colleagues and the public on the seriousness of the growing cyber threat. After our

classified cyber threat briefing last week, it is clear that much, much more needs to be done.

In the words of today's witness, David Powner of GAO, our Nation is under cyber attack and our present strategy and its implementation have not been fully effective in mitigating the threat. Now, I don't believe that this is because people wanted this to be the case or that there was any conscious effort on the part of Members of Congress or previous administrations or people in the private sector. I just think it is a point of fact that what you can't see, can't feel, can't hear, can't touch, sometimes is not what you pay attention to. Cybersecurity, the cyber world which is so important to us, is embedded in so much of what we do but we don't see it.

I use the old analogy of the refrigerator. I open the refrigerator, and all I want is cold milk. I really don't care how it works. We have that attitude toward the cyber world that is embedded in everything that we do. But we can't have that attitude. I believe it is particularly true regarding our information infrastructure, which includes our telecommunications and computer networks and systems and the data they contain. Information technology and computer networks increase information sharing and collaboration, which does a tremendous thing: It raises our productivity, lowers ours costs and improves performance. Would that the rest of our economy could do as well.

However, the rapid growth of the internet and our interconnected computer systems and its networks have, as you so rightly said, made us increasingly vulnerable to things such as cyber crime, cyber espionage, and cyber terrorism. I fully agree with the central finding of the CSIS Commission's report that cybersecurity is one of the most important security challenges this Nation faces. U.S. cyberspace should be declared a vital national asset, perhaps even a critical national asset. This would help the Federal Government marshal its resources and implement a Comprehensive National Cybersecurity Strategy.

I have felt for some time that we are playing catch-up in detecting and defending against the increasing number and sophistication of today's cyber threats, whether they are of the mischievous nature, of the organized crime nature, of the nation-state nature. I agree we need a national cybersecurity strategy, understanding that cyberspace can't be secured by Government alone, and that is a very important point that we have to stress. However, the Government does need to reorganize and focus its national cyber efforts if we hope to defeat the new cyber threats.

I would also suggest we need a true public/private cybersecurity partnership based on trust and cooperation to protect against this new cyber threat. The private sector, let's make it clear, designs, deploys and maintains much of the Nation's critical infrastructure. Therefore, we must honor their experience, their expertise and their ingenuity—that is, that which is found in the private sector—into a trusted partnership with Government, a partnership where both sides benefit and therefore are eager to cooperate and share information. It just seems to me that in many cases we should be setting certain standards or goals but not setting the means to get there because the cyber world moves so fast, we really can't catch up with this. Government, by its very nature, moves more slowly.

I don't want anything that we do to depress the creativity of the private sector. Therein lies our greatest opportunity to protect ourselves.

I believe the CSIS report's recommendation to create three new public/private groups designed to foster better trust and cooperation on cyber issues is the right approach. They would be a new Presidential advisory committee that connects the White House to the important private-sector cyberspace entities; a national town hall organization that provides dialog for education and discussion; and a new cyber operational organization.

The Bush administration recognized the growing threat on our national security from cyberspace, proposed a Comprehensive National Cybersecurity Initiative in 2008. The CSIS Commission came to a similar conclusion in their December report, "Securing Cyberspace for the 44th President," stating only a Comprehensive National Security Strategy that embraces both domestic and international aspects of cybersecurity will make us more secure. Well said.

Everyone seems to agree that we need to do more, so I am anxious to hear the testimony of our expert witnesses today to help us on that journey so that we may do that which needs to be done to meet this 21st century threat.

Once again I thank you, Madam Chairwoman, for the time.

Ms. CLARKE. The Chairwoman now recognizes the Chairman of the full Committee on Homeland Security, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you very much, Madam Chairwoman.

Good afternoon. I believe this is the ninth oversight hearing the Homeland Security Committee has held on Federal cybersecurity issues since the beginning of the 110th Congress, and I thank you, Madam Chairwoman, for continuing our oversight efforts. This is a particularly timely hearing, given the recent resignation of Mr. Beckstrom as director of the National Cybersecurity Center.

Some of our biggest challenges in the Federal cybersecurity, reported by dozens of independent observers, including GAO and CSIS, have come as a result of ineffective leadership, unclear organizational structure and poorly defined roles and responsibilities from agencies and private sector. This is why I, along with many of my colleagues, were very optimistic when Mr. Beckstrom was brought on to lead the National Cybersecurity Center. He has expertise in organizational structure. He has worked extensively in the private sector. But Mr. Beckstrom did not have experience in working miracles, and that is the unfortunate position that the previous administration put him in. Without clear authority or budget, he was placed in a no-win situation.

In his resignation letter, Mr. Beckstrom candidly described the control that is wielded by NSA over the cybersecurity mission today. This parallels the thoughts of some of our witnesses here today.

I don't disagree with the public statements made recently by the DNI, who said that the NSA houses most of the cyber talent in the Federal Government. But I don't think the answer to our problems in cyberspace comes from giving control of the entire Federal Cybersecurity Mission to NSA. I want to clearly state that this com-

mittee believes that there should be a creditable civilian government cybersecurity capability that interfaces with, but is not controlled by the NSA. According to GAO, DHS has not proven itself up to the challenge yet. From our work with DHS through the years, I don't disagree, but there are pockets within DHS showing signs of improvement. US–CERT and the controlled security system program are two of these programs that I believe are demonstrating progress.

I hope the administration can strike the balance between civilian and military cybersecurity capabilities. We here in Congress are looking toward this administration for leadership on this critical issue. I share the Chair's optimism about the President's commitment to cybersecurity, and I hope that, at the end of the 60-day review, we here in Congress will have a clear understanding of the President's vision for cybersecurity.

I yield back the balance of my time, Madam Chairwoman.

Ms. CLARKE. Other Members of the subcommittee are reminded that under the committee rules, opening statements may be submitted for the record.

I welcome our distinguished panel of witnesses. Our first witness is Dave Powner, director for information technology management issues at the Government Accountability Office. Mr. Powner and his team have produced a number of outstanding reports for this subcommittee throughout the last several years, and we are pleased to welcome him back.

Our second witness is Scott Charney, corporate vice president of Microsoft's trustworthy computing group. Prior to Microsoft, Mr. Charney was a principal for PriceWaterhouseCoopers, where he led the firm's cyber crime prevention and response practice. Mr. Charney also served as chief of the computer crime and intellectual property section in the criminal division of the U.S. Department of Justice. Mr. Charney was also co-chair of the CSIS Commission on Cybersecurity. Welcome.

Our third witness is Mr. Amit Yoran, chairman and chief executive officer of NetWitness Corporation, a leading provider of network security products. Prior to NetWitness, he was director of the national cybersecurity division at the Department of Homeland Security. He was also chief executive officer and advisor to Incutel, the venture capital arm of the CIA. Mr. Yoran is a member of the CSIS Cybersecurity Commission.

Our fourth witness is Mary Ann Davidson, the chief secretary—excuse me—the Chief Security Officer at Oracle Corporation, where she is responsible for Oracle product security, as well as security evaluations and assessments. Ms. Davidson represents Oracle on the Information Technology ISAC. She has served on the Defense Science Board and is a member of the CSIS Cybersecurity Commission. Welcome, Ms. Davidson. Nothing against the secretary, but you are chief security officer.

Our fifth witness is Jim Lewis, the director of the Center for Strategic and International Studies and Technology and Public Policy Program. He is also program manager for the CSIS Commission on Cybersecurity for the 44th Presidency. Mr. Lewis has also been a regular witness before this subcommittee, so welcome to you also.

Without objection, the witnesses' full statements will be inserted into the record.

I now ask each witness to summarize his or her statement for 5 minutes, beginning with Mr. Powner.

STATEMENT OF DAVID POWNER, DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. POWNER. Madam Chairwoman, Chairman Thompson, Ranking Member Lungren, Members of the subcommittee, thank you for inviting us to testify on cybersecurity recommendations for the new administration. Over the past several years, our work for the subcommittee has highlighted many areas requiring better leadership and management of our Nation's cyber-critical infrastructure, including improving cybersecurity of control systems, strengthening our ability to respond to internet disruptions, bolstering cyber analysis, and warning capabilities and addressing cyber crime.

This afternoon I will provide a progress report of our on-going work for you, Madam Chairwoman, looking at improvements to our Nation's cybersecurity strategy. Specifically, we held panel discussions with nationally recognized experts and these discussions, coupled with GAO's extensive work in this area, have resulted in 12 specific recommendations for the new administration to improve the approach to protecting both Government systems and our Nation's cyber-critical infrastructures. I will now briefly discuss each of the 12.

No. 1, develop a national strategy that clearly articulates strategic objectives and priorities and provides a means for enforcing action and accountability. The current strategy does not do this, nor does it contain requirements to hold responsible organizations accountable.

No. 2, establish a White House office responsible and accountable for leading and overseeing the National Cybersecurity Policy. Currently, DHS is our national security focal point, and they have not delivered on this responsibility.

No. 3, establish a governance structure for strategy implementation. Create a governing body, similar to a board of directors, responsible for reporting and measuring on the strategic priorities. This body should be led by senior executives from key Federal agencies, as well as key sectors. It should be noted that our experts stress that not all Federal agencies and sectors are key cyber players.

No. 4, acknowledge we are in a cyber war with criminal and adversarial nations. Publicize the severity of prior attacks and raise awareness that we are constantly under attack.

No. 5, create or designate an accountable operational cybersecurity organization. White House-led is not the silver bullet, and DHS has a troubled reputation to overcome. Despite tremendous capability, there are concerns about this being an intelligence organization, because a secretive culture runs counter to the need to partner with the private sector. Our experts suggested a cyber defense organization. Clearly, there was no consensus on where this organization should reside, and this will be a tough policy question

whether the best approach is to create another organization and how.

No. 6, focus less on creating plans and more on prioritizing, assessing and securing cyber assets. We have created many plans that largely go unused. We need to create a prioritized list of our Nation's cyber assets and work toward securing them.

No. 7, bolster public/private partnerships by providing more incentives for private sector participation.

No. 8, focus greater attention on the global aspects of cyberspace. We should work toward an international global cyber strategy and use international agreements to focus cybersecurity issues and thwart cyber crime, like the Council of Europe's cyber crime convention.

No. 9, modernize our legal framework to better address cyber criminals. Domestic and international law is outdated and it needs to be revised to make it easier to catch and prosecute criminals.

No. 10, better coordinate Government and private sector cyber R&D. Cyber R&D is underfunded and not coordinated.

No. 11, increase the number of skilled cyber professionals, including criminal investigators. Experts suggested that the cybersecurity discipline should be a profession that is licensed.

No. 12, make the Federal Government a model for cybersecurity. The CNCI initiative is a good first step, but the Federal Government has much room for improvement.

In summary, Madam Chairwoman, many large cybersecurity policy questions loom for the Obama administration and the Congress. GAO, CSIS and our expert panel recommendations need to be strongly considered as the game plan is defined over the next several months to provide a more secure cyber America.

This concludes my statement, and I look forward to your questions.

[The statement of Mr. Powner follows:]

PREPARED STATEMENT OF DAVID POWNER

MARCH 10, 2009

GAO HIGHLIGHTS

Highlights of GAO–09–432T, a testimony to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

Pervasive and sustained computer-based (cyber) attacks against Federal and private-sector infrastructures pose a potentially devastating impact to systems and operations and the critical infrastructures that they support. To address these threats, President Bush issued a 2003 national strategy and related policy directives aimed at improving cybersecurity Nation-wide. Congress and the Executive branch, including the new administration, have subsequently taken actions to examine the adequacy of the strategy and identify areas for improvement. Nevertheless, GAO has identified this area as high-risk and has reported on needed improvements in implementing the national cybersecurity strategy.

In this testimony, you asked GAO to summarize: (1) Key reports and recommendations on the national cybersecurity strategy, and (2) the views of experts on how to strengthen the strategy. In doing so, GAO relied on its previous reports related to the strategy and conducted panel discussions with key cybersecurity experts to solicit their views on areas for improvement.

What GAO Recommends

GAO has previously made about 30 recommendations, mostly directed at DHS, to improve our Nation's cybersecurity strategy efforts. DHS in large part has concurred with GAO's recommendations and, in many cases, has actions planned and under way to implement them.

NATIONAL CYBERSECURITY STRATEGY.—KEY IMPROVEMENTS ARE NEEDED TO STRENGTHEN THE NATION'S POSTURE

What GAO Found

Over the last several years, GAO has consistently reported that the Department of Homeland Security (DHS) has yet to fully satisfy its responsibilities designated by the national cybersecurity strategy. To address these shortfalls, GAO has made about 30 recommendations in key cybersecurity areas including the 5 listed in the table below. While DHS has since developed and implemented certain capabilities to satisfy aspects of its cybersecurity responsibilities, it still has not fully satisfied the recommendations, and thus further action needs to be taken to fully address these areas.

TABLE 1.—KEY CYBERSECURITY AREAS IDENTIFIED BY GAO AS NEEDING FURTHER ACTION

Item No.	
1.	Bolstering cyber analysis and warning capabilities.
2.	Completing actions identified during cyber exercises.
3.	Improving cybersecurity of infrastructure control systems.
4.	Strengthening DHS's ability to help recover from internet disruptions.
5.	Addressing cybercrime.

Source: GAO analysis of prior GAO reports.

In discussing the areas addressed by GAO's recommendations as well as other critical aspects of the strategy, GAO's panel of cybersecurity experts identified 12 key areas requiring improvement (see table below). GAO found these to be largely consistent with its reports and its extensive research and experience in the area.

TABLE 2.—KEY STRATEGY IMPROVEMENTS IDENTIFIED BY CYBERSECURITY EXPERTS

Item No.	
1.	Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2.	Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3.	Establish a governance structure for strategy implementation.
4.	Publicize and raise awareness about the seriousness of the cybersecurity problem.
5.	Create an accountable, operational cybersecurity organization.
6.	Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7.	Bolster public/private partnerships through an improved value proposition and use of incentives.
8.	Focus greater attention on addressing the global aspects of cyberspace.
9.	Improve law enforcement efforts to address malicious activities in cyberspace.
10.	Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate Government and private sector efforts.
11.	Increase the cadre of cybersecurity professionals.
12.	Make the Federal Government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

Until GAO's recommendations are fully addressed and the above improvements are considered, our Nation's Federal and private-sector infrastructure systems remain at risk of not being adequately protected. Consequently, in addition to fully implementing GAO's recommendations, it is essential that the improvements be considered by the new administration as it begins to make decisions on our Nation's cybersecurity strategy.

Madam Chair and Members of the subcommittee: Thank you for the opportunity to join in today's hearing to discuss efforts to protect our Nation from cybersecurity threats. Pervasive and sustained computer-based (cyber) attacks against the United States and others continue to pose a potentially devastating impact to systems and operations and the critical infrastructures that they support. To address these threats, President Bush issued a 2003 national strategy and related policy directives aimed at improving cybersecurity Nation-wide, including both Government systems and those cyber critical infrastructures owned and operated by the private sector.[1]

Because the threats have persisted and grown, a commission—commonly referred to as the Commission on Cybersecurity for the 44th Presidency and chaired by two congressmen and industry officials—was established in August 2007 to examine the adequacy of the strategy and identify areas for improvement.[2] At about the same time, the Bush administration began to implement a series of initiatives aimed primarily at improving cybersecurity within the Federal Government. More recently, in February 2009, President Obama initiated a review of the Government's overall cybersecurity strategy and supporting activities.

Today, as requested, I will discuss: (1) Our reports, containing about 30 recommendations, on the national cybersecurity strategy and related efforts, and (2) the results of expert panels we convened to discuss how to strengthen the strategy and our Nation's cybersecurity posture. In preparing for this testimony, we relied on our previous reports on Federal efforts to fulfill national cybersecurity responsibilities. These reports contain detailed overviews of the scope and methodology we used. We also obtained the views of nationally recognized cybersecurity experts by means of two panel discussions on the effectiveness of the current national cybersecurity strategy and recommendations for improvement. In summarizing the panel discussions, we provided all panel members an opportunity to comment on our written summaries, and their comments were incorporated as appropriate. The panelists' names and titles are in appendix I. We conducted our work in support of this testimony during February and March 2009, in the Washington, DC, area. The work on which this testimony is based was performed in accordance with generally accepted Government auditing standards.

BACKGROUND

Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. For example, in February 2009, the director of national intelligence testified that foreign nations and criminals have targeted Government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups have expressed a desire to use cyber attacks as a means to target the United States.[3] The director also discussed that in August 2008, the national government of Georgia's Web sites were disabled during hostilities with Russia, which hindered the Government's ability to communicate its perspective about the conflict.

The Federal Government has developed a strategy to address such cyber threats. Specifically, President Bush issued the 2003 *National Strategy to Secure Cyber-*

---

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

[2] The commission was created by the Center for Strategic and International Studies (CSIS), a bipartisan, nonprofit organization that, among other things, provides strategic insights and policy solutions to decision-makers. Entitled the CSIS Commission on Cybersecurity for the 44th Presidency, the body was co-chaired by Representative James Langevin, Representative Michael McCaul, Scott Charney (Microsoft), and Lt. General Harry Raduege, USAF (Ret).

[3] Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

space[4] and related policy directives, such as Homeland Security Presidential Directive 7,[5] that specify key elements of how the Nation is to secure key computer-based systems, including both Government systems and those that support critical infrastructures owned and operated by the private sector. The strategy and related policies also establish the Department of Homeland Security (DHS) as the focal point for cyber CIP and assign the Department multiple leadership roles and responsibilities in this area. They include: (1) Developing a comprehensive national plan for CIP, including cybersecurity; (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;[6] and (5) strengthening international cyberspace security. In addition, the strategy and related policy direct DHS and other relevant stakeholders to use risk management principles to prioritize protection activities within and across the 18 critical infrastructure sectors in an integrated, coordinated fashion.

Because the threats have persisted and grown, President Bush in January 2008 began to implement a series of initiatives—commonly referred to as the Comprehensive National Cybersecurity Initiative (CNCI)—aimed primarily at improving DHS and other Federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[7] While these initiatives have not been made public, the Director of National Intelligence stated that they include defensive, offensive, research and development, and counterintelligence efforts, as well as a project to improve public/private partnerships.[8] Subsequently, in December 2008, the Commission on Cybersecurity for the 44th Presidency reported, among other things, that the failure to protect cyberspace was an urgent national security problem and made 25 recommendations aimed at addressing shortfalls with the strategy and its implementation.[9] Since then, President Obama (in February 2009) initiated a review of the cybersecurity strategy and supporting activities. The review is scheduled to be completed in April 2009.

GAO HAS MADE RECOMMENDATIONS TO ADDRESS SHORTFALLS WITH KEY ASPECTS OF NATIONAL CYBERSECURITY STRATEGY AND ITS IMPLEMENTATION

Over the last several years we have reported on our Nation's efforts to fulfill essential aspects of its cybersecurity strategy. In particular, we have reported consistently since 2005 that DHS has yet to fully satisfy its cybersecurity responsibilities designated by the strategy. To address these shortfalls, we have made about 30 recommendations in key cybersecurity areas including the 5 listed in Table 1. DHS has since developed and implemented certain capabilities to satisfy aspects of its cybersecurity responsibilities, but the Department still has not fully satisfied our recommendations, and thus further action needs to be taken to address these areas.

TABLE 1.—KEY CYBERSECURITY AREAS IDENTIFIED BY GAO AS NEEDING FURTHER ACTION

Item No.	
1.	Bolstering cyber analysis and warning capabilities.
2.	Completing actions identified during cyber exercises.
3.	Improving cybersecurity of infrastructure control systems.
4.	Strengthening DHS's ability to help recover from internet disruptions.

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

[5] The White House, Homeland Security Presidential Directive 7 (Washington, DC: Dec. 17, 2003).

[6] Control systems are computer-based systems that perform vital functions in many of our Nation's critical infrastructures, including electric power generation, transmission, and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing.

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

[8] Statement of the director of national intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

[9] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, DC: December 2008).

TABLE 1.—KEY CYBERSECURITY AREAS IDENTIFIED BY GAO AS NEEDING FURTHER ACTION—Continued

Item No.	
5.	Addressing cybercrime.

Source: GAO analysis of prior GAO reports.

In July 2008, we reported [10] that DHS's United States Computer Emergency Readiness Team (US–CERT) did not fully address 15 key cyber analysis and warning attributes related to: (1) Monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, US–CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. As a result, we recommended that the Department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability as envisioned in the national strategy. DHS agreed in large part with our recommendations.

In September 2008, we reported [11] that since conducting a major cyber attack exercise, called Cyber Storm, DHS had demonstrated progress in addressing eight lessons it had learned from these efforts. However, its actions to address the lessons had not been fully implemented. Specifically, while it had completed 42 of the 66 activities identified, the Department had identified 16 activities as on-going and 7 as planned for the future.[12] Consequently, we recommended that DHS schedule and complete all of the corrective activities identified in order to strengthen coordination between public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation. To date, DHS has continued to make progress in completing some identified activities but has yet to do so for others.

In a September 2007 report and an October 2007 testimony, we reported [13] that consistent with the national strategy requirement to identify and reduce threats and vulnerabilities, DHS was sponsoring multiple control systems security initiatives, including an effort to improve control systems cybersecurity using vulnerability evaluation and response tools. However, DHS had not established a strategy to coordinate the various control systems activities across Federal agencies and the private sector, and it did not effectively share information on control system vulnerabilities with the public and private sectors. Accordingly, we recommended that DHS develop a strategy to guide efforts for securing control systems and establish a rapid and secure process for sharing sensitive control system vulnerability information. DHS recently began developing a strategy and a process to share sensitive information.

We reported and later testified [14] in 2006 that the Department had begun a variety of initiatives to fulfill its responsibility, as called for by the national strategy, for developing an integrated public/private plan for Internet recovery. However, we determined that these efforts were not comprehensive or complete. As such, we recommended that DHS implement nine actions to improve the Department's ability to facilitate public/private efforts to recover the internet in case of a major disruption. In October 2007, we testified [15] that the Department had made progress in implementing our recommendations; however, seven of the nine have not been com-

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

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

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

[13] GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,* GAO–07–1036 (Washington, DC: Sept. 10, 2007) and *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,* GAO–08–119T (Washington, DC: Oct. 17, 2007).

[14] GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan,* GAO–06–672 (Washington, DC: June 16, 2006) and *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan,* GAO–06–863T (Washington, DC: July 28, 2006).

[15] GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan,* GAO–08–212T (Washington, DC: Oct. 23, 2007).

pleted. To date, an integrated public/private plan for internet recovery does not exist.

In 2007, we reported [16] that public and private entities [17] faced a number of challenges in addressing cybercrime, including ensuring adequate analytical and technical capabilities for law enforcement and conducting investigations and prosecuting cybercrimes that cross national and State borders.

CYBERSECURITY EXPERTS HIGHLIGHTED KEY IMPROVEMENTS NEEDED TO STRENGTHEN THE NATION'S CYBERSECURITY POSTURE

In addition to our recommendations on improving key aspects of the national cybersecurity strategy and its implementation, we also obtained the views of experts (by means of panel discussions) on these and other critical aspects of the strategy, including areas for improvement. The experts, who included former Federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. These improvements are in large part consistent with our above-mentioned reports and extensive research and experience in this area. They include:

1. Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.—The strategy should, among other things: (1) Include well-defined strategic objectives, (2) provide understandable goals for the Government and the private sector (end game), (3) articulate cyber priorities among the objectives, (4) provide a vision of what secure cyberspace should be in the future, (5) seek to integrate Federal Government capabilities, (6) establish metrics to gauge whether progress is being made against the strategy, and (7) provide an effective means for enforcing action and accountability when there are progress shortfalls. According to expert panel members, the CNCI provides a good set of tactical initiatives focused on improving primarily Federal cybersecurity; however, it does not provide strategic objectives, goals, and priorities for the Nation as a whole.

2. Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.—The strategy makes DHS the focal point for cybersecurity; however, according to expert panel members, DHS has not met expectations and has not provided the high-level leadership needed to raise cybersecurity to a national focus. Accordingly, panelists stated that to be successful and to send the message to the Nation and cyber critical infrastructure owners that cybersecurity is a priority, this leadership role needs to be elevated to the White House. In addition, to be effective, the office must have, among other things, commensurate authority—for example, over budgets and resources—to implement and employ appropriate incentives to encourage action.

3. Establish a governance structure for strategy implementation.—The strategy establishes a public/private partnership governance structure that includes 18 critical infrastructure sectors, corresponding Government and sector coordinating councils, and cross-sector councils. However, according to panelists, this structure is Government-centric and largely relies on personal relationships to instill trust to share information and take action. In addition, although all sectors are not of equal importance in regard to their cyber assets and functions, the structure treats all sectors and all critical cyber assets and functions equally. To ensure effective strategy implementation, experts stated that the partnership structure should include a committee of senior government representatives (for example, the Departments of Defense, Homeland Security, Justice, State, and the Treasury and the White House) and private sector leaders representing the most critical cyber assets and functions. Expert panel members also suggested that this committee's responsibilities should include measuring and periodically reporting on progress in achieving the goals, objectives, and strategic priorities established in the national strategy and building consensus to hold involved parties accountable when there are progress shortfalls.

4. Publicize and raise awareness about the seriousness of the cybersecurity problem.—Although the strategy establishes cyberspace security awareness as a priority, experts stated that many national leaders in business and Government, including in Congress, who can invest resources to address cybersecurity problems are generally not aware of the severity of the risks to national and economic security posed by the inadequacy of our Nation's cybersecurity posture and the associated intrusions made more likely by that posture. Expert panel members suggested that an

---

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

[17] These public and private entities include the Departments of Justice, Homeland Security, and Defense, and the Federal Trade Commission, internet security providers and software developers.

aggressive awareness campaign is needed to raise the level of knowledge of leaders and the general populace that our Nation is constantly under cyber attack.

5. Create an accountable, operational cybersecurity organization.—DHS established the National Cyber Security Division (within the Office of Cybersecurity and Communications) to be responsible for leading national day-to-day cybersecurity efforts; however, according to panelists, this has not enabled DHS to become the national focal point as envisioned. Panel members stated that currently, DOD and other organizations within the intelligence community that have significant resources and capabilities have come to dominate Federal efforts. They told us that there also needs to be an independent cybersecurity organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, military, intelligence community, and the Nation's international allies to address incidents against the Nation's critical cyber systems and functions. However, there was not consensus among our expert panel members regarding where this organization should reside.

6. Focus more actions on prioritizing assets and functions, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.—The strategy recommends actions to identify critical cyber assets and functions, but panelists stated that efforts to identify which cyber assets and functions are most critical to the Nation have been insufficient. According to panel members, inclusion in cyber critical infrastructure protection efforts and lists of critical assets are currently based on the willingness of the person or entity responsible for the asset or function to participate and not on substantiated technical evidence. In addition, the current strategy establishes vulnerability reduction as a key priority; however, according to panelists, efforts to identify and mitigate known vulnerabilities have been insufficient. They stated that greater efforts should be taken to identify and eliminate common vulnerabilities and that there are techniques available that should be used to assess vulnerabilities in the most critical, prioritized cyber assets and functions.

7. Bolster public/private partnerships through an improved value proposition and use of incentives.—While the strategy encourages action by owners and operators of critical cyber assets and functions, panel members stated that there are not adequate economic and other incentives (i.e., a value proposition) for greater investment and partnering in cybersecurity. Accordingly, panelists stated that the Federal Government should provide valued services (such as offering useful threat or analysis and warning information) or incentives (such as grants or tax reductions) to encourage action by and effective partnerships with the private sector. They also suggested that public and private sector entities use means such as cost-benefit analyses to ensure the efficient use of limited cybersecurity-related resources.

8. Focus greater attention on addressing the global aspects of cyberspace.—The strategy includes recommendations to address the international aspects of cyberspace but, according to panelists, the United States is not addressing global issues impacting how cyberspace is governed and controlled. They added that, while other nations are actively involved in developing treaties, establishing standards, and pursuing international agreements (such as on privacy), the United States is not aggressively working in a coordinated manner to ensure that international agreements are consistent with U.S. practice and that they address cybersecurity and cybercrime considerations. Panel members stated that the United States should pursue a more coordinated, aggressive approach so that there is a level playing field globally for U.S. corporations and enhanced cooperation among government agencies, including law enforcement. In addition, a panelist stated that the United States should work towards building consensus on a global cyber strategy.

9. Improve law enforcement efforts to address malicious activities in cyberspace.—The strategy calls for improving investigative coordination domestically and internationally and promoting a common agreement among nations on addressing cybercrime. According to a panelist, some improvements in domestic law have been made (e.g., enactment of the PROTECT Our Children Act of 2008), but implementation of this act is a work in process due to its recent passage. Panel members also stated that current domestic and international law enforcement efforts, including activities, procedures, methods, and laws are too outdated and outmoded to adequately address the speed, sophistication, and techniques of individuals and groups, such as criminals, terrorists, and adversarial foreign nations with malicious intent. An improved law enforcement is essential to more effectively catch and prosecute malicious individuals and groups and, with stricter penalties, deter malicious behavior.

10. Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate Government and private sector efforts.—While the strategy recommends actions to develop a research and development

agenda and coordinate efforts between the Government and private sectors, experts stated that the United States is not adequately focusing and funding research and development efforts to address cybersecurity or to develop the next generation of cyberspace to include effective security capabilities. In addition, the research and development efforts currently underway are not being well coordinated between Government and the private sector.

11. Increase the cadre of cybersecurity professionals.—The strategy includes efforts to increase the number and skills of cybersecurity professionals but, according to panelists, the results have not created sufficient numbers of professionals, including information security specialists and cybercrime investigators. Expert panel members stated that actions to increase the number professionals with adequate cybersecurity skills should include: (1) Enhancing existing scholarship programs (e.g., Scholarship for Service) and (2) making the cybersecurity discipline a profession through testing and licensing.

12. Make the Federal Government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.—The strategy establishes securing the Government's cyberspace as a key priority and advocates using Federal acquisition to accomplish this goal. Although the Federal Government has taken steps to improve the cybersecurity of agencies (e.g., beginning to implement the CNCI initiatives), panelists stated that it still is not a model for cybersecurity. Further, they said the Federal Government has not made changes in its acquisition function and the training of Government officials in a manner that effectively improves the cybersecurity capabilities of products and services purchased and used by Federal agencies.

In summary, our Nation is under cyber attack, and the present strategy and its implementation have not been fully effective in mitigating the threat. This is due in part to the fact that there are further actions needed by DHS to address key cybersecurity areas, including fully addressing our recommendations. In addition, nationally recognized experts have identified improvements aimed at strengthening the strategy and in turn, our cybersecurity posture. Key improvements include developing a national strategy that clearly articulates strategic objectives, goals, and priorities; establishing White House leadership; improving governance; and creating a capable and respected operational lead organization. Until the recommendations are fully addressed and these improvements are considered, our Nation's most critical Federal and private sector infrastructure systems remain at unnecessary risk to attack from our adversaries. Consequently, in addition to fully implementing our recommendations, it is essential that the Obama administration consider these improvements as it reviews our Nation's cybersecurity strategy and begins to make decisions on moving forward.

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

If you have any questions on matters discussed in this testimony, please contact me. Other key contributors to this testimony include Bradley Becker, Camille Chaires, Michael Gilmore, Nancy Glover, Kush Malhotra, Gary Mountjoy, Lee McCracken, and Andrew Stavisky.

Ms. CLARKE. Thank you very much.

Our next witness, I now recognize Mr. Charney to summarize his statement for 5 minutes.

STATEMENT OF SCOTT CHARNEY, VICE PRESIDENT, TRUSTWORTHY COMPUTING, MICROSOFT

Mr. CHARNEY. Chairwoman Clark, Ranking Member Lungren, Mr. Thompson and Members of the subcommittee, thank you for the opportunity to appear today to provide a perspective on reviewing the Federal Cybersecurity Mission. As you know, I served as one of four co-chairs of the CSIS Commission on Cybersecurity for the 44th Presidency with Representatives Jim Langevin of Rhode Island and Michael McCaul of Texas and General Harry Raduege.

I will address four themes that cross many of the recommendations made in the Commission's report.

First, we have an immediate need for a comprehensive White House Coordinated National Strategy for Cyber Space Security.

Second, we need to to evolve and focus the public/private partnership model.

Third, we should consider a new regulatory model designed to ensure that greater regulation, if enacted, protects innovation while providing appropriate Government oversight of cybersecurity issues.

Fourth, the internet needs an appropriately deployed identity metasystem, if we are to make the internet dramatically more secure but protect important social values such as privacy and free speech. I will address each of these in turn.

First, the need for a Comprehensive and Coordinated National Strategy could not be more clear. In the information age, a country's success is dependent upon information, knowledge, and communications. While the growth of the internet in the early 1990's created new beneficial opportunities for all, including individuals, businesses, and governments, it also created unprecedented opportunities for those who would misuse technology. It permits individual criminals, organized crime groups, and nation-states to target all types of sensitive information, from personal information to business information to military information.

It is therefore clear that our country's future success requires a Comprehensive Cybersecurity Strategy that engages the relevant agencies of the Government and brings to bear all elements of national power including economic, diplomatic, law enforcement, military, and intelligence authorities.

When one recognizes the breadth of the challenge, and the need for a massively decentralized but coordinated response among the Federal agencies, it becomes clear that our National Cybersecurity Strategy and its implementation should be led by the White House. Of course, any successful strategy must include protecting one's own networks from attack. Here it is critical that the Government and private sector work together to improve the state of computer security. Why is partnership required? It is because the private sector drives the design, development, and implementation of the products and services that power cyberspace.

We must also have the right objectives. For years the goal of the partnership has been information sharing which will not, without more, secure America's infrastructures. We must establish a more meaningful public/private partnership where the partners work in complementary fashion toward the clearly identified objective of securing America's networks. Consistent with this philosophy the partnership should focus on sharing information that is actionable and building mechanisms that enable meaningful action to be taken.

With regard to regulation, the Government and private sector should jointly determine the level of security provided by markets, the level of security needed to protect national security, and how the gap between what the markets will provide and what national security demands can be filled most effectively.

While this is not a call for broad regulation, it is a recognition that appropriately tailored legislation, legislation that is technology-neutral and recognizes the best practices created by the innovative private sector may be an important component of any national cybersecurity effort. The fact is, markets respond to customer

demand, and most customers know more security issues today than in the past will not pay for the level of security necessary to protect national security. In short, establishing a cohesive national strategy, a robust public/private partnership and a security model that takes advantage of industry best practices, Government influence, and tailored regulations can dramatically advance security.

Finally, creating the ability to identify what person and which device is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy. Even sophisticated attackers face difficult challenges and find their access restricted because of better authentication. Stronger authentication can also help us create safe places for our children to learn on-line, for businesses to interact with customers, and for Government to serve its citizens.

In addition, because the use of digital IDs also reduces the need to authenticate people by having them provide private details about themselves, stronger authentication can enhance both security and privacy. Thus, as part of an overall cybersecurity strategy, the Government should accelerate the adoption of authentication technologies by actions such as issuing and accepting digital credentials in appropriate circumstances and working to integrate privacy issues into the design, development, and operation of the resulting identity metasystem.

In conclusion, let me say there are complex challenges that obviously will not be solved overnight. Securing America's future in the information age depends upon creating a comprehensive national strategy for cyberspace security, one that simplifies, organizes, and enables effective operational partnerships among the Government, private sector, and internet citizens. There is both an opportunity and a need for leadership as we focus the Nation's attentions on the importance of cybersecurity.

I thank this committee for raising this important issue, for considering my written testimony as part of the record, and I look forward to your questions.

[The statement of Mr. Charney follows:]

PREPARED STATEMENT OF SCOTT CHARNEY

MARCH 10, 2009

Chairwoman Clark, Ranking Member Lungren, and Members of the subcommittee, thank you for the opportunity to appear today at this important hearing on cybersecurity. My name is Scott Charney, and I am the corporate vice president for trustworthy computing at Microsoft. I served as one of four co-chairs of the Center for Strategic and International Studies' (CSIS) Commission on Cybersecurity for the 44th Presidency. I served on the Commission as an industry expert with more than 18 years of security technology experience in both the public and private sectors, and have a long history of leading domestic and international cybersecurity efforts.

Prior to joining Microsoft, I was chief of the computer crime and intellectual property section in the criminal division of the U.S. Department of Justice. I was involved in nearly every major hacker prosecution in the United States from 1991 to 1999, worked on legislative initiatives, such as the National Information Infrastructure Protection Act that was enacted in 1996, and chaired the G8 Subgroup on High Tech Crime from its inception in 1996 until I left Government service in 1999.

Representative Jim Langevin (D–RI), Representative Michael McCaul (R–TX), Lt. Gen. Harry Raduege, USAF (Ret.), and I led the CSIS Commission effort, along with project director Jim Lewis of the Center for Strategic and International Studies, to identify key cybersecurity challenges facing the new administration and provide a

set of recommendations to address those challenges. Guided by our Congressional co-chairs, we assembled a group of individuals with cybersecurity experience in both Government and industry. The aim of the group was to identify both short-term recommendations that the next administration could implement quickly to make a noticeable improvement in the Nation's cybersecurity, and longer-term recommendations that are critical to the Nation's future cyber-objectives.

Thank you for the opportunity to appear today to provide a perspective on "Reviewing the Federal Cybersecurity Mission." I would like to address four specific themes that cross the Commission recommendations including: (1) The need for a comprehensive and coordinated national strategy for cyberspace security; (2) the imperative to radically evolve and elevate the public-private partnership model; (3) the need for an identity metasystem that makes the internet dramatically more secure while protecting important social values such as privacy and free speech; and (4) the necessity for a new regulatory model that protects innovation while providing appropriate Government oversight.

COMPREHENSIVE AND COORDINATED NATIONAL STRATEGY

As the CSIS Commission report makes clear, we are locked in an escalating and sometimes hidden conflict in cyberspace. The battle of bits and bytes has very real consequences for America, other nations, the private sector, and even what we have come to call "the internet citizen." Cyberattack joins terrorism and weapons of mass destruction as one of the new, asymmetric threats that puts the United States and its allies at risk. To be clear, there are risks to cyberspace other than those related to security; for example, the increasing number of machines and applications creates a very complex environment with challenging reliability issues, and our increased dependence on information technology makes the availability of systems a national and international imperative. But for the purposes of this testimony, I will confine my remarks to security.

The information age has arrived, but the United States has not yet built a comprehensive national cyberspace security strategy. The need for such a strategy has never been more urgent. America's leadership in a connected world cannot be assumed from its leadership in the industrial world. In cyberspace, the country does not remain unchallenged, as recent events have clearly proved. Some of the challenges we face include:

- America's reliance on interdependent global networks;
- The misuse of information technologies to support violent extremism;
- The ability of any individual to engage in activities formerly limited to nation-states (e.g., cyber-military espionage and cyber-warfare); and
- The ability of any nation, regardless of traditional measures of sophistication, to gain economic and military advantage through cyber programs.

In addition to these challenges, the Internet citizen—those individuals who use cyberspace for social and commercial interactions—is critically relevant to any solution. Unsecured computers can turn everyday users into a launch platform for attacks. Fear about on-line security and availability can have sweeping economic consequences. Trust in cyberspace, on the other hand, can create new opportunities, markets, and possibilities.

The United States must plan, organize, and act accordingly to develop a national cyberspace security strategy that can address these challenges. Historically, national security strategies have been characterized by their employment of all elements of U.S. power—economic, diplomatic, law enforcement, military and intelligence. A comprehensive cyberspace security strategy must include these elements and articulate how they will be employed to ensure national security and public safety, ensure economic prosperity, and assure delivery of critical services to the American public. Such a strategy must also recognize the ever-mounting importance of economic security. In the industrial age, power was generally based on physical might; in the information age, power is derived from information, knowledge, and communications.

In my opinion, there are three fundamental attributes that span all of the elements of national power. Articulating and advancing a clear understanding of norms, attribution, and deterrence in the context of cybersecurity can dramatically improve the national and international cyberspace ecosystem.

Norms.—U.S. foreign policy and diplomatic engagements on issues related to cyberspace security are not as focused as our efforts to combat terrorism or stem proliferation of nuclear weapons. I believe that the United States should marshal its significant diplomatic skills and expertise to advocate for cyberspace security and increase multilateral cooperation. I would caution that advocacy and cooperation are not goals in themselves. We need to focus advocacy and co-

operation efforts toward specific outcomes. For example, working with like-minded nations to define clearly articulated norms of nation-state behavior in cyberspace could help to deter state support for cyberattacks or hold nation-states that support such efforts accountable for their actions.

Attribution.—Attribution of cyberattacks is one of the most fundamental challenges facing the international community and the United States. The inability to attribute attacks can greatly impede the effectiveness of the Nation's response. Too often, valuable time is lost trying to determine if an attack or penetration of a system was an isolated criminal incident or one perpetrated by a foreign intelligence organization. Attributing the source is essential to ensuring the appropriateness of response—criminal prosecution or military/diplomatic measures. Absent strong attribution abilities, international and national strategies to deter acts will not be taken seriously by the community of attackers who thrive on this diagnostic weakness, nor by criminals that prey on citizens' inboxes and on-line accounts. Thus, we must focus on identity and authentication in cyberspace and enhancing swift international cooperation on cyberattacks.

Deterrence.—Deterrence did not happen overnight in the Cold War; the concept and strategy took several years to develop. Deterrence in the information age is perhaps even more complicated due to the lack of attribution and the inability to identify strong mechanisms to prevent hostile actions. But the United States can learn important lessons from the nuclear experience. In the Cold War, the United States kept sensitive information secret, but disclosed enough about our strategy and capabilities that allies and adversaries alike understood our commitment to national security and our ability to protect it. We must do the same for cyberspace.

Deterrence is very difficult when adversaries and bad actors are motivated and persistent. In order to improve cyberspace security in a meaningful way, deterrence requires a clear and unambiguous commitment by our Nation and understanding by the spectrum of bad actors—from cybercriminals, to organized crime, to nation-states—that violations of our cybersecurity have consequences. What makes deterrence successful is commitment, broadly known and broadly felt.

The sheer number of extremely important issues that transcend agency boundaries suggests that the coordination of any national cybersecurity strategy must reside within the one organization responsible for ensuring that the Government acts as one Government. If the Government wants to use all the instruments of its power—economic, diplomatic, law enforcement, military, and intelligence—then the center of gravity must be in the White House. I support the Commission's recommendations that, if implemented, would elevate the priority of cybersecurity and improve its strategic coordination. Creating a National Office for Cyberspace in the Executive Office of the President will provide the interagency coordination required to identify, assess, and manage cyberspace risks.

This office does not need to assume or manage all cybersecurity functions; rather, it should have a tightly defined mandate to develop strategy and coordinate the implementation of that strategy by the agencies that have jurisdiction over the elements of national power. It must also be recognized that the White House office will be best able to provide strategic leadership only when the agencies of Government responsible for executing their respective cybersecurity responsibilities are staffed with experienced and competent professionals who are resourced appropriately.

As you know, President Obama has directed the National Security Council and Homeland Security Council to initiate a 60-day review of the plans, programs, and activities under way throughout the Government that address cyberspace security. According to the White House, the review will build upon existing policies and structures to formulate a new vision for a national public-private partnership and an action plan to: Enhance economic prosperity and facilitate market leadership for the U.S. information and communications industry; deter, prevent, detect, defend against, respond to, and remediate disruptions and damage to U.S. communications and information infrastructure; ensure U.S. capabilities to operate in cyberspace in support of national goals; and safeguard the privacy rights and civil liberties of our citizens.[1]

A successful cyberspace security strategy requires more than a plan and an organization; it requires partnership. The private sector drives the design, development, and implementation of the products and services that power cyberspace. Our technical expertise and experience in the global marketplace make us key partners in developing national and international cyberspace security strategies. For more than

[1] *http://www.whitehouse.gov/blog/09/03/02/Cyber-review-underway/*.

a decade, the Government and the private sector have partnered to address various aspects of cybersecurity, but this partnership has not achieved the robust results that are needed to protect cyberspace effectively. Therefore, my next key recommendation is to redesign that partnership.

RADICALLY EVOLVE PUBLIC-PRIVATE PARTNERSHIPS TO ADVANCE CYBERSPACE SECURITY

Cyberspace security is a shared challenge and requires Government and the private sector to work together. The private sector designs, deploys, and maintains much of the Nation's critical infrastructure. However, the private sector faces unique challenges because its customer base and supply chains are global. It also builds commercial products that can be targeted by sophisticated advisories, including nation-states. Private sector firms are increasingly being forced to think about security challenges that cannot reasonably be mitigated by commercially realistic development practices, especially as users remain price-sensitive.

The Government also faces challenges. Unlike certain other traditional aspects of national security, cyberspace cannot be secured by the Government alone; it requires a coordinated effort involving the owners, operators, and vendors that make cyberspace possible. The bifurcation of responsibility (the Government must protect national security) and control (it does not manage the assets or provide the functions that must be protected) dictates the need for a close partnership with clearly defined roles and responsibilities that optimizes the capabilities of participating stakeholders.

Since the 1990s, well-intended public-private partnerships have been created to address this need, yielding a perplexing array of advisory groups with overlapping missions, different stakeholders with varying capabilities, insufficiently articulated roles and responsibilities, and plans with literally hundreds upon hundreds of recommendations. In the few instances where groups overcame institutional adversities and developed meaningful recommendations, the repeated unwillingness or inability to implement those recommendations at the Federal level has damaged the partnership significantly. Absent a comprehensive national strategy and clear purpose, both Government and private sector stakeholders will continue to struggle to be effective.

Advancing cyberspace security requires a radical evolution of public-private partnerships as we currently know them. What does radical evolution mean? The Federal Government and private sector stakeholders must articulate a new philosophy for collaboration, one that starts with a very simple premise: Government and private sector efforts should be synergistic and efficient. This requires that the Government and private sector: (1) Identify those security requirements that will be fulfilled by the market; (2) identify national security requirements; and (3) identify how the gap between market security and national security can be filled. This effort must be focused on protecting functions (e.g., communications) as opposed to simply physical assets. Moreover, we must build operational partnerships that let us effectively mitigate and respond to threats. Finally, to the extent important work is ongoing, the parties must identify what works and have the courage to retire what does not, even though retiring organizations may be viewed as draconian by those who have invested in these efforts in the past.

As part of the evolution, it is important that the public-private partnership concentrate on what is truly critical to cyberspace security and build trusted and effective collaboration between Government and private sector stakeholders.

What functions are critical?

The Commission identified four critical cyber-infrastructures:

- Energy;
- Finance;
- Converging information technology and communications;[2] and
- Government services (including State and municipal governments).

This is not to suggest that all these infrastructures are identical. If power fails, the cascading effect is immediate and significant; by contrast, the result of an attack on Government will depend upon what Government service is affected. In essence, energy and information technology and communications form the backbone of cyberspace, and the availability of Government services and finance are particularly important for national security. While other infrastructures depend on cyberspace, an

[2] Outside the United States, this is referred to as the ICT sector. See "Telecommunications Task Group Final Report," CSIS Cybersecurity Commission *http://www.csis.org/media/csis/pubs/081028_telecomm_task_group.pdf,* for more information on why "the boundary between information, information technology, and telecommunications services has become almost indistinguishable."

interruption of their operations would not broadly affect cyberspace itself. If energy, finance, the converging information technology and communications networks, along with Government services, can continue to function as intended while under attack, cyberspace will continue to support the Nation. Thus, these infrastructures should be the focus of a more attentive cyberspace security effort.

Trusted and Effective Collaboration

The majority of public-private partnership efforts to date have focused on information sharing. While information sharing is important, it cannot be—as it had been to date—the end goal; rather, we must focus instead on sharing information that is actionable and then taking action. The CSIS Commission recommended three new partnership groups to advance beyond information sharing to enable trust and action. I will focus my comments on the two that would most significantly and immediately enhance our cybersecurity and resiliency by permitting better strategy development and operational collaboration.

Evolve Strategic Presidential Advisory Bodies

Trust is the foundation of a successful partnership between Government and the private sector. In the past few years, despite good intentions on both sides, trust between Government and the private sector has declined. Trust is built on personal relationships and in small groups, with parity of stakeholders and demonstrated commitment. Large, diffuse groups with floating engagements among a range of participants are not conducive to building the level of dialogue that promotes trust. When the President brings C-Level officers to the table and addresses challenges in a trusted forum, he can drive a powerful set of changes in the cyber-ecosystem. Advisory committees that engage senior-level Government and private sector personnel, such as the National Security and Telecommunications Advisory Committee (NSTAC) and the National Infrastructure Advisory Council (NIAC), have served past presidents well. However, the split between national security and emergency preparedness communications and cybersecurity is artificial and dangerous. In the information age, with its converged information technology and communications infrastructure, the distinction between these two groups creates overlap and limits progress on developing and improving cyberspace security capabilities. Accordingly, the Commission recommended establishing the President's Committee for Secure Cyberspace to replace the NSTAC and NIAC.

In addition to establishing the proposed Committee for Secure Cyberspace as a C-level membership organization operated under Federal Advisory Committee Act, the administration should act to reform current decision-making bodies in Government that do not have private sector involvement. For example, the Joint Telecommunications Resources Board (JTRB), which is chaired by the Office of Science and Technology Policy, consists of agencies, such as the Department of Defense (DOD), the Department of Homeland Security, the General Services Administration, and the Department of Commerce.[3] The JTRB is chartered to make decisions on how to prioritize telecommunications resources in non-wartime crisis, yet absent an effective channel into the private sector, the JTRB would be challenged to fulfill its charter. Another parallel entity is the National Cyber Response Coordination Group, an organization intended to help identify and coordinate response to a cyber-based crisis. Unfortunately, this interagency Government group does not have a meaningful way to engage the private sector, thus limiting its strategic and tactical effectiveness.

Create Operational Collaboration

Over the past 10 years, there have been several attempts to improve operational coordination between and among key Government and private sector stakeholders, but these have met with limited success. For example, the private sector has invested and maintained information sharing and analysis centers, but they are all too often ignored by Government agencies. The Commission recommended creating a new organization, the Center for Cybersecurity Operations (CCSO), to address operational issues that affect cyber infrastructure.

I strongly support creating a more effective model for operational collaboration to move us from the less effective partnerships of the past to a more dynamic and collaborative self-governing approach involving cybersecurity leaders from Government, industry, and academia.

---

[3] Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," section 2(b)(3), April 3, 1984, available at *http://www.ncs.gov/library/policy_docs/eo_12472.html.*

Collaboration is not about plans; it is about outcomes. To create actual operational collaboration, we must learn from the experiences of the past. Collaboration is more than information sharing and is more than coordination; collaboration involves stakeholders working together, jointly assessing operational risks, and developing and implementing mitigation strategies. I would like to add to the Commission recommendation and suggest that an effective collaboration framework for public-private partnerships should include focused efforts to:

- Exchange technical data (at the unclassified level as much as possible), with rules and mechanisms that permit both sides to protect sensitive data;
- Create global situational awareness to understand the state of the computing ecosystem and events that may affect it;
- Analyze the risks (threat, vulnerabilities, and consequences) and develop mitigation strategies;
- When necessary and consistent with their respective roles, respond to threats; and
- Develop cyber threat and risk analytics as a shared discipline. For example, one could combine Government and private sector information and then use the private sector's expertise in analyzing large data sets in pseudonymous ways to get new insights into computer security without raising privacy concerns.

What needs to be accomplished over the long term, and the operational mission, must be clear and articulated; the roles of Government and industry must be well-defined; and all participants must demonstrate commitment and continuity to achieve success. The goal is a trusted and focused collaborative alliance for both strategy and operations among the Government, academia, and the private sector.

TAKE ACTION TODAY TO CREATE A MORE SECURE TOMORROW

On-line collaboration, commerce, and, in some instances, public safety depend on trust. Today the mechanisms to provide authentication and attribution in cyberspace do not meet the needs of the internet citizen, enterprises, or governments. The lack of trust stems in part from our inability to manage on-line identities effectively and the excessive reliance on voluntary efforts to close key gaps in security.

Identity Imperatives

In the context of national security, weak identification and authentication limits an organization's ability to enforce security policies to protect sensitive information and systems, and hinders effective Government and industry response to cyber attacks. From an economic security perspective, these weaknesses prevent internet users from taking reasonable steps to protect themselves from dangerous parties. Creating the ability to know reliably the person and/or device that is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy. Even sophisticated attackers face difficult challenges—and find their access restricted—because of better authentication.

This need for improved identity and authentication in cyberspace has been documented in numerous forums, and Government and industry are progressing on multiple initiatives to address it. For example, in the United States, the Federal Financial Institutions Examination Council's (FFIEC) Guidance for Authentication in an Internet Banking Environment has spurred the use of stronger authentication in on-line banking. The experience of the DOD was that intrusion into its networks fell by more than 50 percent when it implemented Common Access Cards (CAC). Homeland Security Presidential Directive 12 (HSPD–12) ("Policy for a Common Identification Standard for Federal Employees and Contractors") is another U.S. authentication initiative which requires Federal agencies to improve their identity and credentialing processes, using smart cards to secure both physical and logical access to Federal facilities and networks. These and other Federal initiatives have had success, but it is often limited to the sector or domain for which they are attempting to affect change.

Past efforts to radically improve identity management for cybersecurity have not failed due to lack of awareness regarding the problem, nor a lack of efforts to address it. Much more simply, there are too many disparate efforts resulting in stovepiped policies and technologies that conflict and compete with each other, instead of driving toward a coordinated, interoperable, scalable security- and privacy-sensitive solution. There is also, particularly in the consumer sector, a serious "chicken-and-egg" problem: Consumers are not interested in robust on-line identity tokens because Government and commercial sites do not consume them, and Government and commercial sites do not build technology to consume such tokens because, after all, no consumer has them. I want to re-emphasize a point made earlier: Any successful public-private partnership should start with the premise that the Govern-

ment should fill market gaps in security. Thus, as part of an overall cybersecurity strategy, the Government should accelerate the adoption of authentication technologies by supporting the creation and use of digital credentials. This would include issuing and accepting such credentials in appropriate circumstances, catalyzing the private sector market for digital identities, and establishing the appropriate governance structure for the issuance, use, revocation, and destruction of digital credentials.

The use of digital IDs also reduces the need to authenticate people by having them provide private details about themselves, known as Personally Identifiable Information or PII. This usage would reduce the need to transmit, store, and use private information to identify individuals, thus increasing privacy and helping prevent crimes such as identity theft. Stronger authentication, combined with appropriate rules regarding the use of such authentication mechanisms, could enhance both security and privacy.

I recognize that efforts to improve authentication raise sensitive privacy and civil liberties issues, but it is possible to improve authentication for critical functions without unduly compromising our values.[4] This can be done if we integrate privacy issues into the design, development, and operation of the identity metasystem.

The Role of Regulation

Opinions vary widely on how industry and Government can best work together to more effectively increase cybersecurity across critical infrastructures and Government. But even if public and private cooperation is optimized and operationalized, that will not provide the level of security necessary to meet national security demands. This is true because markets respond to customer demand and most customers, even though more aware of security issues today than in the past, will not pay for the level of security likely necessary to protect national security.

This recognition, however, does not mean the first step to address the gaps between the current and desired states of security should be broad-based regulation. Rather, the Government should encourage a balanced approach, one that combines industry self-regulation with Government influence (through, for example, procurement regulations) and then includes carefully tailored regulation when necessary. I believe such a combined approach can be highly effective without unduly raising the costs for users and stifling the very innovation that is needed to make infrastructures more secure.

When security gaps are identified—and neither market forces nor non-regulatory Government intervention suffices to address that gap—Government should focus on adopting the regulatory model suggested by the CSIS Commission. In this model, industry identifies the best practices, and the Government ensures their adoption and works to harmonize requirements across sectors. I would also add that any Government regulation should follow certain key principles: It should solve a clearly identified problem; it should neither be under-inclusive (fail to solve the problem fully) nor over-inclusive (address more than the problem); it should not be crafted in a way that creates unintended consequences; and it should be technology-neutral and not create hard-to-modify statutorily imposed technology requirements that stifle innovation and prevent further enhancements in security.

Progress in cyberspace security is not without cost. Voluntary efforts have closed many security gaps but have not done enough. Establishing a cohesive national strategy with a robust public-private partnership will create a framework for tailored regulations that can advance identity and trust in a manner that markets alone cannot.

MOVING FORWARD

The first major Presidential document on emerging threats in cyberspace was published more than a decade ago when the President's Commission on Critical Infrastructure Protection released its seminal report.[5] At that time, only 1.7% of the world's population (70 million people) had internet access. In the years that have followed, the world has changed dramatically. Attacks have evolved from exploits designed to garner attention to targeted stealth attacks that are designed for more nefarious purposes, such as conducting identity theft, economic espionage, and military espionage. In 2008, almost a quarter of the world's population (more than 1.5

[4] For more on this topic, including how the Government can ensure privacy is protected in a better authenticated environment, see the White Paper on Establishing End-to-End Trust, *www.microsoft.com/endtoendtrust* (pp. 6–7).

[5] *http://cip.gmu.edu/archive/5__PCCIPCriticalFoundations__1097__full__report.pdf.*

billion people) had internet access, and it continues to grow.[6] The rise of the internet has permitted new forms of social connection, and created new educational and economic opportunities. But the richness of cyberspace also permits criminals, foreign intelligence organizations, and nation-states to exploit cyberspace for profit, espionage, or conflict. Securing America's future in the information age depends upon creating a comprehensive national strategy for cyberspace security, one that simplifies, organizes and enables operational partnerships between and among Government and private-sector stakeholders, including internet citizens.

Ms. CLARKE. I thank you for your testimony.

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

STATEMENT OF AMIT YORAN, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, NET WITNESS CORPORATION

Mr. YORAN. Ms. Chairwoman and Members of the committee, thank you for the opportunity to testify on Reviewing the Federal Cybersecurity Mission and for your attention to this important topic. My name is Amit Yoran and I have a lot to say, so I will skip reading my bio and jump right into it.

An effective national cyber effort must leverage the intelligence community's superior technical acumen and scalability. However, it is in grave peril if this effort is dominated by the intelligence community. Simply put, the intelligence community has always and will always prioritize its own collection efforts over the defensive and protection mission of our Government's and Nation's digital systems. When intelligence operations discover a compromise, the decision to inform system defenders or not lacks transparency. Mission conflict exists between those defending systems and those attempting to collect intelligence or counter-intelligence insights.

The current series of cyber programs called for billions of dollars in funding for intelligence and centralized security efforts, but are designed with very little emphasis on helping defenders better protect the systems housing our valuable data and business processes.

For instance, the Center for Disease Control, which houses sensitive research and information about biological threats such as anthrax, has ongoing cyber incidents which it lacks the personnel and technologies to adequately investigate. In the face of spending billions more on centralized cyber intelligence activities, the CDC's cyber budget is being cut by 37 percent. Intelligence focused on national efforts are overclassified, to the point where catastrophic consequences are highly probable. High levels of classification prevent the sharing of information necessary to adequately defend our systems.

For instance, IP addresses, when classified, cannot be loaded into defensive monitor systems. It also creates insurmountable hurdles when working with a broad range of Government IT staffs that do not have appropriate clearances, let alone when trying to work with, communicate, and partner with the private sector. Classification cannot be used effectively as a cyber defensive technique, only one for avoiding responsibility and accountability. Overclassification leads to a narrowly limited review of any program.

One of the hard lessons learned from the terrorist surveillance program is that such a limited review can lead to ineffective legal

[6] *http://www.internetworldstats.com/emarketing.htm.*

vetting of a program. The cyber mission cannot be plagued by the same flaws as the TSP.

An immediate, thorough, and transparent legal analysis of the governance authority's privacy requirements should be performed on the efforts used to both protect our CT systems as well as all cyber collection activities. Given the broad concerns of overclassification and its cascading consequences, conducting these reviews must be a high-priority task.

Cyber research investments are practically nonexistent at a time when bold new visions need to be explored. The Department of Homeland Security has demonstrated inefficiency and leadership failure in its cyber efforts. While pockets of progress have been made, administrative incompetence and political infighting have squandered meaningful advancement for years now, while our adversaries continue to aggressively press their advantage.

DHS has repeatedly failed to attract or retain the leadership and technical acumen required to successfully lead in the cyber mission. While the tendency would be to move the cyber mission to the NSA, it would be ill-advised for all the reasons I provide in my much longer written testimony.

We must enable civil government to succeed in its mission of defense or also concede that the private sector, too, cannot succeed in its defensive mission and subjugate them to intelligence support. DHS is the natural and appropriate place for public/private partnership and cooperative activities, including those in cyber.

The current set of public/private partnerships is at best ill-defined. They categorically suffer from meaningful value creation or private sector incentives for participation. Such incentives might include tax credits, fines, liability levers, public recognition, or even occur at an operational level through mechanisms such as the sharing of threat intelligence, technical knowledge, incident response report, to name just a few.

Trust relationships when dealing in cybersecurity matters are absolutely critical. In discussions among privacy and civil liberties group, the role of the NSA in monitoring or defending U.S. networks is debated. Should such intelligence programs exist, DHS should be very cautious before participating in, supporting or engagement in these activities.

The Department's ability to fulfill its primary mission and responsibilities may be permanently damaged by a loss of public confidence and trust. At a bare minimum, in order to preserve this trust, any interacting with domestic intelligence efforts should be explicitly and clearly articulated.

Sufficient transparency may serve to increase public trust and confidence and offset concerns raised by uncertainty and the uninformed. DHS must be formally charged with and enabled to build an effective cyber capability in support of securing our Federal civilian systems. Special provisions should be made in the hiring, contracting, human resources, and political issues within the cyber mission of DHS to prevent it from remaining a victim of the Department's broader administrative failures.

DHS should be given specific emergency authorities to address security concerns in civil systems, to include the ability to measure compliance with security standards, protocols, and practices, and

take decisive action where organizations are not applying reasonable standards of care. At present, the operation's cybersecurity arm of DHS, US–CERT, remains politically torn apart into three components, completely subjugated to a cadre of detailees from the intelligence community.

In order to regain efficiency, the Department's operational security activities must be reconsolidated in the US–CERT. This operational mission is not resourced to succeed with less than 20 Government FTEs and a budget of only $67 million.

Ms. CLARKE. Mr. Yoran, I am just going to ask if you can summarize and we will probably pick up on more of your testimony through questions. Of course, we have your full testimony in the record.

Mr. YORAN. Yes, Madam Chairwoman.

The newly focused DHS US–CERT should report directly to the Secretary of DHS, just as NTOC reports to the Director of NSA. The cyber responsibilities of the Department must not remain buried in the Department or, alternatively, they must be removed and placed in an independent agency where they can succeed. Thank you.

[The statement of Mr. Yoran follows:]

PREPARED STATEMENT OF AMIT YORAN

MARCH 10, 2009

Ms. Chairwoman and Ranking Member, thank you for the opportunity to testify before the Homeland Security Committee on Reviewing the Federal Cybersecurity Mission.

My name is Amit Yoran and I am the CEO of the NetWitness Corporation, a company providing next generation cybersecurity monitoring technologies to the U.S. Government and private sector, including Fortune 500 companies delivering critical infrastructure cyber protection to the Nation. I serve as a member of the CSIS Cyber Commission advising the 44th Presidency and on numerous security industry advisory bodies.

Previously I have served as the first Director of the National Cyber Security Division (NCSD) in standing up the United States Computer Emergency Readiness Team (US–CERT) and Einstein program at the Department of Homeland Security (DHS), as founder and CEO of Riptech, a leading managed security services provider, and as manager of the Vulnerability Analysis Program (VAP) of the U.S. Department of Defense's Computer Emergency Response Team (DoD CERT). I received Bachelor of Science degree in Computer Science from the United States Military Academy at West Point and Master of Science in Computer Science from The George Washington University.

Over the past 15 years, automation and use of computer systems has permeated every aspect of modern life. Our Nation is entirely reliant upon computer systems and networked technologies in everything from national security and intelligence activities to commerce and business operations to power production and transmission to personal communications and correspondences.

Today's internet has become one of the unifying fabrics driving globalization at an increasingly accelerated pace. It represents the core means by which personal and organizational interactions occur whether those communications take the form of internet email or simply phone calls, which invariably traverse the cyber realm. Beyond its role as a communications medium, computer-based automation and technology are the driving forces behind every major industrial and economic base in the world. Simply put, computer technologies and communications represent the greatest threat to and opportunity for expansion of the U.S. values system.

EVOLVING INTO A NATIONAL CYBER STRATEGY

The past 2 years have brought about an unprecedented level of Federal focus and attention on cyber security matters culminating in a portfolio of activities commonly referred to as the Comprehensive National Cyber Initiative (CNCI). Advocacy for

CNCI under the Bush administration resided in the Office of the Director of National Intelligence (ODNI), under whose charge the billions of dollars in programs were conceived and orchestrated. While many of the CNCI programs are well intended and designed, there are several significant flaws in adopting the Bush administration's CNCI as an on-going national cyber strategy.

- White House leadership. The Obama White House is currently conducting a comprehensive 60-day review of cyber. The purpose of the review is to develop a strategic framework to ensure that "initiatives in this area are appropriately integrated, resourced and coordinated both within the Executive Branch and with Congress and the private sector." This review effort will culminate in recommending an optimal White House organizational structure for dealing with the cyber challenges facing our national and economic security as well as "an action plan on identifying and prioritizing further work in this area." For the reasons outlined below, an effective national effort to address cybersecurity can only succeed through continuous, active, and decisive White House leadership.
- Intelligence.
  - An effective national cyber strategy must leverage the strength of the intelligence community. As information and computer-based technologies increasingly permeate how the world works, opportunities abound to improve the types, quantity, and quality of intelligence the community can provide at various levels of classification to its consumers. In the primary intelligence functions of collection, analysis, and dissemination, cyberspace can provide an effective aspect to operations. The volumes of information and the diversity of sources can quickly become overwhelming. The intelligence community must continue to refine its ability to evaluate the quality and value of such information and accurately assess it in order to assure its appropriate dissemination to decisionmakers. This should include improved functionality around attribution in cyberspace.
  - There is a clear and distinct conflict of interest between intelligence objectives and those of system operators. Simply put, intelligence organizations prioritize the intelligence and counter-intelligence missions; which in cyber focuses on monitoring adversaries, determining their methods and techniques, tracking their activities to a point of origin, and determination of compromise scope, and attack intent and adversary's objectives. While these are very important, they frequently conflict directly with the information assurance objectives of system owners and operators, who are primarily concerned with system defense and protection, and in the event of compromise, a speedy restoration to a functional and assured state. This distinction in core objectives is critical because it represents the difference between programmatic emphasis on information gathering, or system resilience and availability. For instance, intelligence and law enforcement entities often prioritize attack attribution, while almost no emphasis is placed on attribution by those defending systems. Rather than sharing information with operators and better informing them as to how they can defend and monitor themselves, an intelligence community-centric mindset around cyber would limit information exchange and instead focus on enabling the intelligence community to perform an expanded and aggregated monitoring program. Such a monitoring program would face significant cost and scalability impediments. We must remember the purpose for a monitoring program. Are we in fact monitoring to enable better defenses? Who makes the decisions to inform the defense? It is a clear conflict of interest for those who collect to make this decision. The decision should be a balanced one. Prioritizing the intelligence mission also has significant resource allocation implications. Amid news stories of billions of dollars in cyber spending under CNCI a majority of resources are going to intelligence and centralized monitoring activities. For instance, the Center for Disease Control, where sensitive information resides about biological threats, such as anthrax, has on-going incidents which they do not have the manpower or technology to adequately investigate. In the face of these challenges, this year the CDC's cybersecurity budget will be reduced by 37%.
  - For ill-defined reasons, the CNCI led by ODNI has been shrouded by a high degree of secrecy and lack of transparency. The plan itself is so classified that even Members of Congress have not been provided copies and industry has had no access to the document. While the need for high levels of classification may exist in certain components of a national cyber effort, such as offensive capabilities or for the protection of sources and methods, such a broad overclassification is counterproductive to supporting an effective cyber defense. Such information is prevented from being shared with operators, most of which do not hold adequate clearances and creates significant hurdles when

trying to defend unclassified systems. In recent examples adversary internet addresses used in attacks and their various attack methods have been classified to the point they were not broadly available for defensive purposes or provided through channels. In numerous cases this roadblock prevented information from being used effectively in cyber defense and provided further advantage to our adversaries. If you cannot or will not share useful information with cyber defenders, their job is made far more difficult. As the private sector is increasingly the target of foreign intelligence efforts, a national cyber effort will need to further evolve its abilities in working with the private sector. Most importantly, over-classifying a national cyber strategy prevents adequate public review and debate to assure that the programs are designed optimally, contain the highest level of innovation, and are well-aligned with and informed by the total body of knowledge of the cyber security profession. Often classification is used to hide weaknesses found. Classification cannot be used effectively as a cyber defensive technique, only one for avoiding responsibility and accountability. Over-classification leads to a narrowly limited review of any program. One of the hard-learned lessons from the Terrorist Surveillance Program (TSP) is that such limited review can lead to ineffective legal vetting of a program. The cyber mission cannot be plagued by the same flaws as the TSP has been.

- Intel loss/gain analysis has historically been performed by the intelligence community's judgment without substantive subject matter input from those whose systems are being damaged. If the intelligence community takes on a leadership role for the cyber mission it is likely that additional monitoring programs will be put in place to find the adversary. While the technical acumen within NSA is strong, better controls over operations would be needed to reduce the natural emphasis on collection and instead prioritize the protection and availability of Government and industry systems. The cyber mission suffers in favor of the intelligence mission all too often. While protecting sources and methods, the intelligence community needs to better inform public and private sectors on the threat environment and how they can better defend themselves. Moreover, some organizations may be less likely to act responsibly and invest properly in monitoring and defending their own systems if they feel as though they can rely on some federated intelligence monitoring operation.

- Research and Development. The current paradigm in cyber security is not likely to change significantly through improved security products, monitoring, and incident response capabilities. While the private sector makes significant investment in incremental product, application, and protocol improvements; fundamental research is required to meaningfully improve the security of the cyber and critical infrastructures.
  - According to the CSIS Commission work, "The federal government plans to spend about $143 billion in 2009 on R&D. We estimate that two-tenths of 1 percent of that will go to cybersecurity." An inherently Government investment must drive long-term research agendas in cybersecurity, where private sector focus on shorter-term commercialization limits results to more tactical or incremental advancements. The Department of Homeland Security's Science and Technology Directorate invests less than $20 million per year on cybersecurity research efforts, a far cry from any responsible level of resource allocation.
  - The Government should not use this money to be in the security product development business, especially via classified venues. In an overwhelming majority of instances, Government cyber requirements are substantially similar to if not exactly the same as the private sector and only in the rare cases where they are not or in classified instances, do specific tactical Government development efforts make sense to consider. In addition, it is a fact that there is a severe lack of qualified engineers needed to develop these systems. Today, the majority of these engineers are employed by the security industry. The Government and intelligence community should guide and assist in functional requirements for the development of technologies which can help us best address the sophisticated cyber threat environment, not enter the product development business. The resulting improvement in security technologies will not only benefit the Government in protecting its systems, but will also benefit the Nation's critical infrastructure operators and rest of the shared internet fabric that joins our digital world. Additionally, Government development efforts have stranded enterprise cyber defenders without the benefits of product management, maintenance, and professional support.

- Standards and Acquisition reform. The CSIS Commission report provides a lot of insight into how the Government can positively improve its situation as well as security of private networks by leveraging its expertise in standards, setting and using its procurement size to effect product vendor behaviors. We also need to consider more dynamic methods for systems procurement and lifecycle management as the current processes seem marginally nimble enough to enable the purchase of a battle tank or fighter jet. Antiquated and poorly maintained systems compound our challenges. The systems on Federal networks average 5 years old. Unlike responsible parties in the private sector, Federal networks frequently do not have centralized patching, vulnerability understanding, or adequate monitoring technologies and processes. Simply put, they are not achieving or maintaining an appropriate standard of care by any responsible measure. It should be understood the reasons for this are a lack of IT and IT security governance. The technology here is not overly complex; the real challenge is the people and the process. The average Government executive, whether DoD or civil, stays in his/her position for an average of 18 months. There is little or no reason to look ahead at the next executive's tenure and budget or plan for the life cycle management or security of a system 18 months later. In addition, because planning was not done in the previous executive's tenure, the system the executive has to care for is more likely than not to be in an unkempt, dated, and insecure state. There is no governance mechanism or motivation for Government systems to plan, budget, or perform best practice life-cycle management which can significantly reduce risk of loss. Please see the recently published Consensus Audit Guidelines for a reasonable approach to minimal security practices.
- Legal Review and Privacy Oversight.
  - Congress and the Obama Administration must work together to modernize authorities. FISMA and Clinger-Cohen are dated and fraught with politics and games. Without hard-hitting, detailed legislation that structures governance and authorities no program will succeed. Today the CNCI is not codified. HSPDs 54 and 23 are not supported by legislation, therefore are not mandated. An immediate, thorough, and transparent legal analysis of the governance, authorities, and privacy requirements should be performed on both the efforts used to protect IT systems as well as an analysis with the requisite understanding of intelligence and national security law for all cyber collection activities. Given the broad concerns of over-classification, conducting these reviews must be a high priority task.
  - An effective national cyber function requires an informed privacy function. Privacy issues need proper review and advocacy when designing various Government cyber security programs, especially those of the intelligence and law enforcement communities. An effective program should be implemented in a non-partisan fashion by qualified privacy professionals who are not members of the executive or legislative branches and have fixed terms of service without eligibility for reappointment or extension terms. Security can be implemented with and even contribute to enhanced privacy, but it is not easy and often not without strong and deliberate privacy advocacy and oversight.
- Homeland Security.
  - The Department of Homeland Security (DHS) has demonstrated inefficiency and leadership failure in its cyber efforts. While pockets of progress have been made, administrative incompetence and political infighting have squandered meaningful progress and for years now our adversaries continue to aggressively press their advantage. Recently, the Director of National Intelligence, Admiral Dennis Blair, told the House intelligence committee that, "the NSA, rather than the Department of Homeland Security which currently oversees cybersecurity, has the smarts and the skills to secure cyberspace." In his assessment of both organizations he is absolutely correct. DHS has repeated failed to either attract or retain the leadership and technical acumen required to successfully lead in the cyber mission space. On a number of occasions proven, talented, and knowledgeable leaders from within the Government or successful experts from private sector have joined the Department in hopes of meaningful contribution. In its cyber responsibilities DHS has a consistent track record for tolerating political infighting, individual egos, and shenanigans over prioritizing and executing its cyber responsibilities in a mature fashion. While the tendency would be to migrate the cyber mission to the NSA, that would be ill-advised for all of the reasons provided earlier. In Rod Beckstrom's resignation letter last week, he states, "NSA effectively controls DHS cyber efforts thru detailees, technology insertion and the proposed move of NPPD and the NCSC to a Ft. Meade NSA facility. NSA currently domi-

nates most national cyber efforts . . . The intelligence culture is very different than a network operations or security culture. In addition, the threats to our democratic processes are significant if all top level government network security and monitoring are handled by any one organization." This could not have been more accurately stated. We must enable civil government to succeed at this mission. This being said, it is far past time we fix the DHS problems and move forward.

- Public-Private Partnership. In addition to defining increased security functionality and assurances for Commercial Off the Shelf Software (COTS), the Government must work more closely with the private sector and understand their businesses if it is to be effective in constructing useful partnership programs. Programs managed in a vacuum by the intelligence community at a highly classified level are unlikely to work well and in concert with system operators within the Federal Government, let alone in the private sector, where not only are mission objectives completely foreign, but where there are very few people with Government clearances. Government programs need to focus on open dialog and information exchange, and enabling the private sector to better understand the security challenges they face and how they might be overcome with the help of the Government. DHS is the natural and appropriate placement for public-private partnership and cooperative activities, including those in cyber security. The current set of public-private partnerships are at best ill-defined. While well-intentioned and occasionally valuable information is brought to the Department, they categorically suffer from meaningful value creation to the private sector. A deeper understanding of how cyber defense and security operations are implemented in the private sector is required by those crafting the evolution of these programs so that adequate incentives can be appropriately incorporated going forward. Such incentives might include tax consequences, fines, liability levers, public recognition, or even occur at an operational level, such as the sharing of threat intelligence, technical knowledge or incident response support to name just a few. Due to its fluid nature, trust relationships when dealing in cyber security matters are at least as strongly emphasized as in physical security. In news reports and discussions among privacy and civil liberties groups the role of the NSA in monitoring or defending domestic private networks is debated. Should such intelligence programs exist, DHS should be very careful to distance itself from participation, support, or engagement in these activities. The Department's ability to fulfill its primary mission and responsibilities may be permanently damaged by a loss of public confidence and trust. At a bare minimum, in order to preserve public trust, its interaction with domestic intelligence collection efforts should be explicitly and clearly articulated.
- NCSC and US–CERT. Congress and the administration should focus DHS where it can have the greatest positive impact. The Department's culture migrates toward increasing its own mission scope and infrequently emphasizes a crawl, walk, run mentality. Sometimes, it's just time to close PowerPoint and Word, stop the rhetoric and simply roll the sleeves up and begin the actual work at hand. For instance, spending the Department's limited resources on advocacy programs for better software development, where the Department has very limited experience, expertise, and credibility is of exceptionally limited value.
- The US–CERT works to support the security of Government networks through design, deployment and monitoring the Einstein series of programs to enhance situational awareness, be the centralized incident reporting authority for the Federal civilian networks, facilitate efficient incident response and cleanup efforts, support the private sector through information exchange with critical infrastructure operators, and working with IT and IT security product vendors to assure that they can address the needs of the broader Federal Government and critical infrastructures.

  At present the US–CERT remains torn apart into three arms; a technology deployment arm (lead by an intelligence community detailee), a security arm (managing the Trusted Internet Connection program), and the operations arm (performing the core US–CERT mission). This stove-piping has added political strife, inability to spend 2009 money this year, and defocusing all from accomplishing the single US–CERT mission. In order to regain any efficiency, the Department's operational security role, which has been ripped apart by years of political infighting, must be reconsolidated in the US–CERT. The critical work of the US–CERT with its operational mission is not resourced to succeed (fewer than 20 Government FTEs, a budget of only $67 million out of the De-

partment's $355 million spend on cybersecurity). Additionally, the US–CERT must be lead by a single Federal civil executive.

The coordination function of the National Cyber Security Center is underutilized. Rod Beckstrom's recent resignation claims that only 8 weeks of the annual funding have been provided to it. His concerns for NSA management control of DHS' cyber efforts apply to the US–CERT as well, which reports to detailee from the USSS, who reports to detailee from NSA/Navy. All special assistants around the Acting Assistant Secretary are also NSA detailees. The US–CERT must be provided appropriate staffing levels to move forward and given adequate funding. Not doing so cannot help but send the strongest message to the cyber community, the rest of Government, the intelligence community, and the private sector that cybersecurity does not matter to DHS leadership and the Department's role is unnecessary. A newly focused cyber mission must report directly to the Secretary of DHS. This critical mission has been sought aggressively by so many parties, but resisted so strongly by the Department responsible for its successful execution. Cyber must not remain buried in the bureaucracy of DHS or, alternatively, it must be removed and placed where it can succeed.

The House Homeland Security Committee and Congress should work with the Executive branch to assure these fundamental changes are made:

1. DHS must be charged with and enabled to build an effective cyber capability in support of securing Federal civilian systems.
   a. Make special provisions in the hiring, contracting, human resources, political issues within the cyber mission of DHS to prevent it from remaining a victim of the Department's broader administrative failures.
   b. Enable the US–CERT to stand up the capabilities necessary to assist in the defense of Federal civil government as a component of the Federal civil agency charged with defending the homeland.
   c. DHS should also be given specific emergency authorities to specifically address security concerns in civil systems, to include the ability to measure compliance with security standard, protocols, and practices and take decisive action where organizations are not applying reasonable standards of care.
2. Flesh out, define roles, responsibilities and authorities of DHS, DoJ, DoD, NSA, and other Federal departments and agencies engaged in securing digital infrastructure. Such a framework should be publicly stated so that trust and confidence in cyber programs can be restored. It will also be a critical step in guiding more informed and consistent interactions with the private sector. Steps must also be put in place to allow the White House, Congress, departments and agencies to have visibility, input, and clear oversight into the process and solutions.
3. Adequately resourcing for success.
   a. A large-scale reallocation of the DHS cyber monies toward the programs which are operational and provide meaningful value add to its responsibilities to the Federal civil networks is needed.
   b. There exists stronger network controls and millions of dollars spent by DoD and NSA to protect the DoD networks, and that they still are under-resourced to adequately defend themselves. Only a fraction of that is being spent to defend Federal civilian systems and in reality those networks are by comparison 10 times larger than the Defense Department's.

Thank you for the opportunity to testify. I would be happy to answer any questions you may have at this time.

Ms. CLARKE. I thank you as well for your testimony.

I now recognize Ms. Davidson to summarize her statement for 5 minutes.

STATEMENT OF MARY ANN DAVIDSON, CHIEF SECURITY OFFICER, ORACLE CORPORATION

Ms. DAVIDSON. Chairwoman Clarke, Members of the subcommittee, my name is Mary Ann Davidson. I am Chief Security Officer for Oracle. Thank you for the opportunity to testify regarding the important issue of cybersecurity.

The Declaration of Independence states all men are created equal. All information systems, however, are not. The truth of the statement should be self-evident but it isn't, and therein lies a risk

to our freedoms. The ubiquity, flexibility, and configurability of information systems has led to circumstances in which software designed for a particular purpose and environment is too often deployed in an environment it was never designed for, without any thought or explicit acceptance of the risks in so doing. There is no substitute for knowing up front what you need software for, how it is going to be deployed, and what risks you can accept and what risks you won't. The time to make these determinations is during procurement, not afterwards.

The Navy does not purchase container ships and try to deploy them as aircraft carriers, nor does the Air Force purchase Gulfstream V's and try to configure them as F–22 Raptors. While there is nothing wrong with container ships or Gulfstream V's, they were not designed for the operational needs or the threat environment that aircraft carriers and F–22s were designed for.

Why then is information technology somehow different? It isn't. Good security, like good hardware, starts in procurement: Knowing what you need, how it will be used, and explicitly describing the threat environment for deployment. Use procurement wisely and aggressively.

This brings me to my second point. Information technology is mission-critical not merely mission-enabling. Our entire economy rests on an IT backbone; in particular, our homeland security and our military's ability to prosecute war rests on an IT backbone. DOD continues to invest in network-centric operations, which is all about getting the right information to the right warrior at the right time and the right battlespace. This makes the network itself the battlefield and therefore, DOD needs to enhance the treatment of information systems as a core mission specialty as well as using information systems offensively. Absent this capability, the DOD will not be able to use IT as the force multiplier it is.

Just as General Patton knew his tanks and their technical capabilities very well, not just merely how to deploy them, our military and homeland security leaders need to know and how to deploy and embrace the full capability of IT. Putting it differently, do we envision having a contractor at the helm of an aircraft carrier? If not, then why would our cyber offense be any different? General Patton also knew that the 3rd Army would stop without supplies of gas. Netcentric armies stop without supplies of information. Only by holding capability for both function and esteem can offense inform defense.

This brings me to my third point. We are in a conflict. Some would say a war. Let's call it what it is. Given the diversity of potentially hostile entities building cadres of cyber warriors probing our systems, including our defense systems for weaknesses, infiltrating U.S. Government networks and making similar attempts against American businesses and critical industries, is there any other conclusion to be reached?

There are three obvious outgrowths from the above statement. One is that you can't win a war if you don't admit you are in one. The second is that nobody wins on defense. The third is that we need a doctrine for how we intercede in cyberspace that covers both offense and defense and maps to existing legal and societal principles in the off-line world.

In short, Congress should consider developing a 21st century application of the Monroe Doctrine. The need for a framework to guide the Government's role in response to foreign aggression is a point that Melissa Hathaway has specifically noted during her review and an area where this subcommittee can work with the National Security Council.

You may recall that the Monroe Doctrine, introduced in 1823, said that further efforts by European governments to interfere with the States in the Americas, the Western Hemisphere, would be viewed by the United States as acts of aggression, and the United States would intervene. The Monroe Doctrine is one of our longest-standing foreign policy tenets, invoked on multiple occasions by multiple Presidents. We have, as the expression goes, sent in the Marines and the rest of our Armed Forces to uphold it.

Some may argue that cyberspace is virtual and unsuited to declared spheres of influence. But even internet protocol addresses mapped to physical devices in physical locations we care about: Critical infrastructures such as a server for a utility company in New York or a bank in California. Note that the Monroe Doctrine did not detail the same intervention or even specific intervention for each perceived act of aggression. Merely laid out "Here is our turf, stay out or face the consequences," language that allowed great flexibility in terms of potential responses.

We need not militarize all elements of U.S. cyberspace any more than invoking the Monroe Doctrine meant creating permanent military encampments throughout the Western Hemisphere. The advantages of invoking a Monroe Doctrine in cyberspace would be to put the world on notice that the United States has cyber turf, and the second is that we will defend our turf. We need to do both now.

Thank you and I look forward to your questions.

[The statement of Ms. Davidson follows:]

PREPARED STATEMENT OF MARY ANN DAVIDSON

Chairwoman Clark, Members of the subcommittee, my name is Mary Ann Davidson, and I am Chief Security Officer for Oracle. For more than 30 years, information security has been a central part of Oracle's software DNA, and is a big reason why the Federal Government is Oracle's largest customer. Thank you for the opportunity to testify regarding the important issue of cybersecurity.

1. The Declaration of Independence states "All men are created equal." All information systems, however, are not.

This truth of this statement should be self-evident but it isn't, and therein lies a risk to our freedoms. The ubiquity, flexibility, and configurability of information systems has led to circumstances in which software designed for a particular purpose and environment is too often deployed in an environment it was never designed for, without any thought or explicit acceptance of the risks in so doing. Without properly scoping our requirements we are faced with an all-or-nothing approach to cyberspace, simultaneously putting at risk our civil liberties, our homeland security and the women and men of our armed forces.

Let me give you a present-day example: I had a most frightening conversation with a highly placed official in the Defense Department who said that DoD wanted to use popular social networking software and that (direct quote) "you in industry need to secure it." My response to that statement: "What is DoD going to use the software FOR? 'Hi, I'm an al Qaeda operative. I like long walks on the beach and IEDs. Will you friend me?'" Without an appropriate context, I noted to the gentleman, there is no magic security dust we in industry can sprinkle on technology that is already "out there and being used," especially if we do not know what it is being used for. Certainly there are legitimate scenarios where we may want to permit our troops to use social networking software as a morale booster, including contact with their family and friends, but the technical and policy-based security re-

quirements around that use case are different from a use case where the DoD might use similar technology for operational purposes.

There is no substitute for knowing upfront what you need software for, how it is going to be deployed, and what risks you can accept and what risks you won't. The time to make those determinations is during procurement, not after. The Navy does not purchase container ships and try to deploy them as aircrafts carriers. Nor does the Air Force purchase Gulfstream Vs and try to configure them as F–22 Raptors. There is nothing wrong with container ships or Gulfstream Vs, by the way, but they were not designed for the operational needs or—and I emphasize this last point—threat environment that aircraft carriers and F–22s were designed for. Why, then, is information technology somehow "different?" It isn't. Private industry and Government agencies have varying use cases and threat environments in cyberspace, just as they share different requirements in the real world. And where privately run information systems can benefit from defensive technologies informed by our offensive capabilities—to use a metaphor—this rising tide will lift all ships in cyberspace.

Unfortunately, many think software is so flexible and configurable, that one size fits all applications. It doesn't. The military already knows this, but sometimes they need an occasional reminder. When I was a naval officer, I had many different uniforms: dress blues, dress whites, tropical whites, khakis, and utility greens. Each had its purpose. Should one be foolish enough to wear dress blues to a firefight, it isn't merely that you will be breaking uniform regulations; you aren't going to be adequately protected, either. You wear body armor to a firefight. While cost is one consideration in deployment, it need not be the only one, unless we plan on digging up old Lee-Enfield rifles and giving them to the Marine Corps instead of the M–16s they now use. "You get what you pay for" is as true in software as in anything else.

Good security, like good hardware starts in procurement: Knowing what you need, how it will be used, and explicitly describing the threat environment for deployment. Use procurement wisely and aggressively.

This brings me to my second point.

2. Information technology is mission critical, not merely mission enabling.

Our entire economy rests on an IT backbone: The acronym "IT" therefore represents "infrastructure technology" as much as "information technology." In particular, our homeland security and our military's ability to prosecute war rests on an IT backbone. DoD continues to invest in network-centric operations, which is all about getting the right information to the right warrior at the right time in the right battlespace. Therefore, the network itself is the battlefield because the network is what our enemies will attack if they want to deny us the ability to use our own technology (or in an attempt to use our technology against us).

Given that DoD has bet the farm on information systems, they need to enhance its treatment of information systems as a core mission specialty in supporting roles as well as using information systems offensively as a warfare specialty. Absent this capability, the DoD will not able to fully use IT as the force multiplier it can be. Just as Patton knew his tanks and their technical capabilities very well, not just merely how to deploy them, our military and homeland security leaders need to know and embrace the full capability of IT. Putting it differently, do we envision having a contractor at the helm of an in-theatre aircraft carrier? If not, then why would our cyber offense be any different? Note that the ability to deploy and support systems itself is also a critical mission specialty, just as, say, supply/logistics is a staff function in the military but a critical one. Patton knew very well that armies stop without supplies of gas; net-centric armies stop without supporting information systems. Furthermore, only by holding capability for both functions in esteem can "offense inform defense" and vice versa.

We must also remember the strength of the American economy rests on the flexibility afforded the private sector to innovate and market those innovations globally. In the same way our Nation's electrical grid, pipelines, roads, and railways support our military but are not run by our military, our critical cyber infrastructures and the companies who create them cannot simply fall under military control. Of course our Government should defend our cyber interests, but in the same way we would abhor a military presence at every intersection, we must also ensure civilian control over the normal operation of our digital highways.

This brings me to my third point.

3. We are in a conflict—some would say a war. Let's call it what it is.

Given the diversity of potentially hostile entities building cadres of cyberwarriors, probing our systems—including our defense systems—for weaknesses, infiltrating U.S. Government networks and making similar attempts against American busi-

nesses and critical industries, is there any other conclusion to be reached? Whatever term we use, there are three obvious outgrowths from the above statement. One is that you can't win a "conflict"—or war—if you don't admit you are in one. The second is that nobody wins on defense. The third is that we need a doctrine for how we intercede in cyberspace that covers both offense and defense and maps to existing legal and societal principles in the off-line world. In short, Congress should consider developing a 21st century application of a Monroe-like Doctrine. The need for a framework to guide the Government's role in response to foreign aggression is a point that Melissa Hathaway has already noted during her 60-day interagency review of the Federal cybersecurity mission, and an area where this subcommittee can productively collaborate with the National Security Council.

For those a tad rusty on their U.S. history, the Monroe Doctrine (introduced December 2, 1823) said that further efforts by European governments to interfere with states in the Americas—the Western hemisphere—would be viewed by the United States as acts of aggression and the United States would intervene. The Monroe Doctrine is one of our longest-standing foreign policy tenets: Invoked on multiple occasions by multiple presidents, including Teddy Roosevelt, Calvin Coolidge, Herbert Hoover, and John Kennedy. We have, as the expression goes, sent in the Marines—and the rest of our armed forces—to support the Monroe Doctrine.

Note that the Monroe Doctrine did not detail the same intervention or even specific intervention for each perceived act of aggression, merely laid out "here is our turf; stay out or face the consequences" language that allowed great flexibility in terms of potential responses. Some may argue that cyberspace is "virtual" and unsuited to declared spheres of influence. But even internet protocol (IP) addresses map to physical devices in physical locations we care about—critical infrastructures such as a server for a utility company in New York, for example, or a bank in California.

The advantages of invoking a Monroe-like Doctrine in cyberspace would be to put the world on notice that the United States has cyber "turf," (properly and narrowly scoped—we should not claim all cyberspace as our turf). The second is that we will defend our turf. We need to do both. Now.

As I mentioned earlier, having a military response capability does not mean militarizing all elements of U.S. cyberspace any more than invoking the Monroe Doctrine meant necessarily creating permanent encampments throughout the Western hemisphere. Nor should a cyber-Monroe Doctrine lead to permanent Government encampments in private networks, or become a mandate for unilateral intervention in all of cyberspace. With proper guidance, various Government agencies and the private sector can find their natural role in guarding our cyber infrastructures in a framework similar to how we currently protect our real-world interests.

To summarize:

- Technology is only a force multiplier if you pick the right technology for the intended use and intended threat environment. The Government must make security an explicit part of procurement, funding appropriately skilled staff to execute these procurement requirements while recognizing that some non-commercial requirements will incur additional costs.
- We need a skilled cadre of Government information technology professionals—both offense (in the military) and defense (throughout the entire Government).
- We need the cyber-equivalent of the Monroe Doctrine for our 21st-century information age that respects the boundaries of our shared ownership of the Nation's cyber infrastructure.

Ms. CLARKE. We thank you for your testimony.

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

STATEMENT OF JAMES A. LEWIS, PROJECT DIRECTOR, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. LEWIS. Thank you and thank you to the committee for the opportunity to testify. The new administration has a real opportunity to improve our Nation's security in cyberspace, but there are many difficult issues it has to address, and the work of this committee will be essential in helping to guide that effort.

You know, the President has directed the National Security Council to undertake a 60-day review. This review is an important step. Cyberspace, as you have heard, has become one of the central

pillars of our economy and our national security. Securing cyberspace will help enable recovery and future growth. Officials involved in the review have told me it is forward-looking, with a broad scope. It will lay out a strategic framework for the United States.

In my testimony, I would like to discuss how to assess the review. The Center for Strategic and International Studies issued a report in December on steps the next President could take. We made many recommendations and whether you like our recommendations or not, I believe strongly that we identified the right issues. Any review that does not address the issues we identified will be inadequate.

Among our recommendations there are two that I think are crucial. The first is the need for clear leadership from the White House, and the second is a comprehensive plan for moving ahead. We undertook a long discussion of who should lead the Federal cybersecurity effort. It looked at many agencies: Defense, FBI, GSA, DHS, the intelligence community. We were concerned with agency authorities and competencies, but also with the signal that a lead agency would send to the public and to the world. The United States should avoid being perceived as militarizing the internet, and it should avoid solutions that give rise to concerns over privacy and civil liberties. In the end, we decided only the White House had the necessary authority.

Clear White House leadership is essential, but it has to be accompanied by a truly strategic plan, a truly strategic plan—a truly comprehensive plan, I am sorry.

What does comprehensive mean? It means going beyond an effort to secure Government networks. It means integrating offensive and defensive strategies and looking at how to improve attribution and identity in cyberspace. It means engaging with foreign nations, something we have not done particularly well. It means accepting that the Federal Government must use its regulatory powers if we are to make any progress.

I want to emphasize the need to develop regulatory strategies, because this has been largely overlooked in previous national efforts. Regulation is necessary when market forces alone will not provide security. We were careful to note in our report that a new approach is needed, one that avoids both prescriptive regulations, but also rules, that are so diluted as to be meaningless. New regulation must be developed in partnership with the private sector, but with the Government setting the goals and ensuring compliance.

My own view is that regulation is essential if we are to give substance to public/private partnerships. Regulation gives us an opportunity to improve cybersecurity in critical infrastructure, something this committee has worked on in the past and you will be working on, I understand, in the future. The work of this committee has made a tremendous contribution. It helped guide us in writing the report. Regulation of critical infrastructure will become increasingly important. The stimulus package envisions spending on infrastructure and it will build security in. This is a good idea, but when we come to the question of what precisely needs to be done

to make new projects secure, we don't know the answer, and we don't have the time or the people to develop that answer.

A failure to invest in infrastructure modernization for almost 2 decades has made it impossible to build both quickly and securely. Smart Grid projects are an example of this. Smart Grid uses, for example, advanced meters to measure and manage the flow of electricity. These new meters are based on network technologies. Unfortunately, if the new smart meters are not secure, they can be hacked. Regulation can play a role in remedying this by giving Government the ability to mandate actions that mitigate our new vulnerabilities. But if we do not build the regulatory foundation now, the United States will be put at risk.

Let me summarize quickly. It is always difficult batting clean-up because everyone has already said everything. But we need somebody in charge at the White House who will implement a comprehensive plan. That plan has to include strategies for international engagement and for domestic regulation. Then we need to move out.

Okay. I thank the committee and look forward to your questions.

[The statement of Mr. Lewis follows:]

PREPARED STATEMENT OF JAMES A. LEWIS

MARCH 10, 2009

I thank the committee for the opportunity to testify on the Federal Cybersecurity Mission. I believe that the new administration has a real opportunity to make a significant difference in improving our Nation's security in cyberspace, but there are many difficult issues that it must address. The work of this committee will be essential for helping to guide that effort.

As you know, the President directed that the National Security Council undertake a 60-day review of the U.S. approach to cybersecurity. Federal officials involved in the review have told me that this is a forward-looking effort with a broad scope. It looks beyond securing Federal networks, which was the focus of the last administration's efforts, and will endeavor to lay out a strategic framework for the United States.

The decision to undertake this broad review is an important step forward for our Nation. Cyberspace has become one of the central pillars of our economy and our national security. The adoption of network technologies since the 1990's by the United States has been a source of both competitive advantage and the rapid growth. The digital infrastructure is now essential. More importantly, expanding our digital advantage offers the possibility for continued increases in productivity and innovation. Securing cyberspace will help enable recovery and future growth.

Reaping the full advantage of digital technologies will require real improvement in cybersecurity. Estimates of the damage to our economy are imprecise, but millions of dollars are lost each year to fraud and theft, millions of dollars worth of intellectual property lost to foreign competitors, with the total easily reaching into the billion. One of my fears is that as we increase spending on research and science as part of the stimulus package, we are actually subsidizing the research of our economic and military competitors since they can easily access work that cost us millions to develop for only a few dollars.

There is of course additional risk that insecure digital networks could allow foreign militaries and intelligence services, criminals, or other groups, to disrupt the provision of crucial services that are either provided by or depend upon digital technologies. It is easy to overstate the consequences of this sort of attack, and much of the discussion of cybersecurity over the last decade has involved some very silly and exaggerated scenarios for national disaster, but the risk is real and growing, and any national security strategy that does not address it is inadequate.

Where are we today in cyber security? From one perspective, we are in remarkably bad shape. In the last year, we have seen the networks of the two Presidential campaigns, secure networks at the U.S. Central Command and computer networks in Congress and other Federal agencies penetrated by outsiders. 2007 saw a number of significant penetrations of major Federal agencies by an unknown foreign power.

The Secretary of Defense's unclassified email was hacked. The Department of Commerce's Bureau responsible for high tech exports off-line for more than a month. The networks of the Departments of State and Energy, NASA, and other Federal agencies were penetrated and according to public reports, immense quantities of information downloaded. The networks of Federal contractors, the defense industry and other leading companies were also penetrated. Again, our statistics on this are imprecise, as companies prefer to conceal their losses or in many instances may not even be aware they have been hacked. Poor cybersecurity damages national security and drains our economy.

In response to this crisis, the Bush administration created its Comprehensive National Cybersecurity Initiative (known as CNCI). This initiative made real progress in securing Federal networks. CNCI included Einstein, a technology that monitors Federal networks for intrusion. It included the Trusted Internet Connection initiative, TIC. It looked at the question of how to use Federal procurements to improve cybersecurity in an effort know as the Federal Desktop core Configuration—FDCC. The CNCI included several other initiatives and projects, some of which were underway by the time the Bush administration ended. Overall, it was a major step forward.

However, the CNCI had several major drawbacks. It began in the last year of the Bush administration. This late start was a serious impediment and one advantage for the Obama administration is that it came into office understanding that securing cyberspace is a major strategic issue. The CNCI was highly and unnecessarily classified. A few of its elements deserved being labeled top secret, but most did not, and the difficulties that over-classification created for coordinating with the private sector and with our allies seriously impeded the Bush administration effort. Finally, and most importantly, the Comprehensive National Cybersecurity Initiative, despite its name, was not comprehensive.

This was its greatest failing. The CNCI focused on the "dot.gov" space, on Government networks, and while this is important, it is inadequate for cybersecurity. The task involves a global network largely operated by the private sector. The CNCI did not have a serious international component and it did not adequately address how to secure critical infrastructure or the "dot.com" space where most commercial activity takes place. These were serious shortcomings, and they point to crucial areas for work by the new administration.

At the same time that the previous administration began work on the CNCI, the Center for Strategic and International Studies created a commission to develop recommendations for the 44th Presidency on how to improve cybersecurity. CSIS is a nonpartisan, nonprofit research center organization headquartered in Washington, DC with more than 200 staff and a large network of affiliated experts. Its research focus is on security in a changing global environment. CSIS has been working on cybersecurity issues for many years and this work led us, in the face of the damaging events of 2007, to establish this Commission. When we began our work and for many months afterwards, we did not know of the CNCI. Officials involved in the CSNI initially declined our invitations to participate in order to preserve the initiative's secrecy.

The report produced by this commission—I note that the other private sector witnesses on this panel were members of the group—laid out a truly comprehensive approach to securing cyberspace. Thirty-eight thousand copies have been downloaded from the CSIS Web site. We were guided by the conclusions that Federal disorganization and an over-reliance on voluntary efforts had damaged our national security. To summarize our recommendations:

- Create a comprehensive national security strategy for cyberspace that uses all the tools of U.S. power in a coordinated fashion—international engagement and diplomacy; military planning and doctrine; economic policy tools; and the involvement of the intelligence and law enforcement communities.
- Publish a public doctrine for cyberspace. The President should state publicly that the cyber infrastructure of the United States is a vital asset for national security and the economy and that the United States will protect it, using all instruments of national power.
- Clarify governance and responsibility for cyber security and establish White House leadership for cybersecurity based on Presidential Strategy and Directives.
- Use regulation to set minimum standards for securing cyberspace, to ensure that the delivery of critical services can continue when we are attacked.
- Mandate strong authentication for access to critical infrastructure. Strong authentication can significantly improve defense, if it is done in a way that protects privacy and civil liberties.

- Use acquisitions policies and rule to drive security, to encourage the development and use of products and services that are secure, based on standards and guidelines developed in partnership with industry.
- Build human capital and improved technologies for securing cyberspace by expanding research, training, and education.
- Refocus and strengthen public-private partnerships and focus them on action, not information sharing. Build on the CNCI effort, as part of a larger and more transparent comprehensive effort to secure cyberspace.

It is a lengthy list, but this reflects the overarching importance of cyberspace to our Nation and the complexity of the problems involved in securing it. I believe that the issues we identified are central for improving national security and the 60-day review must address them.

Two recommendations deserve additional scrutiny in the context of the 60-day review. These are governance and regulation. We had a lengthy set of discussions in the CSIS commission on how best to organize for cyberspace. We considered many agencies for the lead role, including the Departments of Defense and Homeland Security, the FBI, the General Services Administration, and the intelligence community.

Three problems drove us to reject an agency-led approach. First, the mandate of any one agency would have to be greatly expanded to fully cover cybersecurity. Agency legal authorities differ widely and none—law enforcement, military or intelligence—are by themselves adequate for the range of cyber problems. We did not think that a super agency with broad domestic and international powers made sense. Public perception is important. Giving the intelligence community the lead in cybersecurity, although initially attractive to some of us because of the strong capabilities these agencies possess, would trigger powerful antibodies in the privacy community and the public, particularly after the experience of the previous administration's warrantless surveillance program and the struggles over FISA renewal.

The previous administration gave the Department of Homeland Security a central role in cybersecurity. We concluded that this was a mistake. While DHS has an important role to play, it lacks the competencies to deal with the range of issues involved in cybersecurity or to successfully engage in conflict with foreign militaries and intelligence services. DHS also lacks the interagency stature to direct other, more powerful agencies.

Giving DOD the lead could be interpreted as "militarizing" the internet and would likely also provoke a reaction from both the privacy and the international communities. Foreign nations track U.S. policies closely and a decision to give DOD the lead in securing cyber space would be interpreted as a decision by the United States to make military action the focus of its cyber efforts. This would not be in our interest, as we will need to build a collaborative international approach to improve security.

At the end of the discussion, we concluded that only the White House had the authority to bring many large and powerful agencies to follow a common agenda and to coordinate with each other. A successful approach to cybersecurity blends intelligence, law enforcement, military, diplomatic, and domestic regulatory functions. Coordinating these various functions can be best done from the White House. In recommending a White House lead, we emphasized that a "cyber czar" is not the right solution. The new administration went through a brief fascination with czars of various shapes and flavors for different issues; our view is that for cyber security, the overly centralized approach implied by a czar will fail. The White House and only the White House can set strategy and policy, ensure that agencies are following them and resolve agency disputes.

Regulation is the second issue that deserves extra attention. Our report concluded that the market would never deliver adequate security and the Government must establish regulatory thresholds for critical infrastructure. We proposed a new, more flexible approach to developing regulation that was based on close cooperation with industry in developing standards and an avoidance of prescriptive regulations that spell out in precise detail what companies must do.

Regulation poses a number of challenges. The United States does not need regulations that are costly to implement yet deliver little in the way of improved security. Nor does the United States need regulations that are so diluted as to be meaningless. Finding the required balance will be difficult, but if we fail to use regulation to improve our national cyber security, if we do not identify mandatory actions to secure the digital infrastructure, the Obama administration will have no more success than any of its predecessors.

The stimulus package has inadvertently complicated the issue of regulation. The package includes significant funding for infrastructure projects, such as the Smart Grid. The package envisions that spending on infrastructure will build security into

new projects. All this is good, but we then come to the question of what precisely needs to be done to make these new projects secure? Unfortunately, we do not know the answer to this and we do not have the time or people needed to develop that answer. A failure to invest in infrastructure modernization for more than a decade has makes it impossible to build both quickly and securely.

"Smart Grid" projects are an example of this problem. It uses advanced meters to measure the flow of electricity and allow it to be better managed. These new meters are based on internet technology. Unfortunately, if the new "smart" meters are not secure, they can be "hacked," taken over by attackers, and used to disrupt the delivery of electricity. The United States does not have the guidelines it needs to guide make infrastructure secure.

I am not recommending that we delay stimulus investments while we sort out the requirements for cybersecurity. The most pressing task facing the new administration is to mitigate the suffering that the recession has brought and to take the steps needed to reduce unemployment and restore growth. Infrastructure investment is an important part of this. Years of underinvestment in infrastructure have put us in this unfortunate situation. However, regulation can play a role in remedying this problem, by giving Government the ability to identify and mandate actions that mitigate new vulnerabilities. For example, a requirement that electrical companies strengthen authentication of identity on their control networks would improve security. But if we do not build the regulatory foundation now, the United States will be put at risk, and the task of laying the foundation falls squarely on the 60-day review.

Regulation can also help reshape and strengthen public-private partnerships. For more than a decade, the public dialogue has revolved around threadbare ideas on the need to defer to the private sector as it owns and operates the bulk of the critical infrastructure and on information sharing as an alternative to Government mandates. In fact, the result has been to make public-private partnership less attractive or less important. The partnership groups often serve a largely "representational" function rather than one that is oriented towards action. Companies do not have "skin in the game." Regulate them, and they will come. Regulation is the key to improving public private partnerships, particularly if these partnerships are tasked with developing and maintain the standards upon which regulation must be based.

This administration has a unique opportunity. The United States has pursued a market-led approach to cybersecurity for more than a decade. This approach is inadequate. Now is the time to identify where regulation is needed to improve cybersecurity. Our recommendation was to begin with critical infrastructure—if a service is truly critical, we should not be afraid to require action to secure it.

I began by asking where we are today in cybersecurity and answered that, from one perspective, we are in remarkably bad shape. From another perspective, however, we are at a moment of tremendous opportunity. This administration can define an integrated and comprehensive Federal approach to securing cyberspace, something no previous administration has been able to do. The complexity of the problem means that it will take much longer than 60 days to put in place the policies, structures, and regulations we will need. However, if the 60-day review can establish a clear governance structure led from the White House, if it lays out a broad plan of action for moving ahead, including the development of a comprehensive national security strategy and the use of regulatory authorities to secure critical infrastructure, and if this administration acts upon it, the review will be a success.

Ms. CLARKE. We thank you for your testimony.

I thank all of the witnesses for their testimony, and I will remind each Member that he or she will have 5 minutes to question the panel.

I will now recognize myself for questions. This first question goes to the entire panel. You all have spent a great deal of time putting together cyber recommendations for this administration. I want to express my gratitude for your work. The statements during the campaign and the decision to do a comprehensive review suggest that this administration is committed to a real change in our approach. My question is: How do we judge whether the review has been a success, and what specific things should we be looking at to determine if we are moving in the right direction?

Mr. POWNER. A couple of thoughts here. Looking at whether the review is a success, and echoing what Dr. Lewis mentioned, there have been already a fair number of very good recommendations through the CSIS report. Clearly, the experts we talked to had some additional recommendations. One, that that review needs to take into consideration those many recommendations. The other thing is looking back on this historically, even back to the mid-1980's, we really need to look at a new organization. DHS-led hasn't really cut it. Recently, an 18-sector approach where all sectors are created equal, I am not certain that that is the right approach either. Moving forward we need to look at certain things: A new organizational structure; greater prioritization; and clearly more accountability for those organizations that are in charge.

Ms. CLARKE. Anyone have anything else to add to that?

Mr. LEWIS. Well, we know what a bad plan looks like because we have lived through at least a couple of them. I think that if we were looking at this plan, we would want clear leadership, some comprehensive strategies that include both international and regulatory, that look at combining intelligence, military, law enforcement, diplomatic engagement. We would want a commitment to action. At the end of the day, if we see those three things—leadership, planning, action—we should be better off.

Ms. CLARKE. Let me then move on and direct this question to Mr. Powner. I know that the CSIS Commission met with the review team last week. Have you met with the review team yet?

Mr. POWNER. No, we have not. We are in the process of trying to get that scheduled.

Ms. CLARKE. Would you please let us know how we can help facilitate that meeting?

Mr. POWNER. We will.

Ms. CLARKE. My next question, and it is ironic because I understand that Mr. Beckstrom has joined us in the audience, and I would like to thank him for his service and express my regret for our inability to retain his talent and expertise. But late on Friday, Mr. Rod Beckstrom announced that he was resigning as Director of the National Cybersecurity Center. I think this is a loss for the community and it is unfortunate that Mr. Beckstrom's skills weren't put to good use. In his resignation letter he acknowledges the critical importance of the NSA, but said that their dominance in cybersecurity today is a bad strategy.

Can you all comment on what you agree or disagree with in these comments and what role the NSA should play alongside DHS? Mr. Charney.

Mr. CHARNEY. Yes. So there is no question that the center of technical expertise in the Government, particularly on the operational side, is within NSA. However, I agree with the comments made earlier, that at the end of the day, if you want the public to trust that the networks are being secured well and in a transparent fashion, the mission cannot reside in NSA. So I think it is really important to empower DHS to take the necessary operational role and have a relationship with NSA that captures and utilizes their technical expertise.

Ms. CLARKE. Anyone else want to comment? Okay. I am going to move on to my next question.

On March 24, this subcommittee will hold a hearing entitled "Securing the Smart Grid from Cyber Attack". We will be discussing a number of technological issues related to the new advanced metering technologies that are being developed and deployed.

But this question has to do with policy. What Federal agency is in charge of defending against the cyber attack launched by a nation-state against our electric grid and what agencies do you think should be in charge of defending against such an attack? Any thoughts on that issue?

Mr. YORAN. Ms. Chairwoman, this is an issue that we have been trying to tackle for some time, initially with a National Cyber Incident Response Working Group, co-chaired by the Department of Homeland Security, Department of Justice and the Department of Defense. It is an issue that I think is one that ought to be a key focus for Melissa Hathaway as she conducts her 60-day review, understanding exactly what the authorities are, the priorities, the technical capabilities that exist in various pockets of the Federal Government, and how they can be brought to bear most effectively so that that planning can occur before any time of crisis.

Mr. LEWIS. I was just going to add, for me the answer would be FERC or the NRC or maybe the Department of Energy. I say that because they have the relationships with the companies. They know how the stuff works. They are the people who have the regulatory authorities. The last thing you want is somebody new charging in in a crisis and saying, "I am in charge, do what I say." So I would say look at the folks who are doing this now.

One of the things that this committee has done that has been very useful is hold those regulatory agencies accountable and get them to move out a bit more smartly. I think that would be a good direction to continue.

Mr. POWNER. Chairwoman Clarke, if I can just add to your question on who is responsible for defending—and I want to make sure we are real clear on this. If it is a response—if we are answering that in terms of response I agree it is muddy. It could be various Federal agencies and entities in charge of that response, depending on the severity of the attack. But in charge of defending the grid, it is those public utility companies that own the grid.

Ms. CLARKE. Well, thank you very much. My time is up. I now recognize the Ranking Member of the subcommittee, the gentleman from California, Mr. Lungren, for questions.

Mr. LUNGREN. Thank you very much, Madam Chairwoman, and thank you all for being here. I appreciate the contributions you all have made and there are so many questions to ask. Let me just try one very, very quickly.

Dr. Lewis, you were very specific about saying that the person who should be in charge of the leader of the new comprehensive cybersecurity ought to be in the White House.

Mr. Charney, if I understand what you said, I thought you felt the DHS could be stood up to have that responsibility.

Mr. CHARNEY. Sir, to be clear, there is a difference between developing a strategy and coordinating it through the Federal agencies and the individual responsibility of the various agencies.

Mr. LUNGREN. Right.

Mr. CHARNEY. So if you are going to look at a national strategy that has to determine some very difficult questions like when is a cyber attack an act of war and what is a proportional response, those kinds of key decisions are to be done at the White House level. But you also need an operational capability, things like US–CERT, an agency to help the other agencies deploy best practices. So I view DHS as more operational of implementing the strategy, but I think strategic elements and the cross-government cooperation has to be at the White House.

Mr. LEWIS. I agree completely with that. I think if you look at the agencies, I agree completely FBI has a role, DOD has a role, DHS has a role, the intelligence——

Mr. LUNGREN. I understand they all have roles. My question has been—I think Mr. Charney responded to it and I have articulated it before, but I am concerned about a lack of urgency not only in the Congress, in the White House, in the public domain with respect to the threat, No. 1; and, No. 2, how we do it?

As we have seen DHS develop and pull itself together, I think it is actually starting to get its sea legs and frankly I think doing a far much better job today than it was 2, 3, 4, 5 years ago. That is part of what happens when you stand up an agency like that.

But there is the question of a sense of urgency. The President and his particular delegate in the White House can set the policy, but how do you make sure people follow it? We all know CIOs in the various departments and agencies have a natural protective mechanism about how it ought to be done. We understand that you have got DOD, you have got NSA, you have got the FBI and all of them, and all of them believe they have a certain respected expertise.

How do you engage that sense of urgency throughout the Federal establishment that has not been there? I am not trying to blame anybody. I am just trying to state a fact because it hasn't been there in the public either. How do we leapfrog to that position where we have that policy established at the White House on the one hand, but then we have the implementation or operational motivation and authority? Because if the various individuals responsible for the various agencies and departments think they can just kind of shrug when they get the call from the person at DHS, it doesn't drive what I want to be driven here. Mr. Yoran.

Mr. YORAN. Sir, I think that is a very important issue, when they get the call from DHS, that they have to feel a sense of urgency in getting it fixed or, more importantly, not feel like they can rely on DHS doing the monitoring, where the intelligence community is protecting them. Everybody has to feel a sense of responsibility and ultimately be held accountable for the protection of the information and the systems that they manage and need in order to accomplish their core mission. Until the Executive branch or any branch of Government holds senior leadership accountable for flaws in the security culture, lapses in security which are a result of lack of due care or negligence if you want, until there is some accountability there, I don't think we are going to see meaningful change.

Mr. LUNGREN. Let me follow up and ask a slightly different way. That is, how do we maintain those people that have the quality that can do that job, and how do we attract others to those kinds

of jobs? In other words, you can't pay them as much as the private sector can pay them. It is like when people go in the military service or do some other type of service. They do it in part because they are making a contribution, but they know their contribution is going to be utilized. It is going to be valuable. It is going to be effective.

How do we raise that level of appreciation so it is not just accountability, but it is also responsibility in the sense that it is recognized throughout the establishment, both private sector and public sector?

Ms. DAVIDSON. I believe that one of these—this is one of the issues I tried to touch upon, which is if you don't actually have a career path, you see there are people whose job it is to do information technology. Information technology will continue to be the janitorial service of many organizations where we are cleaning up other people's messes. It absolutely is critical. One of the things that we do to try to make people understand how critical it is is to, quite honestly in our own company, to go into various meetings and say, let me show that a particular tack isn't theoretical; I am going to hack your software. This is exactly how I can do this. This is exactly how I can corrupt a system.

That creates some of the awareness. It is scary but it is necessary. Either that or we wait until we get a real attack.

In terms of, you are talking about compensation trying—we do actually elevate those security professionals to give them some recognition within their jobs so they get training, they get recognition. It is recognized as a specialty that is held in esteem. As you point out, you can't always give people more money, but you can give people respect. I think you need both of those to show what is possible and to show that the, if you will, the warriors who defend it do a good job at it, and that creates the environment by which people who are able to actually do that kind of work are respected.

Mr. LUNGREN. Could I ask one real quick question, maybe for a quick response? That is, how will we enforce the new Davidson doctrine that you articulated to protect our cyberspace?

Mr. LEWIS. Let me try. All of us have worked in the Federal Government for a long time, and if you want power, there are a couple of things that give you power: Access to the President, control of the budget, control of policy. For me, the only place you are going to do that is in the White House. If I have the access to the President, control of your budget, and I can say what the policy is and know that the President or the Vice President or the National Security Adviser will back me up, I will get agencies to do whatever I want. That is what we need.

So you want to know who is going to enforce the Davidson doctrine? It is a good name for it, by the way. You know, we have to put that at the White House.

Ms. CLARKE. I now recognize Mr. Luján from New Mexico for 5 minutes.

Mr. LUJÁN. Thank you, Madam Chairwoman. I am going to just jump right into this, because there are many questions I think that need to be asked, and I am not sure if we will run out of time with doing this.

But specifically with what we are discussing today with understanding that DHS is the lead agency for the Nation's cybersecurity and the key components that exist within DHS, what are your thoughts—and I don't know if we want to start with Mr. Powner, and then I will move down the line a bit—but from the perspective of having DHS move away from their near exclusive internal focus on cybersecurity issues and more toward development and deployment of software and hardware solutions to protect critical infrastructure projects?

Mr. POWNER. We have done a lot of work with the DHS. DHS clearly is the lead cybersecurity focal point for the Nation. Even working with our critical infrastructure owners, if you look at policy and law and how that is laid out, it is pretty clear that they have not lived up to those responsibilities. So the question going forward is, do we want to keep working with them as the operational entity that is the lead or do we just designate them an operational role and put someone else in charge of primarily coordinating with the private sector, with the intelligence community, and with the military organizations? We would think the latter.

Mr. CHARNEY. I think it is really important to get the organizational structure right. Every Federal agency needs to deploy IT systems for their business operations, and therefore, every Federal agency needs a CIO and a CSO, a chief security officer, who manages security at that agency. Now, when you have a distributed organization—and certainly Microsoft is one—you end up with a lot of different, essentially business groups, that are running IT that will service their business mission, and that is fine.

The role that DHS should play in coordination with NST that sets standards for civilian agencies, and NSA because of their technical expertise, is to decide what the minimum bar is for security that should be required to be implemented by the various agencies. You know, in any environment there are things that you have to do, things that would be good to do, and best practices that you might like to deploy. Understanding what is required versus what is recommended versus what is a best practice is really important.

But I don't think you can have, for example, DHS making hardware and software decisions for the various agencies because the hardware and software that is deployed has to map to the agency mission. But DHS could say, as a requirement of deploying whatever you are going to deploy, there are certain security things that must be done: You must have a documented information security program; you must have technical controls and people controls in place to manage risk; you need an incident response plan in place because bad things will happen.

I think that is the appropriate function of DHS.

Mr. LUJÁN. Mr. Yoran, before you answer that, I think that is a perfect segue into an issue that I want to raise.

Within our New Mexico DOE and New Mexico laboratories, there is a real opportunity with the work that they are working on to improve the Nation's cybersecurity posture by bringing the resources to bear on this critical problem. So in speaking specifically to some of the IT teams that are being discussed and making sure that we have a centralized point to be able to have access, whether it is to the President or to others as we are talking about this issue, what

are your thoughts in taking advantage of the expertise that lies in some of our Nation's DOE laboratories that are working with specific issues, some which are partnered with DOD responsibilities as well?

Mr. CHARNEY. It is obviously critically important to grab expertise wherever it resides, and one of the things DHS should be doing is discovering and then propagating best practices across the Government and the private sector. So I think that would be a key thing to do.

Mr. LUJÁN. Thank you. Madam Chairwoman, if I may shift a little bit and get your perspective.

As we are moving forward with the deployment of Smart Grid, including the importance of communications and the potential threats that could exist from attacks, what is the importance of making sure that we are taking into consideration the elements and inventories across the country and making sure we have adequate protections for our critical infrastructure like electricity, renewable generation areas, and the backbone of really what will essentially be our Smart Grid?

Ms. DAVIDSON. I do think that there are entities who are looking at that in their role with the utilities. But if I could actually back up a little earlier than that, if you think of this as a supply chain, one of the things that actually needs to change that none of us touched upon, part of the reason we have these difficulties—I don't think anybody sits down and says I think I am going to deploy a system that is hopelessly insecure and will leak like a sieve. It isn't merely awareness. It is that a lot of the people who are building these at the grassroots level do not understand that they have any responsibility and they don't learn to think like an attacker. That starts with the university system.

It is not just computer science and electrical engineering, it is people who are building these control systems. If you can change one thing, if you can get the people designing and building those things to assume, think like a hacker, assume your system will be attacked, then they will design differently. They will build differently. They will deploy differently. By the time someone like a utility gets something, they will still have to ask intelligent questions in procurement, but they won't have to sit around and wonder, I wonder if anybody had a clue whether somebody is going to try to attack the power grid?

We have to move the supply chain for security-aware people all the way back into the university systems. Unfortunately, having gone to the universities—I believe Scott has as well—you get a resounding nonresponse from universities when you ask, do you teach secure coding practice in all of your engineering and control system disciplines?

Mr. LEWIS. On the question, the national labs are actually places that you could look for. Both Sandia, which has done some excellent work, also Idaho National labs, NERC, FERC, NST, Department of Energy, these are all the people who could help us make sure that Smart Grid is secure.

Ms. CLARKE. Mr. Luján, we will be covering that territory in about 2 weeks when we do our Smart Grid hearings. So this is a precursor to it.

I would like to now recognize Mr. Broun of Georgia for 5 minutes.

Mr. BROUN. Thank you, Madam Chairwoman.

First, I want to respectfully disagree with those of you all that think that the White House is the place to put central control of this problem, for the simple reason that I am disappointed that we haven't been more aggressive in our last administration, and I don't know what kind of aggressiveness we are going to have in this administration to try to solve this problem.

As I have learned more and more about it I am extremely, extremely concerned about our national security, not only from a military perspective but an economic perspective.

At home, I have utilized Koperski, I have used Norton, I have used McAfee to try to make sure that my own home computer networks are secure and have a firewall that are in place. I have just recently learned how inadequate those programs are. So I think we have to have a national effort to develop some kind of very, very strong national security and economic security type of plan.

But I think this committee and the Department of Homeland Security is the best place to do that, for the simple reason that in the administration you have personalities and different focuses and those sorts of things. I do agree we need to have a central focus, but I don't think the White House is that place. I think this committee ought to be setting policy, and not the White House frankly; and the Department of Homeland Security I think is the best way to try to coordinate things within the interagency efforts to make sure that we stay secure, whether it is DOD, Department of Energy or all the other sources as well as within the private sector.

Having said all that, I believe in the private sector, I believe in the marketplace, and I think innovation and development comes probably best in the private sector and not from governmental sources. Can the Government secure our cyberspace without private sector involvement, and how much private sector involvement do we need in that? I just throw that open to the panel.

Mr. POWNER. Well, clearly 85 percent of the cyber-critical infrastructure associated with this Nation is owned by someone other than the Federal Government. So the Federal Government can't do it. The key is partnering with them, where those private sector owners view the Federal Government as a credible partner that provides a valuable service. I think that is what has been determined with DHS with their US–CERT operations where we share threat information. The message really going forward is we in the Federal Government, whether it is DHS or whether it is the White House, they need to do a much better job where they are viewed as a credible partner in helping the private sector secure it.

Mr. YORAN. I would just add to that a little bit. I agree that centralized coordination is required. I think the Department of Homeland Security's key role can be in protecting the *dot.gov,* the Federal civilian agencies. I don't think the DHS can effectively lead sort of offensive capabilities we would need in cyber or counterintelligence capabilities we would need in cyber, nor do I think the Department of Defense would subjugate their cybersecurity efforts, which are necessary for conducting warfare today, to the Department of Homeland Security.

However, I agree with you entirely that the best thing Government can do is fund some fundamental long-term research, but ultimately rely on the private sector and commercial products for the development of IT technologies that have more security and IT security technologies that have more capability by refining their requirements and using their procurement and acquisition capabilities to drive those products and features into the commercial software versus trying to develop technologies in Government development efforts.

Mr. BROUN. My time is about up but I appreciate y'all's comments. I have got a hundred questions to ask you all and don't have the time to do that. I appreciate y'all's efforts.

I see this as a critical national security interest. In fact, just in the commercial sector, if we have an attack, which we are having every day on commercial entities, if we have an attack on our commercial entities, it can totally wreck this Nation. So I think we have got to find a solution, and I look forward to your answers that—I am going to give you all some questions in written form and and I appreciate y'all's candid answers to that.

I think we need to act and act now. Government doesn't do that very well. It is very slow in acting, and that is the reason why I want to try to get the private sector involved as much as we possibly can, because I think the private sector can be more innovative and can act quicker and can find real solutions to this. We need to have some coordinated efforts, and I think the Department of Homeland Security is the best way to do that.

Thank you, Madam Chairwoman.

Ms. CLARKE. The Chairwoman recognizes for 5 minutes the gentleman from Ohio, Mr. Austria.

Mr. AUSTRIA. Thank you, Madam Chairwoman. To our committee, thank you for your testimony today. I appreciate it very much.

I want to follow up on some of the questions that were asked earlier and more on the role of homeland security in your opinion. When you look at the jurisdiction, the electricity, the grid was brought up earlier, and you testified that you know it has fallen on the Department of Energy. Sometimes we see things intertwined between the different departments, whether it be DOD, Department of Justice. What do you see as Homeland Security's role or jurisdiction as a department? I would open that up to the entire panel.

Mr. YORAN. I think that Homeland Security's greatest impact can be summed up in three key areas. The first is in US–CERT series of programs and operations to help protect the *dot.gov,* the Federal civilian systems and agencies.

The second is in cross-critical infrastructure issues. Clearly, the Department of Energy and other regulatory bodies define security standards, measure their effectiveness, and have many levers for forcing change in the private sector.

I think the third is sort of working on issues where the failure of one critical infrastructure or the security levels in one critical infrastructure don't address the requirements of another industry, of another sector of our economy.

The third area is in interaction with the private sector through a series of well-defined public/private partnerships with specific objectives and also with value-add and incentives in the private sector for their voluntary participation.

Mr. CHARNEY. I suggest the way to think about this is separating out the horizontal from the vertical. There are a lot of things in IT that are horizontal on which all the verticals depend. So robust authentication, knowing who is connecting to your network, you need to know whether you are telecom, energy, or something else.

There are other things that are unique to vertical sectors. The energy SCADA systems may be different than phone SCADA systems. As a result of that, I think when you think of DHS' role, I view it as kind of the horizontal base security, and then the sectors and their regulatory agencies have to focus on the vertical uniqueness.

Mr. AUSTRIA. Thank you for that. That is why I do agree with you. I think we need to have clear leadership and a comprehensive strategy and a commitment to take action in those areas so that is much better defined.

Let me jump over to the public/private partnership because I do agree with you on that. I have always believed that the private sector, which designs and deploys and maintains much of our Nation's critical infrastructure is far ahead of Government in their ability to detect, to attribute, and to defend against a cyber attack.

Correct me if you think I am wrong, but isn't that, again, a reason just to follow up on some of the other questions with the public/private sector, that we really should be pursuing this to really achieve national security when it comes to cyberspace?

Mr. CHARNEY. Sir, the answer is yes. We all here I think are big fans of private sector innovation, but I will say I wrote years ago that you couldn't make a market case for the Cold War. I mean, there are certain things in national security where the markets are not designed to address the problem, because when we build products for market we know that we have a large customer base that is global and very price-sensitive. Some of things that the national security community requires is very specific and expensive.

So it has long been my view that you need a symbiotic relationship where—and I described this in my testimony—where you figure out what the market will provide, what national security needs are, and how Government can help bridge that gap. I don't think you can rely on markets alone to bridge the gap because markets aren't designed to do that any more than they are designed to protect national security and provide law enforcement mechanisms. These are things that we tax people for and make them pay for from the Government.

Ms. DAVIDSON. I do agree with Scott largely, but I also think that the Government can be a smarter buyer. Even something as simple as some transparency in procurement around what vendors do and do not do in terms of security, I don't think in many cases the questions have ever been asked. It is certainly asked at the Defense Department level or the intelligence. They want to know how you engineered your software. But the average garden-variety agency does not ask that. Why would that change things?

This is something I think, unfortunately, women can understand better than men, but I call it the bathing suit test. If you have to go out in public in June in a bathing suit, along about March you are going to put it on and you are going to say I can't believe I look like this; I better get in shape before I have to go out in public.

If people had to disclose, so to speak, their development processes related to security, you would want to look a lot better by the time you are actually filling in the form. That per se is not going to cure all our ills, but it will improve what people are buying or at least they will know what they are getting and not getting, and they can make smarter decisions as purchasers.

That will not, as Scott I think would agree with, mean that we are going to—commercial software, unless it has been necessarily engineered to the highest level of software assurance that, for example, the intelligence community could want. But even raising the baseline would be a very good start. It would save people a lot of money they are spending now, trying to patch their security and make it harder for bad guys to do what they do. Make them work harder.

Mr. AUSTRIA. I understand that my time is up. Thank you. I do agree with my colleagues that, you know, cyberspace security is critical to our national security. I have other questions that I will be glad to submit to our panel. But thank you, thank you for your time.

Ms. CLARKE. Thank you. The Chairwoman now recognizes the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Madam Chairwoman. I was listening to the testimony in the rear but I was multitasking, too.

This is basically to each panel member. With the information that you have available to you, do you think the United States is prepared for a major cyber incident?

Mr. POWNER. No, we are clearly not as prepared as we should be. I will go back, several years' work that we did for this subcommittee, I think several Congresses ago, looking at internet recovery. You can look at what happened with 9/11, Katrina, on how we recovered major portions of the internet. There were major lessons learned in that.

The question going forward, do we have—one of the requirements in our current national strategy is a joint public/private internet recovery plan if we have a major, major attack. We still don't have that plan. You need a plan. You need to exercise that plan. So I think today we are not prepared.

Mr. LEWIS. You can look at the experience of 9/11, and I hate to bring it up because it is painful, but one of our co-chairs who couldn't be here today, Harry Raduege was the Director of the Defense Communications Network. On that day, he got phone calls from all the major service providers, all the big telecom companies, all the big IT companies saying, how can we help, what can we do to restore service? I know that Dick Clarke, who was also at the White House then, got similar calls.

So you had two people, people who knew who to call, they had the existing relationships, and they knew how to do things. They

knew how to move trucks from Ohio or from Virginia to New York or to Washington to rebuild services. We don't have that today in cyberspace, and that is one of the things we desperately need.

Ms. DAVIDSON. I would like to tell a story in response, a short one. That is, in the 1920's, there was a Marine Corps colonel who realized the next war would be with Japan, and it is because of him that the Marine Corps developed amphibious warfare capability. He saw this in the 1920's, which was long before December 7, 1941. So we don't have that much time.

There are people who are sounding the warning. There are people who are trying to do things differently. We are not going to have 21 years to get it right. So we do need to act now. No, we are not prepared.

Mr. THOMPSON. Mr. Yoran.

Mr. YORAN. Sir, I would say that the nefariousness of cyber is the fact that we are experiencing the 9/11 in cyber. It just doesn't have the tremendous visibility.

For over 10 years now, for over a decade now, we have had significant incidents going on with foreign adversaries, and our national response has basically been to look the other way or occasionally have an article in the news media about it. So because there is no catastrophic visible outcome, we sort of lie in bed at night and are able to sleep, not realizing exactly how much damage is occurring. So we are not prepared.

Mr. CHARNEY. I would never go against my esteemed colleagues on this point. I would point out, however, that it is important to focus on the nature of the attack so you can figure out your strategy for defending. There are attacks against confidentiality, we have heard a lot about that, where data is taken. There are attacks against integrity where people alter critical systems or data that you rely upon. There are attacks against availability, and then the systems go down. In the availability attacks, I mean one goal is always to keep five-ninths of availability, keep the networks up. But the other part of any strategy has to be about how fast you can reconstitute the capabilities if the capabilities fail.

So this is one of the reasons it is so important to have a comprehensive strategy, because when you think about how you are going to reconstitute across multiple networks and maybe across multiple time zones, it is actually quite challenging. You have to figure out what your strategy is for reconstitution, who is in charge, roles and responsibilities, what is the interface to the private sector that owns 85 percent of this infrastructure. The availability problem is in some ways different than the confidentiality and the integrity problem. It is important to focus on all of them.

Mr. THOMPSON. Well, I would like to say, Madam Chairwoman, that what we have just heard is very troubling, I think to me and the rest of the committee, that we have some work to do. I think perhaps at our next hearing we need to bring some of the people who have the primary responsibility for the plan, or whatever we are operating under, and see if we can get some idea as to what they are doing to keep us safe. But I am real concerned about it. I would say that both the subcommittee and I as Chairman on the full committee will give this our undivided attention, and I would

look to people like yourselves to help provide the leadership, getting us where we need to be. I yield back.

Ms. CLARKE. Thank you. Member Lungren.

Mr. LUNGREN. Madam Chairwoman, I just wanted to tell you this is an outstanding panel that I thank you for putting together. I thank all of you for being here. We could go on with this for hours. Some of us will probably submit some written questions. I know we have already begged your indulgence for the time you have given us, but hopefully if you could respond to those in a timely fashion, we could maybe talk to you later, too, as well. Thank you.

Ms. CLARKE. I thank the witnesses for their valuable testimony and the Members for their questions. The Members of the subcommittee may have additional questions for the witnesses, and we will ask you to respond expeditiously in writing to those questions.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 4:04 p.m., the subcommittee was adjourned.]