COMMITTEE: House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

SUBJECT: Federal Cybersecurity Mission

DATE: Tuesday, 10 March 2009

MEMBERS: See List

WITNESSES:
Dave Powner, Director, Information Technology Management Issues, Government Accountability Office
Jim Lewis, Project Director/Director, Senior Fellow, Technology and Public Policy Program, Center For Strategic and International Studies, Lead Organizer, Csis Commission On Cybersecurity, 44th Presidency
Scott Charney, Vice President, Microsoft Trustworthy Computing Group, Co-Chair, Csis Commission on Cybersecurity
Mary Ann Davidson, Chief Security Officer, Oracle Corporation' Amit Yoran, CEO, Netwitness, Former Director, National Cybersecurity Division, Department Of Homeland Security
Amit Yoran, CEO, Netwitness, Former Director, National Cybersecurity Division, Department Of Homeland Security

---

OPENING STATEMENTS

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 of the witnesses for appearing before us today. I am pleased to chair today's hearing, my first as chair of the Emerging Threats Cybersecurity Science and 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, two years, we will continue our oversight over nuclear detection programs, radiological threats, public health threats, cybersecurity, and the science and technology directorates.

I also look forward to working in the same bipartisan spirit that the previous chairman, our 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 two 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 this subcommittee will hold this month. And it is easy to understand why this issues dominates our agenda. We relay on information technology in every aspect of our lives, from our electric grids, 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 benefits generated by our modern network world.

But in our rush to network everything, few stop to consider the security ramifications of this new world we were creating. And so we find ourselves in an extremely dangerous situation today. Too many vulnerabilities exist on too many critical networks which are exposed too many skilled attackers who can inflict too many damages to our system.

Unfortunately, to this day, too few people are even aware of these dangers and fewer still are doing anything about it.

This committee will continue to sound alarm bells, raise awareness of the problems we face, and hold those in charge accountable for their inactions. 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.

And 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 16th. The review is being conducted by Melissa Hathaway, Senior Director of the NSC on orders from President Obama and the National Security Advisor. The goal for the review is to develop a strategic framework to ensure the U.S. government 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 and the 110th Congress from the work

that our witnesses have already undertaken in this 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 two decades have seen countless reports from America's thought leaders in cybersecurity, containing hundreds of recommendations of 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 peace, 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 importantly, 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 budget for each of these different responsibilities. The CSIS Commission recommended and I fully support an assistant to the president of cyberspace securities to 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 critical infrastructure sectors, I believe this administration should seek to use a combination of regulations and incentives to assure that our electricity grids, including the Smart Grid, water facilities, financial systems, and other key infrastructures are properly secure. 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 thought on the issues I just discussed, as well as your opinion 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'd like to just take a moment to acknowledge that we've 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.

LUNGREN:
Thank you very much, Chairwoman Clarke, and thank you for the bipartisan manner in which you've approached the organization of this subcommittee, and the informal meetings that we have had. I am looking forward to meeting 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 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. And after our classified, cyber-threat briefing last week, it's 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 this is because the people wanted this to be the case, or that there was any conscious effort on the part of members of Congress, or the 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, is sometimes not what you pay attention to.

And cybersecurity which -- or 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, the refrigerator. I open up the refrigerator and all I want is cold milk. I really don't care how it works.

We have that attitude towards the cyber worlds that's embedded in everything that we do. But we can't have that attitude. I believe it's 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 our cost, and improves performance, would that the rest of our economy do as well.

However, the rapid growth of the Internet and our interconnected computers 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 felt for some time that we're playing catch up in detecting and defending against the increasing number and sophistication of today's cyber threat, whether they are of the mischievous nature, of the organized crime nature, of the nation's state nature. I agree we need a national cybersecurity strategy (ph), understanding that cyberspace can't be secured by government alone. And that's a very important point that we have to stress.

However, the government does need to reorganize and focus its national cyber efforts that 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.

There just seems to me 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 cant' catch up with this, and 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 reports a recommendation that creates three, new private -- public/private groups designed of 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 dialogue for education and discussion; and a new, cyber-operational organization.

The Bush administration recognized the growing threat to our national security from cyberspace, proposed a comprehensive, national cybersecurity initiative in 2008. The CSIS Commission came into 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. I'm 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 Chair, for the time.

CLARKE:
The chair now recognizes the chairman of the full committee on homeland security, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

THOMPSON:
Thank you very much, Madam Chairman.

Good afternoon.

I believe 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 Chair, for continuing our oversight efforts.

This is a particularly timely hearing given the recent resignation of Mr. Beckstrom as Director of 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 sectors. 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 had expertise in organization 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 -- excuse me -- 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 committee 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 the critical issue. I share the chair's optimism about the president's commitment to cybersecurity. And I hope that 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 Chair.

CLARKE:
Other members of the subcommittee are reminded that 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 Trustworthy Computing Group. Prior to Microsoft, Mr. Charney was a principal for PricewaterhouseCoopers where he led the first cyber-crime prevention and response practice. Mr. Charney also serves 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 CEO 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 CEO and adviser to Incutel (ph), 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 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 as the Defense Science Board and is a member of the CSIS Cybersecurity Commission.

Welcome, Ms. Davidson; nothing against a secretary, but you are chief security officer.

Our fifth witness is Jim Lewis, the director of the Center for Strategic and International Studies Technology and Public Policy Programs. 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 five minutes, beginning with Mr. Powner.

POWNER:
Madam Chair, Chairman Thompson, Ranking Member Lungren, and 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 this 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 capability, and addressing cyber crime.

This afternoon, I will provide a progress report of our ongoing work for you, Madam Chair, 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, has resulted in 12, specific recommendations for the new administrations to improve the approach to protecting both government systems in our nation's cyber, critical infrastructures.

I will now briefly discuss each of the 12.

Number 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. In order to contain requirements to hold responsible organizations accountable.

Number 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.

Number 3. Establish a government structure for strategy implementation. Create a governing body similar to a board of directors responsible for recording 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.

Number 4. Acknowledge we're in a cyber war with criminal and adversarial nations. Publicize the severity of prior tax and raise awareness that we're constantly under attack.

Number 5. Create or designate an accountable operational cybersecurity organization. White House led is not the silver bullet. And DHS has had the 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.

Number 6. Focus less on creating plans and more on prioritizing, assessing, and securing cyber assets. We have created many plans that will largely go unused. We need to create a prioritized list of our nation's cyber assets and work towards securing them.

Number 7. Bolster public/private partnerships by providing more incentives for private sector participation.

Number 8. Focus greater attention on the global aspects of cyberspace. We should work towards an international, global cyber strategy and use international agreements to focus cybersecurity issues and thwart cyber crimes, like the Council of Europe's Cyber Crime Convention.

Number 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.

Number 10. Better coordinate government and private sector cyber R&D. Cyber R&D is underfunded and not coordinated.

Number 11. Increase the number of skilled cyber professionals, including criminal investigators. Experts suggested that the cybersecurity discipline should be a profession that is licensed.

Number 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 Chair, many, large cyber security 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.

CLARKE:

Thank you very much.

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

CHARNEY:

Thank you, Chairwoman Clarke, 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 to the 44th presidency as 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 cyberspace security. Second, we need 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 meta-system if we're 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 communication. While the growth of the Internet in the early '90s created new, beneficial opportunities for all, including individuals, businesses, and governments, it also created unprecedented opportunities for those who would misuse technology. It permits individuals 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 the 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.

And 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 towards the clearly identified objective of securing America's network. Consistent with this philosophy, the partnership should focus on sharing information that is actionable in 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 market 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, and 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 online for businesses to interact with customers, and for government to service 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 that is 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 meta- system.

In conclusion, let me say there are complex challenges that obviously will not be solved (ph) overnight. Securing America's future in the information age depends upon creating a comprehensive, national strategy for cyberspace securities, one that simplifies, organizes, and enables effective operational partnerships among the government and private sector, and Internet citizens. There's both an opportunity and a need for leadership as we focus the nation's attention 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.

CLARKE:
I thank you for your testimony.

I'll now recognize Mr. Yoran to summarize his statement for five minutes.

YORAN:

Ms. (ph) 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. I have a lot to say. So I'll 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's 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. For intelligence operations to 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 counterintelligence insights.

The current series of cyber programs calls 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 our national cyber efforts are over-classified to the point where catastrophic consequences are highly probable. High levels of classification prevent the sharing of information necessary to adequately defend our systems from inside (ph) IP addresses when classified cannot be loaded into defensive monitoring systems. It also creates insurmountable hurdles when working with a broad range of government IT staff that do not have appropriate clearances let alone when trying to work with, communicate, and partner with the private sector.

Classification not 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 terrorists surveillance program is that such a limited review can lead to ineffective legal vetting of a program.

The cyber mission cannot be plagued by the same flaws as the TSP. And immediate, thorough, and transparent legal analysis of the government's authorities, 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 non-existent 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 efforts have been made, administrative incompetence and political infighting have squandered meaningful advancements for years now 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, 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, but also conceded the private sector too cannot succeed in its defensive mission and subjugate them to intelligence support. DHS is a natural and appropriate place for public/private partnership in 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 incentive 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, instant response support, to name just a few.

Trust relationships, when dealing in cybersecurity matters are absolutely critical. In discussions among privacy and civil liberties groups, 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. Such 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 and 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 authority to address security concerns in (ph) civil systems to include the ability to measure compliance with security standards, protocols, and practices, and take deceive action where organizations are not applying reasonable standards of care. At present, the operations cybersecurity home is DHS. The US-CERT remains politically torn part into three components completely subjugated through a cadre of detailees from the intelligence community. In order to regain efficiency, the department's operational security activities must be reconsolidated in US-CERT. this operational mission does (ph) not resource to succeed with less than 20 government FTEs and a budget of only $67 million.

CLARKE:
Mr. Yoran, I'm just going to ask if you could summarize. And we'll probably pick up some more of your testimony through questions. And of course, we have your full testimony in the record.

YORAN:
Yes, Ms. (ph) Chairwoman.

The --let's see -- the U.S. (inaudible) directed to the Secretary of DHS just as then talk reports to the Director of NSA and 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.

CLARKE:
Thank you as well for your testimony.

And now, recognize Ms. Davidson to summarize her statement for five minutes.

DAVIDSON:
Chairwoman (inaudible), Chairwoman Clarke, members of the subcommittee, my name is Mary Ann Davidson. I'm the 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 this statement should be self evident, but it isn't, and therein lies the risk to our freedom.

The ubiquity, fluxility, and configurability of information systems has led to circumstances in which software design for particular purpose and environment is too often deployed in the environment and we've 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 is the Air Force purchase Gulfstream (inaudible) and try to configure them as F-22 Raptors. While there's nothing wrong with container ships or Gulfstream Spies (ph), they were not designed for the operational needs or the threat environment that aircraft carriers or 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 IT backbone. In particular, our homeland security and our military's ability to prosecute ware 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 battle space. This make 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 system defensively.

Absent this capability, the DOD will not be able to use IT as a 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. Net-centric armies stop without supplies of information. Only by holding capability for both function and its theme can offensive form 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 system 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're in one. The second is that nobody wins on defense. And 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 offline 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 and response in foreign aggression is a point Melissa Hathaway as specifically noted during her review in 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 states in the Americas, the western hemisphere, would be viewed by the U.S. as acts of aggression, and the U.S. would intervene. The Monroe Doctrine is one of our longest standing foreign policy tenants (ph) and broke down multiple occasions by multiple presidents. And we have, as the saying 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 map 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.

Not that the Monroe Doctrine did not detail the same intervention or even specific intervention for each perceived act of aggression. It 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 U.S. has cyber turf. And the second is, we will defend our turf. We need to do both now.

Thank you. And I look forward to your questions.

CLARKE:
We thank you for your testimony.

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

LEWIS:
Thank you and thank you for 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 enough 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've 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's forward- looking with a broad scope. It will lay out a strategic framework for the United States.

In my testimony, I'd like to discuss how to access the review.

The Center for Strategic International Studies issued a report in December on steps the next president could take. We made many recommendations. And whether or not you like our recommendations or not, I believe strongly that we identified the right issues. And 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 the comprehensive plan for moving ahead.

We undertook a long discussion of who should lead the federal cybersecurity effort. We 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 U.S. should avoid being perceived as militarizing the Internet and it should avoid solutions that give rise to concerns over privacy and civil liberties. And 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 comprehensive plan -- I'm sorry.

What does comprehensive mean? It means going beyond the effort to secure government networks. It means integrating offensive and defensive strategies, and looking how to improve attribution and identity in cyberspace. It means engaging with foreign nations, something we have not done particularly well. And 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 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'll be working on, I understand, in the future.

The work of this committee has made a tremendous contribution and it helps 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 the answer.

A failure to invest in infrastructure modernization for almost two decades has made it impossible to build both quickly and securely. Smart Grid projects are an example of this. Smart Grid uses, for examples, 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 U.S. will be put at risk.

Let me summarize quickly, it's always difficult batting cleanup because everyone's 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 regulations. And then we need to move out.

OK, I thank the committee and look forward to your questions.

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 five minutes to question the panel.

I will now recognize myself for questions. And this first questions goes the entire panel. You all have spent a great deal of time putting together cyber recommendations for this administration. And I want to express my gratitude for your work. The statements during the campaign and the decision to do a comprehensive review suggested 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 thing should we be looking at to determine if we're moving in the right direction?

You all don't have to jump in a one time.

(UNKNOWN)
A couple of thoughts here looking at whether the review is a success in echoing what Dr. Lewis mentioned. There have been already a fair number of very good recommendations through the CSIS report. Clearly, the experts that we talked to had some additional recommendations. One, that review needs to take into consideration those many recommendations.

The other thing is looking back on this historically, even back to the mid-1980s. We really need to look at a new organization. DHS- led hasn't really cut it recently. And 18-sector approach where all sectors are created equal. I'm not certain that that's the right approach either. And though looking forward, we need to look at certain things. An new organizational structure, greater prioritization, and clearly, more accountability for those organizations that are in charge.

CLARKE:

Anyone have anything else to add to that?

(UNKNOWN)
Well, we know what a bad plan looks like because we've lived through at least a couple of them. And I think that that if we're looking at this plan, we'd want clear leadership, some comprehensive strategies that include both international and regulatory that look at combining intelligence, military, law enforcement, diplomatic engagement. And we 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.

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?

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

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

POWNER:
We will.

CLARKE:
My next question -- and it's ironic because I understand that Mr. Beckstrom has joined us in the audience, but -- and I'd 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. Rob 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 the 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?

CHARNEY:
Yes. So there's no question that the center of technical expertise in the government, particularly on the operational side within NSA, I would agree with the comments made earlier that at the end of the day, if you want the public trust that the networks are being secured well in a transparent fashion, the mission cannot reside in NSA. And 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.

CLARKE:
Anyone else want to comment?

OK. I'm going to move on to my next question. On March 24th, this subcommittee will hold a hearing entitled, "Securing the Smart Grid from Cyber Attacks." We'll 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 a 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?

(UNKNOWN)
Ms. Chairwoman, this is an issue we've been trying to take 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. And it's an issue that I think is one that ought to be a key focus for Melissa Hathaway as she conducts her 60-day review, understand 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 planning can occur before a time of crisis.

(UNKNOWN)
I would just add that, you know, for me, the answer would be FRC (ph), you know, or the NRC, or maybe the Department of Energy. And I say that because they have the relationships with the companies. They know how the stuff works. They're the people who have the regulatory authorities. And the last thing you want is somebody new charging in in a crisis and yelling I'm in charge. Do what I say.

So I would say, look at the folks who are doing this now. One of things 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.

(UNKNOWN)
Chairwoman Clarke, if I can just add. Your question on who's responsible for defending, and I want to make sure we're real clear on this, if it's a response, if we're answering that in terms of response, I agree that I think it's muddied and 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.

CLARKE:
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.

LUNGREN:
Thank you very much, Madam Chair. And thank you all for being here. I appreciate the contributions you've all 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 League of the New Comprehensive Cybersecurity Program ought to be in the White House. Mr. Charney, if I understand what you said, I thought you felt that the DHS could be stood up to have that responsibility.

CHARNEY:
To be clear, there's a difference between developing the strategy and coordinating it through the federal agencies.

LUNGREN:
Right.

CHARNEY:
And the individual responsibility of the various agencies.

LUNGREN:
Right.

CHARNEY:

So if you're going to look at a national strategy, it has to determine some very difficult questions, like when is a cyber attack an act of war? And what's a proportional response? Those kinds of key decisions have 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. And so, I view DHS as more operational, of implementing the strategy, but I think the strategic elements and the cross-government cooperation has to be at the White House.

LUNGREN:
Dr. Lewis?

LEWIS:
(Inaudible) -- I'm sorry.

I agree completely. FBI had a role. DOD has a role. DHS has a role. The intelligence...

LUNGREN:
I understand they all have roles. My question has been, I think, Mr. Charney responded to it. And I have articulated this before, but I'm concerned about a lack of urgency, not only in the Congress, in the White House, in the public domain with respect to the threat, number 1, and number 2, how we do it.

And as we've seen, DHS develop and pull itself together, I think it's actually starting to get its sea legs, and frankly, I think doing a far much better job today than it was two, three, four, five years ago, and that's 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 a policy. But how do you make sure people follow it? And 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've got DOD. You've got NSA. You've got the FBI on all of them. And all of them believe they have a certain respected expertise. But how do you engage that sense of urgency throughout the federal establishment that has not been there? And I'm not trying to blame anybody. I'm just trying to state a fact, because it hasn't been there with the public either.

And how do we leapfrog to that position where we have that policy established at the White House on one end? But then we have the implementation or operational motivation and authority. Because if the various individuals responsible for the various agency departments think they can just kind of shrug when they get the call from the person at DHS, that doesn't drive what I want to be driven here.

Mr. Yoran?

YORAN:
(Inaudible), I think there's a -- that's 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 or the intelligence community 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.

And until the executive branch holds or any branch of government holds senior leadership accountable for flaws in security culture, lapses in security which are a result of, you know, lack of due care or negligence, if you will, until there's some accountability there, I don't think we're going to see meaningful...

LUNGREN:
Let me follow up and ask in a slightly different way. And that is, how do we attract -- how do we maintain those people who are of the quality to 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's like when people go into the military service or do some other type of service, they do it in part because they're making a contribution. But they know their contribution is going to be utilized. It's going to be valuable. It's going to be effective. How do we raise that level of appreciation so it's not just accountability, but it's also responsibility in the sense that it is recognized throughout the establishment, both private sector and public sector?

DAVIDSON:
I believe that one of the -- this is one of the issues that I try to touch upon, which is, if you don't actually have a career path who say 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're cleaning up other people's messes. It absolutely is critical.

And one of the things that we, you know, we do to try to make people understand how critical it is, is quite honestly, in our own company, to go into various meetings and say, well, let me show you that a particular attack isn't theoretical, I'm going to hack your software. This is exactly how I can do this. This is exactly how I can corrupt the system. That creates some of the awareness. It's scary, but it's necessary. Either that, or we wait until we get a real attack.

In terms of, you're 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's held in esteem. As you point out, you can't always give people more money, but you can give people respect. And 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 are able to actually do that kind of work are respected.

LUNGREN:
Could I ask just one, real quick question, maybe for a quick response?

That is, how would we enforce the new Davidson Doctrine that you articulated to protect our cyberspace? I'm serious.

(UNKNOWN)
Let me try. Look, a lot of us have worked in the federal government for a long time, and if you want power, there's a couple of things that give you power. Access to the president, control of the budget, control of policy. And for me, the only place you're going to do that is in the White House. If I have 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 advisor will back me up, I will get agencies to do whatever I want. And that's what we need.

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

CLARKE:
I now recognize Mr. Lujan from New Mexico.

LUJAN:
Thanks, Madam Chair.

CLARKE:
You have five minutes.

LUJAN:
Thank you, Madam Chairman.

I'm just going to jump right into this because there are many questions that I think need to be asked. And I'm not sure if we run out of time with doing this.

But, specifically from with what we're 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'll 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?

POWNER:

We've done a lot of work looking at DHS. And DHS is clearly specified as the lead cybersecurity focal point from the nation, even working with our critical infrastructure owners. If you look at policy and law, and how that's laid out.

It's 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's the lead, or we just designate them an operational role and put someone else in charge of the primarily coordinating with the private sector with the intelligence community and with the military organizations?

We would think the latter.

(UNKNOWN)
I think it's 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, chief security officer, to manage the security of 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 to service their business mission. And that's fine.

The role that the DHS should play in coordination with (inaudible), 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. And understanding what's required versus what's recommended versus what's our 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's deployed has to map to the agency mission. But DHS could say, as a requirement of the deploying whatever you're 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.

And I think that is the appropriate function of DHS.

LUJAN:
Thank you, Mr. Charney (ph). Before you answer that, I think that's a perfect segue into just an issue I want to raise. Within our -- New Mexico DOE, New Mexico laboratories, there's a real opportunity with the work that they're 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's the president or to others as we're talking about this issue, what are your thoughts in taking advantage of the expertise that relies on some of our nations' DOE laboratories that are working these specific issues, some of which are partnered with DOD responsibilities as well?

(UNKNOWN)
It's obviously critical and important, critically important to grab expertise wherever it resides. And one of the things DHS should be doing is discovering and propagating best practices across the government and the private sector. So I think that would be a key thing to do.

LUJAN:
And, Madam Chair, I'm planning to share a little bit and get your perspective. As we're moving forward with the deployment of Smart Grid, including the importance of communications and the potential threats that could exist from attacks, what's the importance of making sure that we're taking into consideration the elements and inventories across the country and making sure we have adequate protections for critical infrastructure like electricity, renewable generation areas, and the backbone of really will be essentially our Smart Grid?

DAVIDSON:
I do think these are entities who are looking 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'm going to deploy a system that's hopelessly insecure and will leak like a sieve.

It isn't merely awareness. It's a lot of the people who are building these at the grass roots level who do not understand that they have any responsibility and they don't learn to think like an attacker. That's starts at the university system. And as much as computer science and electrical engineering, it's people who are building these control systems.

If you could change one thing, if you could get the people to 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. And by the time someone like the utility gets something, they won't -- 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 someone is going to try to attack a power grid.

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

(UNKNOWN)
Let me -- oh, I'm sorry. Good. On the question, the national labs are actually places you could look for both Sandia which has done some excellent work and also IDO (ph) National Labs. NERC, FRC, NIST, Department of Energy. These are all the people who could help us make sure that Smart Grid is secure.

CLARKE:
Mr. Lujan, we'll be covering that territory in about two weeks when we do our Smart Grid hearing. So just a precursor to it.

I'd like to now recognize Mr. Brown of Georgia for five minutes?

BROWN:
That you, Madam Chairman.

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'm disappointed that we haven't been more aggressive in our last administration. And I don't know what kind of aggressiveness we're going to have in this administration to try to solve this problem.

As I learned more and more about it, I'm extremely, extremely concerned about our national security, not only from a military perspective, but an economic perspective. At home, I have utilized Kaparsky, I've use Norton, I've used McAfee to try to just make sure that my own home computer networks are secure and have a firewall there in place. And I've just recently learned how inadequate those programs are.

And so I think we have to have a national effort to develop some kind of very, very strong natural 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 these sorts of things.

I do agree we need to have a central focus. But I don't think the White House is that place. And 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's 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 form governmental sources. Can the government secure our cyberspace without private sector involvement? And how much private sector involvement do we need in that?

I'll just throw that open to the panel.

(UNKNOWN)
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's what was intended 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's DHS or whether it's the White House, they need to do a much better job where they're viewed as a credible partner in helping the private sector secure.

(UNKNOWN)
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 .gov, the federal civilian agencies. I don't think DHS can effectively lead sort of offensive capabilities we would need in cyber and counter- intelligence capabilities we would need in cyber. What I think the Department of Defense would subjugate their cybersecurity efforts to -- 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 on commercial products for the development of IT technology that have more security capability, and IT security technologies that have more capability by refining their requirement in using their procurement and acquisition capabilities to drive those products and features into the commercial software versus trying to development technologies, government -- in government development efforts.

BROWN:
My time's about up and I appreciate you all's time. I've got 100 questions to ask you all. I don't have the time to that. I appreciate you all's efforts.

I see this as a critical, national security interest. In fact, if 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've got to find a solution now.

I look forward to your answers that I'm going to give you some questions in written form. I appreciate you all's candid answers to them.

But I think we need to act and we need to act now. Government doesn't do that very well. It's just very slow in acting, and that's reason 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. It can act quicker

and find real solutions to this. And 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 Chairman.

CLARKE:
The chair recognizes for five minutes, the gentleman from Ohio, Mr. Austria.

AUSTRIA:
(OFF-MIKE)

I'll get it right. Thank you, Madam Chair and 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 one of the role of homeland security in your opinion. And when you look at the jurisdiction, you know, the electricity, the grid was brought up earlier, and you testified that, you know, fall under 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? And I'd open that up to the entire panel.

(UNKNOWN)
I think the Homeland Security's greatest impact can be summed up in three, key areas.

The first is in the US-CERT series of programs and operations to help protect the .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 can -- and have many levers for forcing change in the private sector.

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

(UNKNOWN)
And 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 which all the verticals depend. So robust authentication, knowing who's connecting to your network, you need to know that whether you're telecom, energy, or something else.

There are other things that are unique to vertical sectors. The energy skate (ph) assistance, they'd be different than phone skate (ph) systems. As a result of that, I think when you think about DHS's role, I view it as kind of the horizontal based security. And then the sectors and their regulatory agencies have to focus on the vertical uniqueness.

AUSTRIA:
And thanks for that. And that's 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. And I've 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 cyber attacks. And correct me if you think I'm wrong, but you know, isn't that again, reason just to follow up on what some of the other questions with the public/private sector that we really should be pursuing this to really achieve security, national security when it comes to cyberspace?

(UNKNOWN)
The answer is yes. You know, we're all here, I think, 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 built products for the market, we know that we have a large customer base that's global, and very price-sensitive.

And some of things the national security community requires is very specific and expensive. And 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 need's are, and how government can help bridge that gap.

I don't think can rely on markets alone to bridge the gap because markets aren't designed to do that any more than they're 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.

DAVIDSON:
I do agree with Scott largely, but I also think that the government can be a smarter buyer. And even in 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 question's ever been asked. It's 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. And you have to go out in public in June in a bathing suit. Along about March, you're going to put it on and you're going to say, I can't believe I look like this. I better get in shape before I have to go out in public. And if people had to disclose, so to speak, their development processes related to security, you'd want to look a lot better by the time you're actually filling in the form.

That per se in not going to cure all our ills. But it will improve what people are buying, or at least, they'll know what they're getting and not getting. And they can make smarter decisions as purchasers that will not, as Scott, I think will agree with, mean that we're going to commercial software unless it's 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're spending now trying to patch their way to security and it would make it harder for bad guys to do what they do. Make them work harder.

AUSTIRA:
Madam Chair, my time's up. But thank you. I, too, agree with my colleague that, you know, cyberspace security is critical to our national security. And I have other questions that I'll be glad to submit to our panel. But thank you for your -- thank you for your time.

CLARKE:
Thank you.

The chair now recognizes the chairman of the full committee, the gentleman from Mississippi, Mr. Thompson.

THOMPSON:
Thank you very much, Madam Chair. And I was listing to the testimony in the rear, but I was multi-tasking too.

And this is basically to each panel member. With the information that you have available to you, do you think the U.S. is prepared for a major cyber incident?

(UNKNOWN)
No. We're clearly not as prepared as we should be.

I'll go back several years' work that we did for this subcommittee. I think several congresses ago, looking at Internet recovery. And 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. And 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 we're not prepared.

(UNKNOWN)
You can look at the experience of 9/11 and I hate to bring it up, because it's painful. But one of our co-chairs who couldn't be here today, Harry Raduege, who 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 Clark (ph), who was also at the White House, got similar calls. So you had two people, people who knew to call. They had the existing relationships. And they knew how to do things. They know how to move trucks from Ohio or from Virginia to New York or to Washington, to rebuild services. And we don't have that today in cyberspace.

And that's one of the things we desperately need.

DAVIDSON:
I'd like to tell a story in response, a short one. And that is, in the 1920s, there was a Marine Corps Colonel who realized the next war to be with Japan. And it is because of him that the Marine Corps developed amphibious warfare capabilities. He saw this in the 1920s, which was long before December 7th, 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're not going to have 21 years to get it right. So we do need to act now.

And, no, we are not prepared.

THOMPSON:
Mr. Yoran?

YORAN:
Some 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've 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's no catastrophic, visible outcome, we sort of (inaudible) not realizing exactly how much damage is occurring.

We're not prepared.

(UNKNOWN)
I would never go against my esteemed colleagues on this point. I would point out however, that it's important to focus on the nature of the attack so you can figure out your strategy for defending.

There are attacks against confidentiality. We've read a lot about those where data is taken. There are attacks against integrity where people, all the critical systems are data that you relay upon. And there are attacks against availability. And then the systems go down.

And in the availability attacks, I mean, one goal is always to keep five nines (ph) of availability, keep the networks up. But the other part of any strategy is it has to be how fast you can reconstitute the capabilities if the capabilities fail.

And so, this is one of the reasons it's so important to have a comprehensive strategy. Because when you think about how you're going to reconstitute across multiple networks and maybe across multiple time zones, it's actually quite challenging. And you have to figure out what your strategy is for reconstitution, who's in charge, roles and responsibilities, what's 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 integrity problems. It's important to focus on all of those.

THOMPSON:
Well, I'd like to say, Madam Chair, that what we've just heard is very troubling, I think to me and the rest of the committee, that we have some work to do. And I think perhaps, our next hearing, we need to bring some of the people who have the primary responsibility for the playing hand or whatever we're operating under and see if we can get some ideas to what they are doing to keep us safe.

But I'm really concerned about it. And I would say that both the subcommittee and as chair of the full committee, will give this our undivided attention and would look to people like yourselves to help provide the leadership getting us where we need to be.

I yield back.

CLARKE:
Thank you.

Member Lungren?

LUNGREN:
Madam Chair, I just want to tell you this is an outstanding panel. I thank you for putting it together. I thank all of you for being here.

We could go on this for hours. Some of us will probably submit some written questions. And I know we've already begged your indulgence for the time you've 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.

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.

List of Members
REP. YVETTE D. CLARKE, D-N.Y. CHAIRWOMAN
REP. LORETTA SANCHEZ, D-CALIF.
REP. LAURA RICHARDSON, D-CALIF.
REP. BEN LUJAN, D-N.M.
REP. MARY JO KILROY, D-OHIO
REP. BENNIE THOMPSON, D-MISS. EX OFFICIO
REP. DAN LUNGREN, R-CALIF. RANKING MEMBER
REP. STEVE AUSTRIA, R-OHIO
REP. PETER T. KING, R-N.Y. EX OFFICIO