DRAFT LEGISLATIVE PROPOSAL ON CYBERSECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

DECEMBER 6, 2011

Serial No. 112–61

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

74–646 PDF WASHINGTON : 2012

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

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

DANIEL E. LUNGREN, California, *Chairman*

MICHAEL T. MCCAUL, Texas
TIM WALBERG, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
BILLY LONG, Missouri
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

COLEY C. O'BRIEN, *Staff Director*
ZACHARY D. HARRIS, *Subcommittee Clerk*
CHRIS SCHEPIS, *Minority Senior Professional Staff Member*

CONTENTS

DRAFT LEGISLATIVE PROPOSAL ON CYBERSECURITY

Tuesday, December 6, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:15 a.m., in Room 311, Cannon House Office Building, Hon. Daniel E. Lungren [Chairman of the subcommittee] presiding.

Present: Representatives Lungren, McCaul, Walberg, Meehan, Long, King (ex officio), Clarke, Richardson, Richmond, Keating, and Thompson (ex officio).

Mr. LUNGREN. The Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. We have been advised by top staff on the subcommittee that we may proceed. Ms. Clarke, unfortunately, is caught in traffic, which I think a lot of people are this morning, but we will proceed.

The subcommittee is meeting today to examine the committee's "Draft Legislative Proposal on Cybersecurity." The draft legislation was distributed with the hearing notice, although the draft was circulated with Members of the other side of the aisle, I believe, in August, and there have been very few changes made since that time. I would ask other Members if they wish at the conclusion of this hearing to co-sponsor the draft before us. We intend to drop this immediately so that we can begin the process moving this forward.

Top Government intelligence and military leaders point to cybersecurity as the issue that worries them the most, primarily because it touches every aspect of American life, including our military operations. Tomorrow is December 7, the date recalled by CIA Director Leon Panetta in recent testimony before Congress about his fear of a cyber Pearl Harbor. The growing connectivity between information systems, the internet, and our critical infrastructure creates opportunities for attackers to disrupt telecommunications, electric power, energy pipelines, and our financial networks. We hear every day that cyber attacks are escalating around the world, but particularly here in the United States where extensive digital networks' information systems provide a rich target for thieves and rogue nations. Disgruntled employees, hackers, even foreign governments, "are knocking on the door of these systems and there have been intrusions." There has been a 40 percent spike in

cyberthreats to Government networks in the last year alone, as reported. The Commerce Department estimates that the theft of intellectual property, most stolen via electronic means, costs $250 billion annually and eliminates approximately 750,000 U.S. jobs.

Cybertheft, unfortunately, is no longer our only concern. The Stuxnet virus demonstrates the offensive capability to attack and incapacitate critical infrastructure. This presents a more immediate destructive threat, a digital warhead delivered through the internet. Cybersecurity is now recognized as a critical component of our National economic and National security. Failure to improve our cyberdefenses will expose our intellectual property to continued theft and damage to our critical infrastructure, putting in jeopardy our future economic prosperity. Congress needs to act to improve our cyberdefenses by designating the responsible agency and Government to coordinate defense of the Government networks.

We agree with the administration that the Department of Homeland Security is the appropriate agency to lead this effort and protect our critical information infrastructure, and our bill codifies DHS' cyber roles and responsibilities. Further, we need to improve our ability to assess cyber risks and strengthen cyber standards, generally with help from NIST. We should also encourage existing regulators to improve the cyber standards for the most critical infrastructure within their purview. The cyberthreat must be addressed in partnership with the private sector which owns, as we know, most of the country's critical infrastructure. This will require establishing a true, trusted partnership between Government and the private sector. Our objective is to create a partnership of equals designed to facilitate the exchange of cyber information and intelligence, thereby to accelerate cyberthreat identification and remedies. This trusted partnership under our bill will be known as the National information-sharing organization.

These changes proposed in our legislation are within our committee's jurisdiction and will, we believe, enhance cybersecurity of our critical information infrastructure. Today's hearing will afford our private sector partners another opportunity to weigh in on our approach to protecting critical information infrastructure from this escalating cyberthreat.

We look forward to hearing your comments. I now would recognize the Ranking Member of our subcommittee, the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman, and thank you for bringing your proposed legislation to our subcommittee. I appreciate the diligence that our witnesses have shown in analysis of the legislation and want to particularly thank Mr. Kosar for his scholarly work and quick turnaround. From my perspective, the Department must have sufficient authority to make sure that Government and privately-owned critical infrastructure install and monitor ample protection for their cyber systems, both agency-wide in the Federal Government and for identified critical infrastructure that supports the economic, social, and security needs of our Nation. Effective implementation of that authority will enable DHS to lead by example a prerequisite for building credibility and trust with privately-owned critical infrastructure.

In H.R. 174, the Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, introduced by Mr. Thompson in January of this year, and which I co-sponsor, the Department is specifically given major cybersecurity responsibility and includes a plan to oversee cybersecurity efforts for identified critical infrastructure, much like we already do in the CFATS program, which I think is a prudent risk-based approach.

The draft legislation we have before us includes an emphasis on voluntary incentives for private companies with some narrowly-targeted regulation for critical infrastructure industries that are already highly regulated. I think we are all looking for a way not to have regulation that duplicates what is already being done. Government can ask the critical infrastructure systems to improve security only if Government is a model leading by example.

Mr. Chairman, I am glad to see the language of the discussion draft does provide some provisions that are broadly similar to provisions in H.R. 174 and the White House cyber proposal. For example, by increasing the responsibilities of the Department for cybersecurity in Federal agencies and critical infrastructure, authorizing US–CERT, addressing supply chain vulnerabilities, increasing cyber R&D, and providing enhanced personnel authorities to improve the cybersecurity workforce.

My concern is two-fold. How can we realistically increase our cybersecurity efforts if the House appropriations drastically-reduced level of funding is implemented? Second, the discussion draft relies on purely voluntary actions and establishes a non-profit quasi-Governmental entity, the National Information-Sharing Organization, with private and public sector members, for the purposes of facilitating information exchange, performing collaborative cybersecurity R&D, and encouraging non-Federal use of voluntary cybersecurity standards.

I think it is important that we look closely at the details of this quasi-Governmental entity to explore the real-life implications of such a body and its actions, and how it would affect the Department's ability to enhance cybersecurity for our Government agencies, our crucial critical infrastructure, and ultimately for our citizens.

So thank you again, Mr. Chairman. These are issues that I am anxious to learn more about, and I look forward to the testimony today, and I yield back.

Mr. LUNGREN. I thank the gentlelady. Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have a very distinguished panel of witnesses before us today on this very important topic.

Dr. Greg Shannon is the chief scientist for the CERT Program at Carnegie Mellon University Software Engineering Institute. In this role he works with CERT management and staff to establish and enhance the program's research visibility, initiatives, strategies and policies. Prior to joining CERT, Dr. Shannon was the chief scientist at two startups where he worked on insider threats, the science of cybersecurity and statistical anomaly detection.

Ms. Cheri McGuire serves as the vice president of Global Government Affairs and Cybersecurity Policy, where she leads a global

team focused on cybersecurity, data integrity, and privacy issues. She works extensively with industry and Government, including serving as chair of the IT Sector Coordinating Council. That is one of the 18 critical sectors identified by the President and DHS to work with the Government on critical infrastructure, protection, and cybersecurity matters. Prior to joining Symantec in 2010, she served as director for critical infrastructure and cybersecurity in Microsoft's trustworthy computing group.

Mr. Gregory Nojeim is senior counsel at the Center for Democracy and Technology, or CDT. In this capacity he conducts much of CDT's work in the areas of National security, terrorism, and Fourth Amendment protection. Prior to joining CDT in May 2007, he was legislative counsel of the American Civil Liberties Union and for 7 years was the associate director and chief legislative counsel of the ACLU's Washington legislative office.

Dr. Kevin Kosar is an Analyst in American National Government for the Congressional Research Service where he has served since 2003. CRS' research portfolio includes Congressionally-chartered organizations, the U.S. Postal Service classified information policy, Government communications and privatization, all obviously non-controversial areas. He previously testified before Congress in April 2010, before the House Oversight and Government Reform Committee, regarding the U.S. Postal Service's financial condition. A contributing editor at Public Administration Review Journal, Dr. Kosar received his Ph.D. in politics from New York University.

As you all know, your printed texts will be made a part of the record in their entirety. You are each recognized for 5 minutes to give us a summary of your testimony, and at the conclusion of which we will go in order for questions.

So the Chairman will recognize Dr. Shannon to testify.

STATEMENT OF GREGORY E. SHANNON, CHIEF SCIENTIST FOR COMPUTER EMERGENCY READINESS TEAM, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY

Mr. SHANNON. Thank you Chairman Lungren, Ranking Member Clarke, and subcommittee Members. I am honored to testify before you again now on this important legislation. I am the chief scientist for the CERT cybersecurity program at the Software Engineering Institute which is a DOD FFRDEC, operated by Carnegie Mellon. The CERT Program's Associated Coordination Center was created in 1988 in response to the moratorium incident, and we have grown into a National asset in cybersecurity with 250 staff supporting the cybersecurity needs of the DOD, DHS, and others. CERT has been and continues to be a key partner with US–CERT in its important work.

As we talk today about the draft legislation and in particular the concept of a National Information-Sharing Organization, or NISO, please consider the role of trust in sharing sensitive information, especially the process of establishing trust. Consider for a moment, if you will, your own personal experience in trusting—consider for a moment, if you will, your own personal experience in trusted sharing of sensitive information with an organization such as your last visit to the doctor, a parent-teacher conference, or the voting booth. Your willingness to share sensitive information was prob-

ably driven by the degree to which you trusted that organization and derived benefit from that organization. That trust took time to establish and is expressed in cultural norms, laws, relationships, processes, et cetera. That trust wasn't legislated, though it often is assisted by a legislation. So it is likewise with sensitive cybersecurity information provided by private entities to a NISO.

I appreciate the frustrations with the current range and pace of information sharing. We all wish for more, better, sooner. Our view is that DHS is making great progress and this legislation should augment that work. I endorse the committee's proposal to establish a non-profit private entity to serve as a National clearinghouse for the exchange of cyberthreat information. We believe that a third-party, honest broker facilitator for the disclosure and dissemination of cybersecurity knowledge creates an excellent environment where all participants, both Government and non-Government, almost readily share sensitive information. Like with the conflict of a working group, trusted relationships are a critical success factor for NISO and reliable trust takes time to establish, especially that scale.

The type of information that organizations are being asked to share with each other in the U.S. Government is sensitive, and sharing such information requires trusted relationships established and tested over time.

Another critical success factor is data value, in addition to protections and policy that we discuss in our testimony. The data information and knowledge that the NISO collects and shares must be distinct and not readily available; else there is little or no incentive to participate. Value results from not only access to unique data but also from analysis that enables reactive and proactive responses by participants. Like the CDC, the Centers for Disease Control, the NISO must have distinct capabilities that make it the go-to organization for cyberthreat awareness for private entities.

Federally-enabled sharing of cybersecurity information is evolving. Many of the existing sharing relationships are shown in diagram 2 of my written testimony. The jumbledness of the links demonstrates that a NISO should complement sharing, clarify roles and responsibilities and, as appropriate, help consolidate those roles and responsibilities. We don't need yet another loosely mandated cybersecurity information-sharing organization, and NISO can be a step in the right direction, especially in helping to clarify interactions.

Since we are discussing data, information, and knowledge, let's also talk about the importance of operationally and scientifically valid data, especially in the context of research, development, acquisition, and assessment. This applies to both sections 2 and 4 of the draft legislation.

Given the preponderance of threats, standards, technologies, products, best practices, et cetera, in cybersecurity, I strongly encourage the committee to include language in the legislation that emphasizes the need for operationally and scientifically valid, scientifically sound capabilities. Not every best practice scales well and not every technology has scientifically sound evidence of its efficacy and its limitations. Such legislation language would create an important positive demand for well-formed pilots and experi-

ments that produce broadly meaningful data and results. This would stimulate the development and maturation of ever-improving methodologies for pilot projects, assessments, experiments, and research.

In conclusion, I look forward to working with the subcommittee to improve the timely sharing of actionable cybersecurity information that is operationally and scientifically valid. Thank you.

[The statement of Mr. Shannon follows:]

PREPARED STATEMENT OF GREGORY E. SHANNON

DECEMBER 6, 2011

Chairman Lungren, Ranking Member Clarke, and other distinguished Members of the subcommittee, thank you for the opportunity to testify; it is my pleasure to discuss your draft legislation.

ABOUT CERT®

The CERT Program is part of the Carnegie Mellon University Software Engineering Institute (SEI), a Department of Defense Federally-funded research and development center (FFRDC) located on the Carnegie Mellon campus in Pittsburgh, Pennsylvania *(www.sei.cmu.edu)*.

The CERT Program *(www.cert.org)* has evolved from the first computer emergency response team, created by the SEI at the request of the Defense Advanced Research Projects Agency (DARPA), in 1988 as a direct response to the Morris worm incident. The CERT Program continues to research, develop, and promote the use of appropriate technology and systems management practices to resist attacks on networked systems, limit damage, restore continuity of critical systems services, and investigate methods and root causes. CERT works both to mitigate cyber risks and to facilitate local, National, and international cyber incident responses. Over the past 23 years, CERT has led efforts to establish over 200 computer security incident response teams (CSIRTs) around the world—including the Department of Homeland Security (DHS) US–CERT. We have a proven track record of success in transitioning research and technology to those who can implement it on a National scale.

I am Dr. Greg Shannon, the Chief Scientist for the CERT Program, where I lead efforts to sustain and broaden CERT's strategic research, development, and policy initiatives.

TESTIMONY

I first want to ensure that the committee appreciates the exceptional work that is under way at the Department of Homeland Security (DHS) in the area of information sharing. I understand frustrations with the current range and pace of information sharing, but I assure you that DHS is making great progress. The type of information that organizations are being asked to share with each other and the U.S. Government is sensitive, and sharing such information requires trusted relationships, established and tested over time. Established trust is a key success factor for such programs, and reliable trust takes time.

Working from the objectives of the current draft legislation, drawing on CERT's 23 years of experience, and using concepts from public health models,[1] I will discuss how to leverage current efforts, the strengths and challenges of both the current efforts and the legislation, and specific recommendations. The mission of our FFRDC is to improve the state of the practice, so I will focus on what should be done versus who should be doing it.

I endorse the committee's proposal to position a non-profit private entity to serve as a National clearinghouse for the exchange of cyber threat information—the NISO (National Information Sharing Organization). We believe that a "third-party, honest broker" facilitator for the disclosure and dissemination of cyber-security intelligence creates a superior and more productive environment where all participants, both Government and non-Government, more readily share sensitive information. Moreover, it is imperative that the designated organization is making decisions for the

[1] I am drawing on ideas and language in the forthcoming report from the EastWest Institute, Using a Public Health Model to Support Collective Action to Improve Global Internet Health, that is being written by an international private-sector-led working group.

greater good based on the highest quality data, openly acquired and objectively analyzed.

Many of the goals proposed for the NISO have parallels to the activities of the Centers for Disease Control and Prevention (CDC)—the fact that it is a Federal agency notwithstanding. As the Nation's leader in health, monitoring, prevention, and preparedness, the CDC works to monitor and prevent outbreaks, implement prevention strategies, and maintain National statistics—it is a central clearinghouse for information with response capabilities. Crucially, it does so by working with partners throughout the Nation and the world to collaboratively create the expertise, information, and tools that people and communities need to protect themselves.

We envision the NISO, like the CDC, filling a cyber information leadership role while interacting with existing groups. The NISO, run by a non-profit would have in-house functions, maintain a common operating picture, and the 24/7 help desk, but its biggest role will be to interface with present-day efforts and improve communications and collaboration. I want to ensure the committee recognizes the on-going work within established frameworks and discuss the benefits of utilizing progress already made. To add yet another institution could in practice derail the current advancements and delay the committee's ultimate goal of timely information sharing. I suggest that instead of creating a duplicative organization, the committee charge the NISO with being the single point of interaction for those successful efforts and, when appropriate, consolidate work under the NISO.

I share and understand frustration that capabilities for cyber threat information sharing are not being created quickly enough. Human nature reasons that adding people to a late or slow project will accelerate performance; however, Brooks's Law, also known as the "mythical man-month," suggests otherwise. Based on his experiences at IBM, Dr. Fred Brooks states: "adding manpower to a late software project makes it later."[2] Brooks found that there is "ramp-up" time to adding staff to a project—they aren't productive immediately, and their education diverts resources from the rest of the team. Furthermore, a new player sharply increases communication costs. As you add additional "reporting" bodies, confusion as to who should be told what and when is only exacerbated. Everyone working on the same task needs stay synchronized, so as more people are added, they spend more time trying to find out what everyone else is doing. Furthermore, Dr. Brooks famously said, "Nine women can't make a baby in one month," implying that regardless of the manpower, some undertakings just take time. For information sharing, building the necessary trust relationships cannot be rushed.

To better understand our vision, I have mapped out how a NISO organization might look—see Diagram 1. In doing so, we made assumptions about the overall goals of the organization based on the stated and implied objectives, and I encourage the committee to think carefully about what problems they want the NISO to solve and how the structure and authority of the NISO helps solve those problems. Using CERT's experience we have listed what we see as the necessary capabilities and enablers for a successful NISO.

There are four critical success factors for such an entity to accomplish the objectives set out: Data of value, trust, protections, and policy. First, for the NISO to have success, it absolutely must be able both to share and facilitate the sharing of timely, actionable information. The existence of the former will enable the latter. Furthermore, that which the NISO shares must be distinct and not readily attainable by participating organizations. Otherwise there is little or no incentive to participate. The value of NISO's information would come from either being the exclusive distributor of an insight through novel aggregations or applying a new analysis technique to unique, participant-shared, or public information. Providing valuable data is not only the result of having access to unique data, but also the ability to fundamentally analyze the data differently to provide real, actionable, intelligence from which best practices are derived. For the NISO to truly serve a significant and useful role, the timely and actionable information they disseminate to participating organizations must be reactive as well as proactive, such as best practices. The promise of exclusive information, such as fused analysis of network data, network traffic, or forensic artifacts, will be the value added that NISO participants need to justify their participation. This information will also differentiate the suggested common operating picture (COP) from the several entities that offer situational awareness, and bring the necessary added value to ensure participant involvement. Furthermore, the COP should strive to be able to fundamentally analyze the data differently, further differentiating the NISO from similar organizations and enticing participation. This function would draw nicely from the anticipated collaborative re-

[2] Frederick P. Brooks, Jr. "The Mythical Man-Month." 1995 [1975]. Addison-Wesley.

search and development. Like the CDC, the NISO needs distinctive capabilities that make it the "go-to" organization for cyber threat awareness.

Next, I want to stress to the committee the importance of trust to facilitate meaningful exchanges. The need for trust is yet another reason that building on existing efforts is important. While there may be frustrations with the current range and pace of information sharing, you cannot legislate trust, and any new organization needs time to build the necessary relationships for meaningful communications. I believe the committee's intentions are best served by building upon the existing rapports.

Last, it is imperative that solid protection mechanisms and safe harbors be in place for the designated organization and its participants for unencumbered information sharing and analytical product delivery to occur. This will likely require both legislative updates and policy changes, which must be done with the utmost care to privacy and civil liberties. This is an important yet difficult task, and I commend the committee for beginning the dialogue.

Moving on to the information-sharing objective of the NISO organization: As you can see from Diagram 2[3] (NISO relationships with existing efforts), there are currently many organizations that "specialize" in information sharing. Several Government agencies have information-sharing entities—not just DHS—and not to mention the hundreds of private-sector and academic entities, some quasi-Government, that all claim to be centers where cyber information can be shared. Without a recognized body, coordinated with United States Government (USG) efforts, private-sector organizations are confused about with whom and under what circumstances they should engage all of these other efforts. This fragmentation results in sub-optimal dissemination of timely information. NISO would serve as the National cyber-security aggregation point and coordination center endorsed by and coordinating with the Federal Government. We advocate establishing a single point of interaction, to be run by the designated non-profit entity, while collaborating and working with the mechanisms and organizations already in place. For certain operational tasks, it might make sense to re-brand current efforts and place them under the NISO, all the while ensuring we are building on the successes and not starting over.

For the sake of clarity I will run through a real-world example of a cyber threat and how a NISO, organized as suggested above, would have had a positive impact on the situation. Let us take the Conficker worm, first discovered in early November 2008, which used flaws in Microsoft Windows software to infect millions of computers. Realizing a collaborative effort was needed to combat the advanced malware techniques behind Conficker, an industry group was serendipitously formed during an ICANN conference in February 2009. While the Conficker working group (CWG) had many successes, and several similar working groups have since formed using the same model, the threat clearly demonstrated gaps in our National capabilities. First and foremost, the ramp-up delay: The effort expended to form the group and time spent finding the right skill sets, capabilities, and authorities before any work could be done on the problem at hand. Had there been an established and trusted entity, such as a NISO, Microsoft could have approached them and begun combating the problem much sooner. There are other gaps the CWG has conceded they were unable to fill, such as the need for a dedicated project manager, administrative support, testing facilities, and a more coordinated approach with the anti-malware tool vendors—roles that a NISO could clearly execute. Likewise, there are lessons to be learned from why the group was successful. The CWG has attributed their success to trust. The operational members of the group all knew each other, had previously worked with each other, and had confidence that all members would a good job, follow through with their given tasks, and do no intentional harm. That trust was the glue that enabled a group of colleagues to form an effective collaboration that was largely able to contain the worm. Their success corroborates the model of a third-party organization working with existing functions and building on already established relationships.[4]

I encourage the committee to require that the NISO maintain a National repository of malware for research purposes. Currently there are several organizations that have malware repositories but they are seen as a competitive advantage and rarely shared. Access to such a repository would enable cyber research to reach new

---

[3] Caveat: The diagram is in no way truly comprehensive of all the current organizations that claim to be cyber information-sharing centers. These are simply some of the most prominent entities. Furthermore the relationships represented in the diagram are derived from public mission statements and budget documents and are meant to be illustrative, not comprehensive.

[4] Nazario, Jose. "Conficker Working Group Overview." Institute for Information Infrastructure Protection (I3P). 12 October 2011. Web. *http://www.thei3p.org/docs/events/cybercprfiles/NAZARIOI3PCONFICKER.pdf.*

levels. Currently researchers work with only small pieces of the puzzle, resulting in reactive research, and impeding research that can look more globally at the problem. Again, if we use the public health model, imagine if cancer researchers were only told that cancer affects thousands of people who die every year, and the data was broken down by neither type nor outcome. Such data would make it impossible to make well-informed decisions about priorities for response as well as research. Armed with a well-maintained malware repository, with appropriate controls on access, the NISO could provide more effective methods for basic cyber hygiene.

Finally, I want to touch upon the bill's research and development objectives. Given the preponderance of threats, standards, technologies, products, best practices, etc. in cybersecurity, I strongly encourage the committee to include language in the legislation that emphasizes the need for operationally and scientifically sound capabilities. Not every best practice scales well, and not every technology has scientifically sound evidence of its efficacy and its limitations. The academic research community increasingly recognizes the need for such sound methods as evidenced by workshops on Cyber Security Experimentation and Testing (CSET)[5] and Learning from Authoritative Security Experiment Results (LASER).[6] Such legislation language would create an important positive demand for well-formed pilots and experiments that produce broadly meaningful data and results. This would stimulate the development and maturation of ever-improving methodologies for pilot projects, assessments, experiments, and research.

For example, in the draft language, phrases such as the following are used:

- Develop and conduct risk assessments;
- Comprehensive assessment techniques;
- Foster the development of essential information security technologies;
- Facilitate the adoption of new cybersecurity technologies and practices;
- Guidelines for making information systems more secure at a fundamental level;
- Catalogue of risk-based performance standards;
- Cybersecurity research and development.

I recommend adding clarifications that such artifacts and activities are:

- Operationally valid and scalable in situ;
- Scientifically, theoretically, and/or experimentally valid or sound;
- Evidence-based capabilities and limitations.

Participants can further facilitate effective security by authorizing the NISO to support creation of and access to high-fidelity data sets to qualified researchers, of course with appropriate access controls. Access to such data is essential for creating and evaluating critical technologies and best practices, especially to understand important limitations.

To finish, I want to applaud the committee's foresight in combining research functions with operational objectives in the NISO design. It is an ambitious and difficult task, and consequently there are currently few successful mixed organizations. Nevertheless, combining research and operations can and does have many benefits. I see the SEI's CERT Program as a viable model for successfully bringing together research and operations to add value to both communities. At CERT, our strategy is to create usable technologies, apply them to real problems, and amplify their impact by accelerating broad adoption. Having one foot in operations gives us the insight into real-world problems and ensures our research has real-world applications. Moreover, having operational access gives us the opportunity to test our research and make the necessary improvements for a successful and scalable transition.

Thank you for the opportunity to comment on this important legislation and leverage CERT's 23 years of experience in the area of information sharing.

---

[5] Established 2008: *http://www.usenix.org/events/cset12/index.html.*

[6] New: Learning from Authoritative Security Experiment Results (LASER), *http://www.laser-workshop.org*.

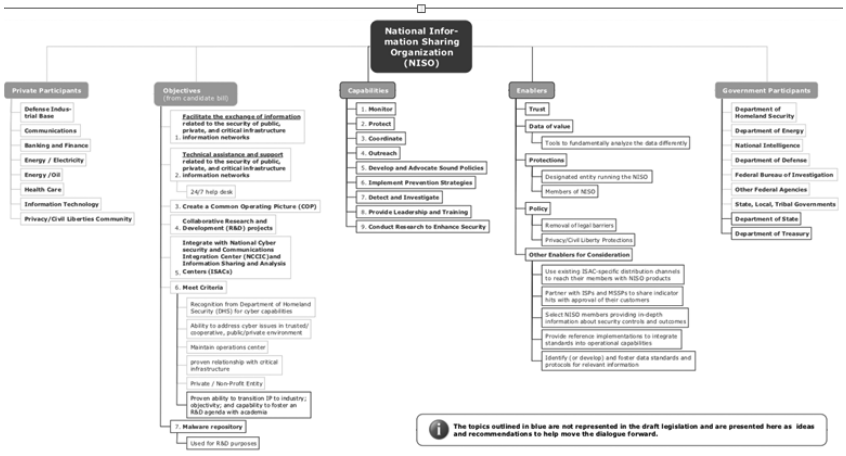

Diagram 1

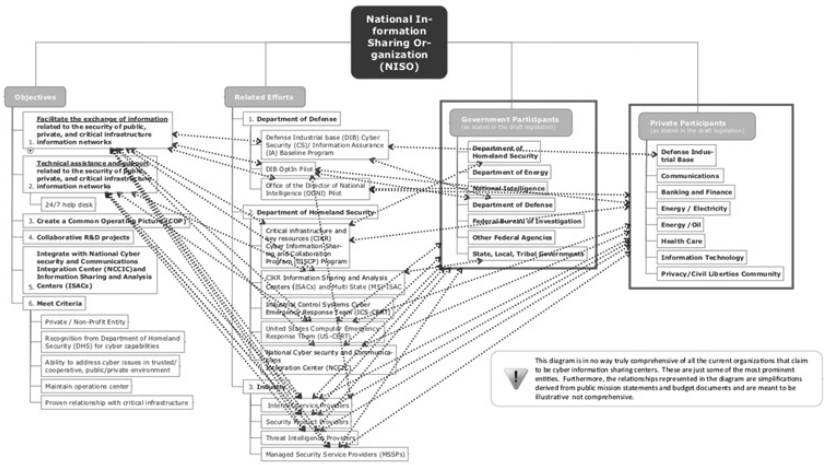

Diagram 2

Mr. LUNGREN. Thank you very much.
Ms. McGuire.

STATEMENT OF CHERI F. MC GUIRE, VICE PRESIDENT OF GLOBAL GOVERNMENT AFFAIRS AND CYBERSECURITY POLICY, SYMANTEC CORPORATION

Ms. MCGUIRE. Chairman Lungren, Ranking Member Clarke, and distinguished Members of the subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation and the Business Software Alliance. In addition to my role at Symantec Corporation, I also serve as the chair of the IT Sector Coordinating Council, as well as a member of the board of Information Technology and Information Sharing and Analysis Center or the IT ISAC. I also serve as the principal IT sector representative to the Partnership for Critical Infrastructure Security, which is the cross-sector cyber working group, a cross-sector critical infrastructure working group that works most closely with the Department of Homeland Security and other agencies on infrastructure protection matters.

As the world's information security leader, Symantec maintains 11 security response centers globally and we utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year.

As you all are too well aware, our Nation's critical infrastructure systems are constantly under attack. In our latest internet security threat report, we observed a 19 percent year-over-year increase in threat activity and identified more than 286 million unique variations of malware alone. In addition, based on data in our 2011 Norton cybercrime survey we estimated that 431 million cybercrime victims have been impacted globally with cyber attacks in the past year. At an annual combined cost of $388 billion globally, based on both financial losses and the lost time to recover from attacks, cybercrime costs us more today than the global black market for marijuana, cocaine, and heroin combined.

Symantec has been a long-time proponent for improving our Nation's cybersecurity. As a member of the Business Software Alliance, we were part of a coalition that offered a white paper on improving our Nation's cybersecurity through public-private partnerships. This paper laid out core principles for cybersecurity policy. I would like to submit it for the record as part of my testimony today.

As part of these core principles, first we must promote and improve information sharing, which is often referred to as the key to combating cyberthreats. However, we also must recognize that information sharing is not an end goal but rather is a tool to providing situational awareness or visibility so that appropriate protective and risk mitigation actions may be taken.

Second, effective and efficient cybersecurity cannot be accomplished under a one-size-fits-all regime. For example, a small mom-and-pop convenience store should not be required to implement the same policies or standards as a nuclear facility. Using a risk-based approach provides a mechanism for the Government and industry to assess risk and expend the necessary resources on areas that are truly needed.

Third, any proposed legislation must also promote, not stifle, innovation. Cybersecurity policy should maximize the ability of orga-

nizations to develop and adopt the widest possible choice of cutting-edge cybersecurity solutions.

With regard to roles of industry and Government in cybersecurity, the private sector's role is clearly defined to operate and protect their networks. Industry must continually tune their security environments to manage the level of risk associated with the information they are protecting, while at the same time working within the current economic pressures of doing more with less.

Further, industry must move from a device-centric security model to one that is identity- and information-centric. This new security paradigm of data-centricity is not only about protection of devices, but more importantly is about protecting the information. The Government, of course, plays an important role in cybersecurity. Government can create incentives to encourage the adoption of cybersecurity technologies, it can assist with education, training, and awareness to empower users, it can serve as a facilitator for preparedness by sponsoring exercises, and it can share actionable information with industry to improve cybersecurity situational awareness and the ability to respond.

Symantec was very pleased to review the draft bill that has been circulated by you, Mr. Chairman. The draft legislation we believe is a positive step forward in developing a National cybersecurity policy that helps fulfill the core principles that I have just discussed.

First, we believe there needs to be improved coordination between and among public and private entities. Thus we are very supportive of the bill's designation of a single entity as the National cybersecurity authority.

Second, we support the bill's inclusion of a risk-based approach to cybersecurity so that we do not overburden small businesses with unnecessary security requirements, while still ensuring that our critical infrastructures are protected.

We are also supportive of using existing internationally-recognized performance standards, including those developed by NIST. We are also pleased that the legislation takes into account how our National cybersecurity policy will enhance economic prosperity. Keeping this goal in mind will help to prevent burdensome regulations, and it also appropriately emphasizes the need to maximize market-based incentives and public-private partnerships.

Finally, we support the bill's emphasis on promoting information sharing. The bill clearly articulates that the Government must share real-time actionable information with critical infrastructure, owners, and operators. The mandate within the structure of the proposed NISO that the Government must share information is a strong step in the right direction. However, some questions still remain about how we will continue to utilize the existing entities under the proposed framework. We believe that it is important to give the significant time and resources that companies have invested in the sector coordinating councils and the ISACs the appropriate venue to participate.

In conclusion, recognizing that there is no silver bullet for cybersecurity as a first step, but we really do have to shift this dialogue from solving the cybersecurity problem to managing the risks asso-

ciated with it. We welcome the opportunity to answer any questions you may have at this time. Thank you.

[The statement of Ms. McGuire follows:]

PREPARED STATEMENT OF CHERI F. MCGUIRE

DECEMBER 6, 2011

INTRODUCTION

Chairman Lungren, Ranking Member Clarke and distinguished Members of the subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation [1] and the Business Software Alliance (BSA) [2] as you consider this very important issue.

My name is Cheri McGuire and I am the vice president of global government affairs and cybersecurity policy at Symantec Corporation. I also serve as the current chair of the Information Technology (IT) Sector Coordinating Council (SCC), which is one of 18 critical sectors identified by the President and the U.S. Department of Homeland Security (DHS) to work in partnership with the Government on critical infrastructure protection (CIP) and cybersecurity policy and operational matters. I am also a member of the board for the IT Information Sharing and Analysis Center (ISAC), and serve as the principal IT Sector representative to the Partnership for Critical Infrastructure Security (PCIS). Prior to joining Symantec in 2010, I served as Director for Critical Infrastructure and Cybersecurity in Microsoft's Trustworthy Computing Group, and before that, at the U.S. Department of Homeland Security (DHS), where I led the National Cyber Security Division and the U.S. Computer Emergency Readiness Team (US–CERT).

Symantec is the world's information security leader, with over 25 years of experience in developing internet security technology. Today, we protect more people and businesses from more on-line threats than anyone in the world. We maintain 11 Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. Our best-in-class Global Intelligence Network allows us to capture world-wide security intelligence data that gives our analysts an unparalleled view of the entire internet threat landscape, including emerging cyber attack trends, malicious code activity, phishing, and spam. In short, if there is a class of threat on the internet, Symantec knows about it.

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

We welcome the opportunity to provide comments as the committee continues its important efforts to bolster the state of cybersecurity in the United States and abroad. In my testimony today, I will provide the subcommittee with:

- our latest analysis of the threat landscape as detailed in the Symantec Internet Security Threat Report Volume XVI (ISTR XVI) and in the 2011 Norton Cybercrime Report;
- principles for improving our Nation's cybersecurity;
- appropriate roles of industry and Government in cybersecurity; and
- our views on your draft legislative proposal for cybersecurity.

THREAT LANDSCAPE

Today, we rely on technology for virtually everything we do, from driving to and from work, to mobile banking, to securing our most critical systems that protect our

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

[2] The Business Software Alliance *(www.bsa.org)* is the leading global advocate for the software industry. It is an association of nearly 100 world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement, and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward.

Nation such as our nuclear plants and electric grid. Our Nation's critical infrastructure systems are constantly under attack, and the methods for attacking us are constantly evolving and becoming more sophisticated with each passing minute. It is our goal to ensure that we are thinking ten steps ahead of the attackers. Looking at the current threat landscape is not enough—we must also keep our eyes on the horizon for evolving trends.

In the latest Symantec Internet Security Threat Report (ISTR) Volume XVI, we observed significant changes to the threat landscape in 2010.[3] The volume and sophistication of threat activity increased more than 19 percent over 2009, with Symantec identifying more than 286 million unique variations of malicious software or malware. These included threats to social networking sites and users, mobile devices, and phishing.

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

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

Over the years, we have observed an ominous change that has swept across the internet. The threat landscape once dominated by worms and viruses developed by irresponsible hackers is now being ruled by a new breed of cybercriminals. As more people have access to technology, criminals leverage it for criminal purposes. In October, we released our 2011 Norton Cybercrime Report where we examined on-line behavior in 24 countries and interviewed nearly 20,000 consumers.[4] We calculated the cost of global cybercrime at $114 billion annually. We also calculated that lost time due to recovery and impact on personal lives was an additional $274 billion world-wide. Further, we found that more than two-thirds of on-line adults (69 percent) reported having been a victim of cybercrime in their lifetime. Every second, 14 adults become a victim of cybercrime, resulting in more than 1 million cybercrime victims every day.

With an estimated 431 million adult victims globally in the past year, and at an annual combined cost of $388 billion globally based on financial losses and time lost, cybercrime costs are significantly more than the global black market in marijuana, cocaine, and heroin combined—which is estimated at $288 billion per year.

It is not just our computers that we need to secure from cybercriminals. Today, a high percentage of consumers use their mobile phones to conduct nearly every aspect of their life, from basic communication to on-line shopping to mobile banking. Most of these phones are not secure. The Norton Cybercrime Report revealed that 10 percent of adults on-line have experienced cybercrime on their mobile phone. Further, we reported in the Symantec ISTR XVI that there were 42 percent more mobile vulnerabilities in 2010 compared to 2009—a sign that cybercriminals are turning their efforts to the mobile space.

Recently, there has been an up-swing in press reports regarding cyber attacks and the "advanced persistent threat" or APT. While APT is one of the most overused terms in the security industry today, it is nevertheless something to be taken seriously. APTs covertly infiltrate systems and hide and wait for opportune moments to steal information or damage systems.

The APT is not one entity; rather it is many different and independent entities, with a tremendous range of motivations. Some of these motivations include financial gain, exfiltration (or theft) of sensitive and personal information, cyber espionage,

---

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

[4] 2011 Norton Cybercrime Report. *www.norton.com/cybercrimereport*

and a new turn in the last 18 months, cyber sabotage as exemplified by the Stuxnet malware.

Another trait of the APT is to infiltrate a system, enterprise, or organization, but not immediately execute the ultimate mission. Often the APT will lie in wait, gaining intelligence, observing patterns, and use this information to glean information to further refine the ultimate attack.

The threats we are seeing are not new, they are just newly packaged. However, while the attacks are not new, they are becoming more targeted and the monetary losses have grown exponentially. Most indicators point to future cyber attacks as being more severe, more complex, and more difficult to prevent and address than current threats. Thus, it is even more vital that we have a cybersecurity policy that is flexible, fosters innovation, and enables us to stay ahead of those with bad intentions.

PRINCIPLES FOR IMPROVING OUR NATION'S CYBERSECURITY

Symantec has been a long-time proponent for improving our Nation's cybersecurity. We have testified before Congress on the issue each of the last 4 years and have been a key stakeholder in the numerous legislative efforts and public-private partnerships to improve cyber research and development, cyber education, security standard setting, CIP, and more. We have also participated in various multi-industry efforts aimed at improving our cybersecurity policies. For example, as a member of the Business Software Alliance, we were part of a large coalition of cybersecurity stakeholders that authored a white paper on "Improving our Nation's Cybersecurity through Public Private Partnerships."[5] This paper laid out a number of principles, and we believe any cybersecurity legislation should stay true to the core principles associated with these key elements:

- Risk management standards, assessment, and incentives;
- Incident management;
- Information sharing and privacy;
- International engagement;
- Supply chain security;
- Innovation and research and development (R&D); and,
- Education and awareness.

For the purposes of my testimony, I will discuss a few of these in the context of your draft legislative proposal.

Information Sharing

Any cybersecurity legislation must promote and improve information sharing. Information sharing is often referred to as the key to combating cyber threats. However, we must first recognize that information sharing is not an end goal, but rather a tool or mechanism to provide situational awareness, or visibility, so that appropriate protective and risk mitigation actions may be taken. In order for information sharing to be effective, information must be shared in a timely manner, must be shared with the right people or organizations, and must be shared with the understanding that so long as an entity shares information in good faith, it will not be faced with legal liability for sharing the information.

In order to achieve truly effective information sharing, there must be increased coordination between and among industry and Government. In my roles both inside and outside of the Government, and more recently as Chair of the IT Sector Coordinating Council and on the Board of the IT–ISAC, I have seen first-hand both successes and challenges in our current public-private partnership with respect to information sharing.

In particular, cybersecurity exercises have been one of the most successful public-private partnership and information-sharing initiatives to date. The level of engagement and resources brought to bear from the Government and industry to jointly plan, develop scenarios, define information-sharing processes, and execute the exercises has been unprecedented. The lessons learned from these exercises have been invaluable to both industry and Government. However, much work still needs to be done to address recommended actions associated with information sharing and realize improvements.

One way to improve information sharing is to provide the Government with the proper tools and authority to effectively disseminate information. I have seen too many instances of the Government releasing information on cyber threats, days and sometimes weeks, after the threat has been identified. In many of these cases, by

[5] March 8, 2011. "Improving our Nation's Cybersecurity through Public Private Partnerships: A White Paper." *http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/cybersecurity__white__paper__publicprivatepartnership.ashx.*

the time the Government releases the information, it has little use because the private sector has already identified and taken actions to mitigate the threat. There is no single solution that will eliminate these delays, but passing legislation that sends a clear message to the Government that sharing information with the private sector is both a priority and necessary to protect our infrastructure from cyber attacks will go a long way.

At Symantec, we also support an incentive-based approach to information sharing. There is no doubt that businesses can gain a competitive advantage by not disclosing information to their competitors. However, a well-incentivized program of collaboration can help offset the disadvantages and keep the information flowing freely.

At the same time, Government does have an important role in fostering the effectiveness of information sharing. For example, Government can increase voluntary information sharing through tax incentives, grant funding, and streamlining of regulatory procedures. We also need to address policies that discourage businesses who would be willing to share information but choose not to because of fear of prosecution. Therefore, liability protections are necessary to improve bi-directional information sharing.

As with any partnership, information sharing is founded upon and enabled by trust. That trust is weakened when Government information-sharing mandates are imposed on industry. Enhanced self-interest and a flexible approach are more likely to improve information sharing than Government mandates to private industry.

Risk Assessment

Effective and efficient cybersecurity cannot be accomplished under a "one-size-fits-all" regime. Each system within our critical infrastructure and each cyber threat pose different risks. For example, a small mom-and-pop convenience store should not be required to implement the same policies or standards as a nuclear facility. Using a risk-based approach, as outlined in the National Infrastructure Protection Plan (NIPP),[6] provides a mechanism for the Government and industry to assess risk and expend the necessary resources on areas that truly need it, rather than spending equal amounts of resources on both high- and low-risk targets. Thus, it is imperative that any cybersecurity legislation use a risk-based analysis system rather than a one-size-fits-all regime. Leveraging existing regulatory and voluntary regimes to encourage cybersecurity risk assessments and the adoption of standards should be considered first in any proposals.

Innovation

Any proposed legislation must also promote, not stifle, innovation. As I discussed earlier, threats are constantly evolving and so must the technology to mitigate those threats. Symantec has long been a supporter of a National cyber R&D strategy. Any cybersecurity innovation legislation must promote technology advancement so we can stay ahead of the curve. Cybersecurity policy should therefore maximize the ability of organizations to develop and adopt the widest possible choice of cutting-edge cybersecurity solutions. An effective way to do this is through the creation and implementation of a National Cybersecurity R&D Plan.

Currently, we have a Federal plan for cyber R&D, but industry must be part of the larger process, with prioritized, National-level objectives set jointly by public and private partners. The public-private partnership should be used to create a genuine National Cybersecurity R&D Plan that contains a detailed road map and specifies the respective roles of each partner. This would include input from industry, academia, and Federal, State, and local governments. The plan and its implementation road map should be regularly reviewed by the partners to verify the action plan, determine progress and accountability, and adjust as necessary.

ROLES OF INDUSTRY AND GOVERNMENT IN CYBERSECURITY

In discussing public-private partnerships, we should first consider the various roles of industry and Government with regard to defending critical infrastructure. The private sector's role is clearly defined to operate and protect their critical information networks. Just as a private citizen needs to lock the doors to their home, infrastructure owners and operators need to ensure that their network security environment is the most up to date to defend against the latest threats.

In addition, industry must continually tune their security environments to manage the level of risk associated with the information they are protecting, while at the same time working within the current economic pressures of doing more with

[6] National Infrastructure Protection Plan, *http://www.dhs.gov/xlibrary/assets/NIPP__Plan.pdf*.

less. Further, industry must move from a device-centric security model to one that is identity- and information-centric, with a focus on infrastructure that is secured and more importantly trustworthy. The new security paradigm of "data-centricity" is not only about protection of devices, but more importantly is about protecting the information.

While the defense of critical infrastructures and the networks they rely on rests with owners and operators, the Government does play an important role in cybersecurity. As discussed above, Government has the ability to create incentives that encourage the adoption of cybersecurity technologies. It can also assist with education, training, and awareness to improve the first line of defense by empowering users. In addition, the Government can serve as a facilitator for preparedness by sponsoring exercises and drills that include private industry. Further, it can raise the bar of security within the Government by outlining minimum requirements for Government procurement. Last, the Government can support public-private partnerships and information sharing with industry to improve overall cybersecurity situational awareness.

While the Government plays a number of roles in cybersecurity, one of the challenges is measuring the effectiveness of Government CIP programs. To examine awareness, engagement, and readiness with regard to Government CIP programs, Symantec conducts an annual global survey of critical infrastructure providers. Released in October, our 2011 Critical Infrastructure Protection Survey, found a drop in awareness and engagement on a global basis.[7] We saw a marked decline in companies that are engaged in Government CIP programs, with 37 percent in 2011, compared to 56 percent in 2010.

While the findings of this survey are somewhat alarming, it is not that surprising. Many survey respondents reported limitations on staffing and resources which help explain why critical infrastructure providers have had to prioritize and focus their efforts on more day-to-day cyber threats. However, given the increase in targeted attacks, such as Stuxnet, Duqu, and Nitro, against critical infrastructure providers, businesses and governments around the world should be aggressive in their efforts to promote and coordinate protection of critical cyber networks. Given the survey results, we have several recommendations for governments to promote CIP programs to owners and operators in order to raise awareness:

- Governments should continue to put forth the resources to establish government critical infrastructure programs.
  - The majority of critical infrastructure providers confirm that they are aware of government critical infrastructure programs.
  - Furthermore, a majority of critical infrastructure providers support efforts by the government to develop protection programs.
- Governments should partner with industry associations and private enterprise groups to disseminate information to raise awareness of government CIP organizations and plans, with specifics about how a response would work in the face of a national cyber attack, what the roles of government would be, who the specific contacts are for various industries at a regional and national level, and how government and private business would share information in the event of an emergency.
- Governments should emphasize to critical infrastructure providers and enterprises that their information be stored, backed up, organized, prioritized, and that proper identity and access control processes are in place.

VIEWS ON DRAFT LEGISLATIVE PROPOSAL FOR CYBERSECURITY

Symantec was pleased to review the draft bill that has been circulated by you, Mr. Chairman. The draft legislation is a positive step forward in developing a National cybersecurity policy that helps fulfill the core principles I discussed above.

National Cybersecurity Authority

To accomplish the goal of improving cybersecurity, we believe there needs to be improved coordination between and among entities. Currently, there are several Government agencies working on various aspects of cybersecurity, though there is no designated lead. Thus, we are supportive of the bill's designation of a single enti-

[7] Symantec's Critical Infrastructure Protection Survey is the result of research conducted in August and September 2011 by Applied Research, which surveyed C-level, IT professionals in SMBs and enterprises in 14 industries specifically designated as critical infrastructure industries. The survey included 3,475 organizations from 37 countries in North America, Europe, Middle East and Africa, Asia Pacific, and Latin America *http://www.symantec.com/about/news/release/article.jsp?prid=20111030_01.*

ty as the "National Cybersecurity Authority." We must be mindful, however, that we do not create an additional level of bureaucracy.

Risk Assessment and Standards

We support the bill's inclusion of a risk-based approach to cybersecurity. Requiring the Secretary of Homeland Security—in collaboration with industry—to identify risks within our cybersecurity infrastructure ensures that we do not overburden small businesses with unnecessary security requirements, while ensuring that our chemical facilities, dams, and electric grid are appropriately protected. We are also supportive of using existing internationally recognized consensus-developed risk-based performance standards, including those developed by the National Institute of Standards and Technology (NIST). In addition, we support the bill's instruction to the Secretary to develop market-based incentives designed to encourage the use of such standards.

We are also especially pleased that the legislation directs DHS to take into account how our National cybersecurity strategy and implementation policies will enhance economic prosperity. Keeping this goal in mind will help to prevent burdensome regulatory policies from being implemented. It also appropriately emphasizes the need to maximize market-based incentives and public-private partnerships for improved cybersecurity.

Information Sharing

Finally, we support the bill's emphasis on promoting information sharing. The bill clearly articulates that the Government must share real-time, actionable information with critical infrastructure owners and operators.

We also understand the motivation to create a National Information Sharing Organization, or the NISO. The current system of SCCs and ISACs was developed to facilitate bi-directional information sharing between and among Government and private industry. These entities have been successful in facilitating information sharing within industry, and have had varying levels of success in industry-to-Government sharing. However, improvements must be made with regard to how well the Government shares threat information with private industry.

We believe that one of the reasons the Government is reluctant to share real-time actionable information is because there is no mandate to do so. The mandate within the structure of the NISO that the Government must share information is a strong step in the right direction. However, questions remain about how we will continue to utilize the existing entities under the proposed NISO framework. We believe this is important given the significant time and resources that companies have invested in the SCCs and ISACs. We look forward to working with the committee to address these important issues.

CONCLUSION

In conclusion, if we are to successfully mitigate today's multi-dimensional threats more effectively—and use public-private partnerships and information sharing as tools—we must incorporate a comprehensive approach for risk, resiliency, and collaboration to improve critical infrastructure and cybersecurity. The U.S. public-private partnership has encountered both successes and challenges over the years, but it is clear that we must continue to work together to leverage the best that industry and Government bring to the table and confront the challenges directly. Recognizing there is no silver bullet for cybersecurity, we must shift the dialogue from "solving" the cybersecurity problem, to "managing the risk" associated with it.

On behalf of Symantec and the Businesses Software Alliance, we commend you and your staff's efforts in crafting this legislation that appropriately focuses on risk management, information sharing, and technology innovation. We look forward to working with you in the future as the bill moves through the Congress. I look forward to answering any questions you may have.

Mr. LUNGREN. Thank you very much.

Mr. Nojeim.

STATEMENT OF GREGORY T. NOJEIM, SENIOR COUNSEL AND DIRECTOR, PROJECT ON FREEDOM, SECURITY AND TECHNOLOGY, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. NOJEIM. Chairman Lungren, Ranking Member Clarke, and Members of the subcommittee, thank you for the opportunity to testify today on behalf of the Center for Democracy and Tech-

nology. CDT is a nonprofit public-interest organization dedicated to keeping the internet open, innovative, and free.

We applaud the subcommittee for holding this hearing on cybersecurity legislation. I will address the information-sharing provisions in the draft bill in some detail, but start with some high-level observations about the bill which we think is a very good start. It has a light regulatory touch, generally relying on market incentives rather than Government mandates to increase cybersecurity performance. A heavy-handed approach, by contrast, could discourage security innovation. The regulation it imposes would extend primarily to owners and operators of critical infrastructure information systems. It defines critical infrastructure more carefully than do other bills, but more specificity would be helpful. It properly cements DHS as the lead Federal agency for the civilian cybersecurity program instead of giving this role to NSA or Cyber Command.

Civilian control promotes the transparency and trust that are essential to program success. The bill appropriately avoids giving the Government the authority to shut down or limit internet traffic in a cybersecurity emergency. Conferring such authority is anthema to civil liberties. It also undermines security by discouraging companies from sharing information that could be used to shut down their operations. Most importantly, instead of giving the Government the authority to monitor privately-owned networks for intrusions, it leaves this authority where it belongs: With the private sector network operators who know their systems best.

We are, concerned, though about the information-sharing provisions of the bill and we encourage you to tighten them. The bill would create a non-profit industry-led, quasi-Governmental National Information-Sharing Organization, NISO, through which cyberthreat information would be shared among its Governmental and private sector members. A privately-run information-sharing organization is more likely to have the necessary agility than would a Government-run entity. NISO's initial board of directors, hand-picked by DHS, would set the information-sharing rules, but the current draft of the bill gives it little guidance on what those rules should require and provides little privacy protection.

Some amendments could address these problems. The bill should narrowly define the cyberthreat information that can be shared. This would preclude the flow—the unnecessary flow of large streams of private communications through NISO to its Governmental members.

The bill should ensure that information shared for cybersecurity purposes is used for cybersecurity. This would prevent cybersecurity information sharing from devolving into something approaching a surveillance program. It would also prevent companies from using the data that is shared for commercial purposes unrelated to cybersecurity, such as for behavioral advertising.

The bill should require minimization of personally identifiable information and communication shared through NISO.

Finally, the information-sharing rule should be enforceable. The bill currently imposes no liability on private-sector employees and on employees of State and local governments who violate the information-sharing rules. These matters must be addressed in the legislation. NISO's board will not adopt rules to adequately address

them absent clear, strong, specific Congressional direction to do so. We caution you against amending the bill to permit information to flow to or from NISO, notwithstanding any law. Such provisions are almost sure to have unintended consequences.

The cybersecurity bill of the House Intelligence Committee reported last week includes such a provision, and it is coupled with an overbroad definition of cyberthreat. They worked together in that legislation to permit communication service providers to share with intelligence, law enforcement, and other agencies' ordinary user traffic that the providers routinely monitor for cyberthreats. It would be unwise to go down that road. Cybersecurity legislation need not override privacy and other laws to promote information sharing. An incremental approach is called for.

Targeted exceptions to privacy and other laws may be necessary and we will work with you to craft them. Thank you.

[The statement of Mr. Nojeim follows:]

PREPARED STATEMENT OF GREGORY T. NOJEIM

DECEMBER 6, 2011

Chairman Lungren, Ranking Member Clarke, and Members of the subcommittee: Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology.[1] We applaud the subcommittee for holding a hearing on draft legislation to address significant cybersecurity challenges. Clearly, cybersecurity is a growing problem that Congress needs to address, but with a careful, nuanced, and incremental approach in order to minimize the unintended consequences, such inhibiting innovation, diminishing privacy, or damaging civil liberties. We believe that the legislation you are considering is a good start in many ways and that it could use some improvements in key areas:

- The draft bill has a light regulatory touch, generally relying on market incentives rather than Government mandates to increase cybersecurity performance. This approach, which we favor, encourages companies to enhance their cyber defenses without forcing compliance with Government-imposed standards that could discourage security innovation.
- The regulation that the draft bill would impose extends primarily to owners and operators of critical infrastructure systems, so it is important to carefully define those systems.
- The draft bill wisely cements the role of the Department of Homeland Security as the lead Federal agency for cybersecurity for the civilian Government and private sectors, instead of putting an element of the Defense Department in this role.
- The draft bill appropriately avoids giving the Government authority to shut down or limit internet traffic in a "cybersecurity emergency."
- We are concerned about the information-sharing provisions of the draft bill and the impact that they could have on privacy. We will share our suggested changes to those provisions.

NETWORK PROVIDERS—NOT THE GOVERNMENT—SHOULD MONITOR PRIVATELY-OWNED NETWORKS FOR INTRUSIONS

One of the most important things to get right about cybersecurity—for civil liberties and for effectiveness—is to ensure that the private sector remains responsible for monitoring and protecting its own networks and that monitoring authority not be transferred, directly or indirectly, to the Government. When the White House released the Cyberspace Policy Review on May 29, 2009, President Obama embraced this principle, stating:

[1] The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the internet open, innovative, and free. Among our priorities is preserving the balance between security and freedom. CDT coordinates a number of working groups, including the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies, and trade associations interested in information privacy and security issues.

"Our pursuit of cybersecurity will not—I repeat, will not—include monitoring private sector networks or internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."

CDT strongly agrees. No Governmental entity should be involved in monitoring private communications networks as part of a cybersecurity initiative. This is the job of the private-sector communications service providers themselves, not of the Government. Most critical infrastructure computer networks are owned and maintained by the private sector. Private system operators know their systems best and they already monitor those systems on a routine basis to detect and respond to attacks as necessary to protect their networks; it is in their business interest to continue to ramp up these defenses.

At a top-line level, all of the major cybersecurity bills, including the legislation the White House has proposed, honor the administration's pledge. But Government monitoring of private-to-private communications likely will not occur through the front door. Rather, Government monitoring would most likely grow as an indirect result of information sharing between the private and public sectors or as an unintended by-product of programs put in place to monitor communications to or from the Government. For that reason, we focus extensively here on the information-sharing provisions of the draft bill. We conclude that they have benefits over the language in both the administration bill and the Cyber Intelligence Sharing and Protection Act reported by the House Intelligence Committee on December 1 (H.R. 3523), but we also see areas that need to be clarified or otherwise improved.

SHARING INFORMATION BETWEEN THE PRIVATE SECTOR AND THE GOVERNMENT

There is widespread agreement that the current level of cybersecurity information sharing is inadequate. Private-sector network operators and Government agencies monitoring their own networks could better respond to threats if they had more information about what other network operators are seeing. How to encourage more robust information sharing without putting privacy at risk is a central policy challenge that falls to Congress to resolve.

Preferred Approach to Information Sharing

CDT strongly recommends an incremental approach to the information-sharing problem. First, Congress should determine exactly what information should be shared that is not shared currently, and why it is not being shared. We believe that what is most important to share is attack signatures, information describing other exploits, and information identifying the source or attribution of attacks or probes. The assessment of current practices should start with an understanding of why existing structures, such as the U.S. Computer Emergency Readiness Team ("US–CERT")[2] and the public-private partnerships represented by the Information Sharing and Analysis Centers (ISACs),[3] are inadequate. The Government Accountability Office (GAO) has made a series of suggestions for improving the performance of US–CERT.[4] The suggestions include giving US–CERT analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing US–CERT sustained leadership within DHS that could make cyber analysis and warning a priority. All of these suggestions merit attention.

Second, an assessment should be made of whether the newly-established National Cybersecurity and Communications Integration Center (NCCIC) has addressed some of the information-sharing issues that have arisen. The NCCIC is a round-the-clock watch and warning center established at DHS. It combines US–CERT and the

---

[2] US–CERT is the operational arm of the Department of Homeland Security's National Cyber Security Division. It helps Federal agencies in the .gov space to defend against and respond to cyber attacks. It also supports information sharing and collaboration on cybersecurity with the private sector operators of critical infrastructures and with State and local governments.

[3] Each critical infrastructure industry sector defined in Presidential Decision Directive 63 has established an Information Sharing and Analysis Center (ISAC) to facilitate communication among critical infrastructure industry representatives, a corresponding Government agency, and other ISACs about threats, vulnerabilities, and protective strategies. See Memorandum from President Bill Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC–63) (May 22, 1998), *http://www.fas.org/irp/offdocs/pdd/pdd-63.htm*. The ISACs are linked through an ISAC Council, and they can play an important role in critical infrastructure protection. See The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection 1 (January 2009), *http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf*.

[4] See Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (July 2008), *http://www.gao.gov/products/GAO-08-588*.

National Coordinating Center for Communications and is designed to provide integrated incident response to protect infrastructure and networks.[5] Industry is now represented at the NCCIC[6] and its presence there should facilitate the sharing of cybersecurity information about incidents.

Third, Congress must make a realistic assessment as to whether an information-sharing model that puts the Government at the center—receiving information, analyzing it, and sharing the resulting analysis with industry—could ever act quickly enough to respond to fast-moving threats. Though the White House cybersecurity proposal[7] and the lead Senate bill, the Cybersecurity and Internet Freedom Act, (S. 413) adopt the Government-centric approach, we have serious concerns about it. An industry-based model, subject to strong privacy protections, would be able to act more quickly and would raise few, if any, of the Fourth Amendment concerns associated with a Government-centric model.

Fourth, Congress must account for the significant authority current law gives providers of communications service authority to monitor their own systems and to disclose to Governmental entities in formation about cyber attack incidents for the purpose of protecting their own networks. In particular, the Federal Wiretap Act already provides that it is lawful for any provider of electronic communications service to intercept, disclose, or use communications passing over its network while engaged in any activity that is a necessary incident to the protection of the rights and property of the provider.[8] This includes the authority to disclose communications to the Government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, under the Electronic Communications Privacy Act (ECPA), a service provider, when necessary to protect its system, can disclose stored communications[9] and customer records[10] to any Governmental or private entity.[11] Furthermore, the Wiretap Act provides that it is lawful for a service provider to invite in the Government to intercept the communications of a "computer trespasser"[12] if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to investigation of the trespass.[13] These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to Governmental entities but, rather, go a long way to authorizing the type of targeted information sharing that we believe is needed.

While current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, the law does not authorize service providers to make disclosures to other service providers or to the Government to help protect the systems of those other service providers. We believe it probably should. There may be a need for a very narrow exception to the Wiretap Act, ECPA, FISA, and other laws that would permit disclosures about specific attacks and malicious code on a voluntary basis and that would immunize companies against liability for these disclosures.

The exception would be narrow so that routine disclosure of internet traffic to the Government or other entities remains clearly prohibited. It would bar the disclosure to the Government of vast streams of communications data, but permit liberal disclosure of carefully defined cyber attack signatures and cyber attack attribution information. It may also need to permit disclosure of communications content that defines a method or the process of a cyber attack. Rather than taking the dangerous step of overriding the surveillance statutes, such a narrow exception could operate within them, limiting the impact of cybersecurity information sharing on personal privacy.

---

[5] See DHS Press Release announcing opening of the NCCIC, *http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.*

[6] See DHS Press Release announcing that it has agreed with the Information Technology Information Sharing and Analysis Center (IT–ISAC) to embed a full-time IT–ISAC analyst at the NCCIC, November 18, 2010, *http://www.dhs.gov/ynews/releases/pr_1290115887831.shtm.*

[7] The text and an analysis of the White House proposal are at *http://www.whitehouse.gov/omb/legislative_letters.*

[8] 18 U.S.C. § 2511(2)(a)(i).

[9] 18 U.S.C. § 2702(b)(3).

[10] 18 U.S.C. § 2702(c)(5).

[11] Another set of exceptions authorizes disclosure if "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications [or information] relating to the emergency." 18 U.S.C. §§ 2702(b)(8) and (c)(4).

[12] A "computer trespasser" is someone who accesses a computer used in interstate commerce without authorization. 18 U.S.C. § 2510(21).

[13] 18 U.S.C. § 2511(2)(i).

Information Sharing in the Draft Bill[14]

The draft bill establishes[15] the National Information Sharing Organization (NISO), a non-profit, quasi-Governmental organization to serve as a National clearinghouse for the exchange of undefined "cyber threat information"—including information derived from intelligence collection—among owners and operators of critical and non-critical networks and systems in the private sector, the Federal Government, State and local governments, and educational institutions. One of its goals would be to create a "common operating picture" by combining network and cyber threat warning information shared with the Federal Government and with NISO members designated by its board of directors. NISO would be required by law to ensure that information exchanged is stripped of all information that identifies the submitting entity, but it would not be required by law to minimize personally identifiable information that is shared. Threat and vulnerability information derived from intelligence collection could only be shared with cleared NISO members.

DHS would select NISO's initial board of directors. That board would set procedures for future board elections and criteria for membership in NISO by non-Federal entities. It would establish a governing charter setting information-sharing rules for NISO and its members, including the treatment of intellectual property, limitations on liability, measures to mitigate anti-trust concerns, and protections of privacy and civil liberties. NISO would determine the extent to which its own activities would be transparent to the public—information submitted to and exchanged through NISO would be exempt from disclosure under FOIA and information it shares with State and local governments would be exempt from disclosure under State law.

Participation in NISO would be mandatory for the Departments of Energy, Defense, and Homeland Security and the FBI. Other entities such as companies, State and local governments, and academic institutions would participate voluntarily by becoming members under criteria established by the NISO board of directors and by paying membership fees determined by the board.[16] Industry representatives would dominate its board of directors, which would include representatives of small business, seven critical infrastructure sectors, DHS, the Department of Defense, the Department of Justice, the intelligence community and the privacy and civil liberties community.[17]

Evaluation of the Proposed Information-Sharing Regime

At a top-line level, NISO would be something of a "super ISAC." Like an ISAC, it would be convened by the Government, devoted to cybersecurity information sharing, and dominated and paid for by industry. It would partner with the same Governmental and private organizations that an effective ISAC would. The largest differences are that NISO is not sector-specific, thus facilitating information sharing across sectors, that some of its information-sharing rules are guided by statute instead of being set by its members or governing board, and its enabling statute removes any doubt that classified cybersecurity information could be shared with participating entities cleared to receive it. Whether NISO will be effective or not seems to turn on whether it addresses deficiencies in the current ISAC/US–CERT structures. We suggest that you measure NISO against any identified shortcomings in these existing structures to ensure that the bill does not establish a redundant information-sharing entity.

We would make a number of suggestions to protect privacy and promote efficacy if the committee determines to move forward with NISO:[18]

> *1. Carefully define, with reference to existing law, the cyber threat information that can be shared with or through NISO.* It is not necessary to run a bulldozer through existing laws that protect privacy and other societal values with a pro-

[14] In addition to the information-sharing entity discussed at length below, the draft bill calls on DHS to facilitate information sharing and interactions and collaborations among Federal agencies, State and local governments and academic and international partners, to disseminate timely and actionable cybersecurity threat, vulnerability, and mitigation information, to compile and analyze risks and incidents regarding threats to Federal systems and critical infrastructure information systems, and to provide incident detection, analysis, mitigation, and response information to Federal agencies and to private entities and other Governmental entities that own or operate critical infrastructure. This is consistent with its duties today.

[15] It is not clear whether NISO is a newly-established non-profit, or whether an existing non-profit, or existing non-profits, would become NISO. This should be clarified.

[16] Up to 15 percent of NISO's annual expenses would come out of the DHS budget.

[17] Industry representatives would outnumber Governmental representatives by 2–1 and would outnumber privacy and civil liberties community representatives by 5–1.

[18] The NISO provisions are very much a work in progress and we will be suggesting some technical clarifications to staff that are not outlined here.

vision permitting the sharing of broadly-defined cyber threat information "notwithstanding any law." Such an open-ended exception would be damaging to privacy and would likely have adverse unintended effects. Both the White House information-sharing proposal and the House Intelligence Committee's Cyber Intelligence Sharing and Protection Act, H.R. 3523, have this defect.[19] In contrast, CIFA, the lead Senate bill, explicitly provides that cyber attack reporting must comply with the surveillance statutes, rather than override them.[20]

2. Restrict the purpose and use of the information being shared to cybersecurity. Cybersecurity should not become a back door for the flow of information to the Government for law enforcement purposes, or to the private sector to help it target advertising or for other commercial purposes unrelated to cybersecurity. The draft bill falls short in this area, permitting Government participants in NISO to use information shared to prosecute any crime,[21] and permitting industry participants to use the information for any commercial purpose, including commercial purposes that might be at odds with the interests of the party submitting the information. While the bill permits entities submitting information to NISO to impose use and disclosure restrictions on the information when it is disclosed to officials of the U.S. Government, this provides little comfort to the computer user to whom the disclosed information may pertain and whose interests may not align with those of the company submitting the information. We are particularly concerned about the degree to which personally identifiable information and communications content would flow to Governmental entities through the NISO. These issues should be addressed by law; rules and procedures the NISO board adopts will not be sufficient.

3. Make the restrictions on information sharing enforceable by people and entities aggrieved by violations. Companies that share carefully-defined cyber threat information through NISO should be insulated against liability for doing so. However, if they break the rules, there should be consequences. The current draft makes it a misdemeanor for an employee of the Federal Government to knowingly disclose without authorization cyber threat information protected against disclosure. There are no penalties if a State or local official or an employee of a company participating in the NISO makes a similar disclosure. The bill's penalties should apply to intentional violations by State or local officials or private-sector employees.

4. Require that information sharing to and from the NISO minimize the personally identifiable information and communications content that is shared. When cyber threat information includes PII or communications content that is not necessary to identify and respond to the threat, such information need not, and should not be shared, and the bill should so provide. Like the White House bill, it should require destruction of communications intercepted or disclosed for cybersecurity purposes that do not appear to be related to cybersecurity threats.

5. Ensure that information sharing by NISO members is voluntary. We assume that the bill does not intend to mandate information sharing, but proposed Section 248 in the draft bill, entitled "Voluntary Information Sharing," does not actually specify that information-sharing be voluntary. Instead, the bill permits the NISO board to set the information-sharing rules, which could be misread as permitting the board to adopt a rule that would require members to share information as a condition of membership. The enabling statute should prohibit the NISO board from adopting any such rule.

6. Enhance transparency with audits and Inspector General reports. DHS Inspector General should be required to issue an annual report that evaluates the efficacy of NISO's information-sharing activities and their impact on privacy. These reports should be public, but may have a classified annex. The bill could also require publicly-reported independent audits to ensure that information

---

[19] The House Intelligence Committee's bill defines cyber threat information so broadly that it would permit carriers to share all of the communications traffic they scan to protect their networks, and to share that traffic with the FBI, NSA, and other Governmental agencies. Our analysis of the bill can be found at *http://www.cdt.org/blogs/gregnojeim/112cyber-intelligence-bill-threatens-privacy-and-civilian-control.*

[20] S. 413, the Cybersecurity and Internet Freedom Act of 2011, proposed Section 246(c)(1)(A)(ii) to the Homeland Security Act.

[21] Since the prosecution of cybersecurity crimes serves a cybersecurity purpose, cyber threat information shared through the NISO could be used to prosecute such crimes, including violations of the Computer Fraud and Abuse Act.

sharing though NISO comports with statutory requirements and rules and procedures adopted by the NISO board.

7. Consider whether information sharing through NISO should be complemented by efforts to enhance information sharing directly within industry, subject to audits, reporting and other privacy controls. While it may have disadvantages, a distributed information-sharing system may be more nimble than a centralized, hub-and-spoke model.

CYBERSECURITY ROLE OF THE DEPARTMENT OF HOMELAND SECURITY AND OF DOD ENTITIES

The draft bill would firmly establish DHS as lead Federal agency responsible for improving the security of civilian Federal systems and for working with the private sector to improve the security of civilian critical infrastructure systems. Under the bill, DHS cybersecurity activities would include: Conducting risk assessments of Federal systems and, upon request, of privately-owned critical infrastructure information systems; facilitating adoption of new cybersecurity policies and practices; becoming a focal point within the Federal Government for protecting Federal systems and critical infrastructure systems; coordinating among Federal agencies and State and local governments, academia, and international partners on cybersecurity; developing a cybersecurity incident response plan; sharing information about cyber threats and vulnerabilities and mitigation strategies with Governmental agencies and with owners and operators of critical infrastructure information systems; and a host of other cybersecurity activities.

Putting DHS in the lead is the right approach, and in this regard the draft bill is superior to other proposals that could put an element of the Department of Defense—the National Security Agency or Cyber Command—formally or de facto at the head of civilian cybersecurity efforts. Some have suggested that these military entities be given a lead role because of their expertise and resources. We believe that to be most effective, the Government's cybersecurity program should harness the expertise and resources of the DOD, but a civilian agency must remain in control of the overall program in order to ensure transparency and thereby instill trust of the private sector and the public. Less transparency means less trust, less corporate participation, and less effectiveness of the Government's cybersecurity program.

Over 85% of critical infrastructure information systems are owned and operated by the private sector, which also provides much of the hardware and software on which Government systems rely, including the Government's classified systems. The private sector has valuable information about vulnerabilities, exploits, patches, and responses. Private-sector operators may hesitate to share this information if they do not know how it will be used and whether it will be shared with competitors. Private-sector cooperation with Government cybersecurity effort depends on trust. A lack of transparency undermines trust and has hampered cybersecurity efforts to date. In addition, without transparency, there is no assurance that cybersecurity measures adequately protect privacy and civil liberties and adhere to due process and Fair Information Practice Principles. Transparency is also essential if the public is to hold the Government accountable for the effectiveness of its cybersecurity measures and for any abuses that occur.

NSA and Cyber Command, operate, understandably, in a culture of secrecy that is incompatible with the information sharing necessary for the success of a civilian cybersecurity program. As a result, a DOD entity should not be given a leading role in monitoring the traffic on unclassified civilian Government systems, nor in making decisions about cybersecurity as it affects such systems; its role in monitoring private sector systems should be even smaller. Instead, procedures should be developed for ensuring that whatever expertise and technology DOD has in discerning attacks is made available to a civilian agency. We applaud steps taken in this direction, such as the September 27, 2010 MOU between DHS and DOD setting forth the terms by which each agency provides personnel, equipment, and facilities to increase collaboration and support and synchronize each other's cybersecurity operations.[22]

DESIGNATIONS OF CRITICAL INFRASTRUCTURE SHOULD BE NARROWLY TARGETED

DHS should concern itself only with genuinely critical infrastructure, and that infrastructure should be narrowly defined. A narrow definition focuses agency re-

[22] Memorandum Agreement Between DHS and DOD Regarding Cybersecurity, effective September 27, 2010, *http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.*

sources where they are most needed and ensures minimal conflicts with other regulatory regimes. Such a definition also ensures that the burdens of Government reporting and regulatory compliance are imposed only on private-sector network operators who are truly "critical" and limits impact on traditionally non-regulated entities.

In this regard, other cybersecurity proposals raise very serious concerns. The May 12, 2011 White House proposal does little to provide specificity, defining critical infrastructure as those entities whose incapacity or disruption would cause "a debilitating impact."[23] This standard is ambiguous and could sweep vast swaths of U.S. industry into a regulatory fold. The Senate's CIFA bill does a better job, and requires that the disruption of any critical infrastructure system would cause "a mass casualty event which includes an extraordinary number of fatalities," "severe economic consequences," "mass evacuations with a prolonged absence," or "severe degradation of National security capabilities, including intelligence and defense functions."[24]

The draft bill does better than either the administration proposal or the Senate bill. It defines covered critical infrastructure as a facility or function which, if destroyed, disrupted, or accessed without authorization, through exploitation of a cyber vulnerability, would result in: (i) loss of thousands of lives; (ii) major economic disruption, including disruption or failure of financial markets; (iii) mass evacuation of a major metropolitan area for longer than 30 days; or (iv) severe degradation of national security or non-military defense functions. While more precise than the definition of critical infrastructure in either the White House proposal or in CIFA, this definition, too, would benefit from more specificity.

It would be useful, for example, for the statute to define the level of economic disruption and of lives lost that would trigger coverage as "critical infrastructure." DHS has already drawn these lines in its definitions of Tier 1 and Tier 2 Critical Infrastructures and Key Resources, and DHS uses these more precise definitions to allocate resources used to protect critical assets. If the draft bill becomes law as written, DHS would have discretion in specifying what is critical and what is not. It could draw those lines as it already has or it could draw new lines. The question for the committee is whether Congress draws the lines that determine what assets are subject to DHS regulation or whether to leave that decision to DHS. We favor Congress drawing those lines in a transparent, precise, and measureable way. We also suggest that the draft bill be amended to include a meaningful appeal process companies could trigger when they believe an asset of theirs has been incorrectly designated as "critical infrastructure."

INCENTIVIZING RISK-BASED CONDUCT TO SECURE CRITICAL INFRASTRUCTURE

In terms of enhancing the security of private networks and systems, the Government may assist the private sector but it should not intrude into the details of private sector cybersecurity planning processes and it should not dictate technology standards. Certain agencies may have unique insights into burgeoning threats, specific attack signatures, or useful defensive techniques, but private-sector information technologists typically understand the operation of their own networks better than Government regulators. The goal should be to enhance the capability of the private sector, not to transfer it to the Government. Furthermore, when it comes to securing critical infrastructure, one size does not fit all. Existing regulatory regimes reflect this reality: The regime governing operation of a nuclear power plant is much more prescriptive that the regulatory regime governing most information technology. Cybersecurity measures should build on this insight.

The draft bill would authorize DHS, in coordination with Federal agencies and owners and operators of critical infrastructure, to assess cybersecurity risks to critical infrastructure and the harms that could result from disruption, destruction, or unauthorized use of critical infrastructure information systems. DHS would also catalogue internationally recognized consensus-developed risk-based performance standards and develop unspecified market-based incentives designed to encourage use of those standards. It would then coordinate with the relevant regulatory agencies and private-sector entities to work to include the risk-based performance standards in the regulatory regimes applicable to the covered critical infrastructure. This approach helps ensure alignment between existing regulatory regimes and performance standards DHS has identified. In cases where there is no existing risk-based

[23] White House proposal, proposed Section 3(b)(1)(A) of the Cybersecurity Regulatory Framework for Critical Infrastructure Act.

[24] S. 413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 254 of the Homeland Security Act and amendments to Section 210E of the Homeland Security Act.

security performance standard, DHS would work with the owners and operators of critical infrastructure to mitigate identified risks and would coordinate with international bodies to develop and strengthen standards to address the identified risks.

We believe this consultative, risk-based approach will contribute to cybersecurity without inhibiting innovation. It gives DHS flexibility to draw distinctions between different types of critical infrastructure and to work with industry to identify appropriate risk-based performance standards for each.

For the sake of privacy, innovation, and effectiveness, Government efforts to improve private-sector cybersecurity should adhere to several overarching principles. The Government should generally avoid technical mandates. DHS in particular should not have the power to dictate technical standards or to override a company's decisions about how to best protect its information systems. Nor should DHS have any enforcement power with respect to the performance-based standards it identifies. Instead, enforcement and oversight should occur through existing regulatory schemes. When trying to raise standards, the Government should generally avoid punitive measures. Penalizing companies that fall short of some standard will discourage the reporting of security incidents and will put the Government in the role of adversary rather than partner.

As we understand the section of the draft bill adding a new Section 227 to the Homeland Security Act, it adheres to these principles. In contrast, some of the Senate bills have been particularly worrisome in this regard, giving DHS open-ended regulatory powers to approve security plans and to penalize actors who fail to comply with those regulations.[25] Under the draft bill, existing regulatory regimes that already authorize a Governmental agency (other than DHS) to dictate technical standards for an industry or to override decisions of a particular company would remain in place. This seems appropriate—it would leave enforcement with those agencies already set up to regulate a given sector, most of which have already been addressing cybersecurity, sometimes for years. The draft bill seeks to empower those regulators with additional knowledge about risk-based performance standards. It would encourage DHS to play a consultative, rather than a directive role, and to work with industry rather than against it. We believe the bill is intended to leave decisions about the measures a company should take to reach the necessary level of performance where those decisions belong, with the people who know those systems best—the owners and operators of critical infrastructure information systems and the regulators who intimately know the industry. It might be appropriate to amend the bill to make the foregoing more explicit, as the White House did in its own legislative proposal.[26]

For companies that operate critical infrastructure in sectors that do not have an existing regulatory regime, the bill includes no mechanism to promote the adoption of internationally recognized, consensus-driven risk-based performance standards, other than market-based incentives and the existing authority of the Federal Trade Commission, which has brought cases against companies engaging in inappropriate security practices involving consumers' personal data. While this seems to leave a gap in oversight and enforcement, we believe that there is relatively little critical infrastructure that does not fall within an existing regulatory scheme. To the extent that there are such critical infrastructure systems that do not fall within an existing scheme (other than the FTC's overarching Section 5 authority), the committee to might consider whether it would be appropriate to require some level of transparency for companies of a certain size so that the public and/or Congress is made aware of when such companies fail to adopt and adhere to relevant standards. Any transparency requirement should not mandate disclosure of information that would tip off hackers to particular vulnerabilities.

PRESIDENTIAL AUTHORITY IN CYBERSECURITY EMERGENCIES

There has been much discussion about whether the President or the Department of Homeland Security ought to be given authority to limit or shut down internet traffic to or over a privately-owned[27] critical infrastructure information system in an emergency or to disconnect such systems from other networks for reasons of Na-

---

[25] S. 413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 250(c) of the Homeland Security Act (civil authorizing penalties for violators of Section 248, as added by the bill, which establishes a risk management regulatory regime).

[26] White House proposal, proposed Section 4(b)(5) of the Cybersecurity Regulatory Framework for Critical Infrastructure Act.

[27] Presumably, the Government already has the authority to disconnect its own systems from the internet and CDT does not challenge such authority.

tional security.[28] Through omission, both the draft bill, and the White House legislative package implicitly reject this dangerous idea, and we urge you to oppose any efforts that may be made to include it in any cybersecurity legislation.

To our knowledge, no circumstance has yet arisen that could justify a Governmental order to limit or cut off internet traffic to a particular privately owned and controlled critical infrastructure system. We know of no dispute where a critical infrastructure operator has refused to take appropriate action on its network that would justify the exercise of such a power. Operators have strong financial incentives to quarantine network elements and limit or cut off internet traffic to particular systems when they need to do so. They know better than do Government officials whether their systems need to be shut down or isolated.

In contrast, a new Presidential "shut-down" power comes with a myriad of unexamined risks. A shut-down could interfere with the flow of billions of dollars necessary for the daily functioning of the economy. It could deprive doctors of access to medical records and cripple communications among first responders in an emergency. These and other consequences could have world-wide effect because much of the world's internet traffic flows through U.S. networks.

Even if such power over private networks were exercised only rarely, its mere existence would pose other risks, enabling a President to coerce costly, questionable—even illegal—conduct by threatening to shut down a system.

Giving the Government the power to shut down or limit internet traffic would also create perverse incentives. Private-sector operators will be reluctant to share information if they know the Government could use that information to order them to shut down. Conversely, when private operators do determine that shutting down a system would be advisable, they might hesitate to do so without a Government order, and could lose precious time waiting to be ordered by the Government to shut down so as to avoid liability for the damage a shut-down could cause others.

Finally, the grant of unfettered "shut-down" authority to the President would give aid and comfort to repressive countries around the world. The Government of Egypt was widely condemned when it cut off internet services to much of its population on January 27, 2011, in order to stifle dissent. The United States should not now endorse such a power, even if only for cybersecurity purposes, because to do so would set a precedent other countries would cite when shutting down internet services for other purposes.

We urge you to reject proposals to give the President or another Governmental entity power to limit or shut down internet traffic to privately-held critical infrastructure systems.

CONCLUSION

We appreciate the opportunity to testify about the draft legislative proposal that is before the committee. We believe the legislation is in many ways a good start and that its light regulatory touch would enhance cybersecurity without stifling innovation. The bill would benefit from some substantial tightening of the information-sharing provisions, and we have suggested a number of changes. We look forward to working with you on those changes and on other provisions of the draft legislation as it moves through the legislative process.

Mr. LUNGREN. Thank you very much, Mr. Nojeim.

Mr. Kosar.

STATEMENT OF KEVIN R. KOSAR, ANALYST IN AMERICAN GOVERNMENT, CONGRESSIONAL RESEARCH SERVICE

Mr. KOSAR. Chairman Lungren, Ranking Member Clarke, Members of the subcommittee, on behalf of the Congressional Research Service I would like to thank you for the opportunity to testify today.

CRS was asked to examine draft legislation to amend the Homeland Security Act of 2002 to establish a National Information-Sharing Organization, or NISO. CRS' examination focused solely upon

[28] The leading Senate cybersecurity bill, S. 413, the Cybersecurity and Internet Freedom Act, includes such a provision. For an analysis, see *http://www.cdt.org/blogs/greg-nojeim/does-senate-cyber-bill-include-internet-killswitch.*

the organizational structure of NISO and does not address cybersecurity policy.

My written testimony provided a preliminary examination and analysis of NISO as presently proposed. In my limited time here, I will briefly review NISO's proposed structure and provide comments on it.

The draft legislation would establish NISO as a not-for-profit organization for sharing cyberthreat information and exchanging technical assistance, advice, and support, and developing and disseminating necessary information security technology. NISO would have a 15-person board of directors that initially would be appointed by the Secretary of the Department of Homeland Security. Board members would include a representative from DHS, four persons from Federal agencies with cybersecurity responsibilities and ten individuals from the private sector.

After the first year, the private-sector members would be replaced through elections held by NISO. As my written statement indicates, NISO would appear to meet CRS' definition of a quasi-Governmental entity. It would be a Government-established organization that combines the legal characteristics of both the Governmental and private sectors. NISO would be authorized by Federal statute and required to serve purposes set by Federal statute. Yet NISO also would be led by a board comprised mostly of individuals from the private sector, and NISO would be mostly funded by the private sector.

In the limited time available, I was able to locate only one precedent for an organization that was substantially structured like NISO: SEMATECH, which Congress established by a statute in 1987. That said, NISO would have notable differences from SEMATECH. Now, quasi-Governmental organizations are not new in the United States. Congress chartered the quasi-Governmental First Bank of the United States in 1791. Quasi-Governmental entities can be creative vehicles for addressing complex public policy issues.

However, for Congress an enduring question with quasi-Governmental entities is the matter of accountability; specifically, how to ensure a partially or mostly private organization will faithfully execute the law and be responsive to policymakers.

Now, trying to ascertain how an organization might behave based upon examining its statute is inherently challenging as its plain organizational behavior is affected by non-statutory factors, such as the quality of its management and the Federal Government's oversight thereof.

With those caveats noted, based upon a preliminary analysis, NISO appeared to likely be an organization that would operate in a largely self-directed private-sector manner.

I suggest this based upon the following observations:

First, the draft legislation would have Federal representatives fill a minority, five, of the 15 board positions. The rest would be private-sector representatives.

Second, the board itself, not the President or the DHS Secretary, would have the authority to choose NISO's chair and co-chair, and these persons must be private-sector representatives. Additionally, the board would also be empowered to incorporate NISO as an or-

ganization, set all its rules for operations, employment, and compensation, and to appoint its officers.

Third, who would actually do the day-to-day work of NISO is unclear. NISO's board would choose one or more operators based upon the criteria set in section 241(d). Additionally, whether board members would be full-time employees actively engaged in operational oversight is not clear.

Fourth, NISO would appear to have considerable discretion to decide which non-Federal organizations would be permitted or able to join NISO.

Fifth, there would not appear to be any requirement that GAO or an inspector general be able to audit or examine NISO's books. NISO would not be required, so far as I can tell, to provide annual reports to the Congress and the President on its operations and whether or not it is reaching its benchmarks.

Sixth and finally, the draft legislation would limit the Federal Government's contribution to no more than 15 percent of NISO's annual operating costs. Whether the threat of losing that 15 percent contribution would be a sufficient carrot to encourage on-going NISO compliance to Government direction is not clear.

I will conclude my testimony here. If CRS may be of further assistance to you, I and my colleagues stand ready to help. Once again, thank you for the privilege to appear before you today.

[The statement of Mr. Kosar follows:]

PREPARED STATEMENT OF KEVIN R. KOSAR

DECEMBER 6, 2011

INTRODUCTION

Chairman Lungren and Ranking Member Clarke, and Members of subcommittee—on behalf of the Congressional Research Service, I would like to thank you for this opportunity to appear before you today.

CRS was asked to examine draft legislation that would amend the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.; HSA) for multiple purposes.[1] In particular, CRS was asked to provide its observations on Section 3 of the draft legislation, which would amend Title II of HSA to establish a National Information Sharing Organization (NISO).

Per your request, this written statement focuses solely upon the organizational structure of the NISO.[2] It first describes the organizational attributes of NISO as proposed in draft legislation, and then provides observations on NISO as a type of quasi-Governmental entity.

ORGANIZATIONAL ATTRIBUTES OF THE PROPOSED NISO

The draft legislation would establish NISO as a "not-for-profit organization for sharing cyber threat information and exchanging technical assistance, advice, and support and developing and disseminating necessary information security technology." The draft further defines the NISO's purpose as:

"serving as a National clearinghouse for the exchange of cyber threat information so that the owners and operators of networks or systems in the private sector, educational institutions, State, Tribal, and local governments, entities operating critical infrastructure, and the Federal Government have access to timely and actionable information in order to protect their networks or systems as effectively as possible."

The NISO would have a 15-person Board of Directors that would be appointed by the Secretary of the Department of Homeland Security. Board members would include a representative from the Department of Homeland Security, four persons

[1] The draft legislation supplied by the committee is dated November 2, 2011 (1:58 p.m.).

[2] Thus, no analysis is provided of the role the NISO would play in the realm of cybersecurity policy or how NISO would integrate or coordinate with existing cybersecurity authorities.

from Federal agencies with "significant responsibility for cybersecurity," and 10 individuals from the private sector. These latter appointees would include two representatives from the "privacy and civil liberties community," and eight representatives of critical infrastructure stakeholders, including: Banking and finance, communications, defense industrial base, energy (electricity, oil, and natural gas), health care, and information technology. Each Board member would serve 3-year terms, and private sector members would be replaced through elections held by the NISO.[3]

The Board would be empowered to incorporate the NISO, to choose its own chairperson and co-chairperson, and to devise all bylaws and rules for the operation of NISO. The draft bill does not address explicate whether NISO Board Members would be full-time employees or what their compensation would be.

The draft legislation would limit the Federal Government's contribution to 15% of NISO's annual operating costs.

OBSERVATIONS

NISO: A Governmental, Private Sector, or Quasi-Governmental Entity?

According to the discussion draft, the NISO would appear to meet CRS's definition of a quasi-Governmental entity: A Government-established organization that combines the legal characteristics of both the Governmental and private sectors.[4] As Table 1 indicates, the NISO would have attributes that are Governmental, private sector, and hybrid (both Governmental and private sector).

TABLE 1.—ATTRIBUTES OF THE PROPOSED NISO

Governmental Attributes	Private Sector Attributes	Hybrid Attributes
Authorized by Federal statute.	Board members would incorporate the NISO by filing incorporation papers with a non-Federal authority (e.g., a State or District of Columbia).	The Board of Directors is comprised of 10 private-sector representatives and 5 Federal agency representatives.
Required to serve purposes set by Federal statute.	The NISO would have the authority to establish its own operating procedures and mission statement.	NISO would be funded by both the Federal Government and the private sector.
Secretary of Homeland Security appoints the Board of Directors.	The NISO is explicitly exempted from the Freedom of Information (Act 5 U.S.C. 552).	NISO membership is partially set by statute, and partially devised by NISO's Board of Directors.

When Congress creates quasi-Governmental entities, it tends to do so on an ad hoc basis. That is, each quasi-Governmental entity is crafted by a separate statute, and that statute is sculpted according to a variety of policy and political considerations. That caveat noted, CRS previously has identified a number of types of quasi-Governmental entities.[5] The entities for each of these types share basic organizational attributes (e.g., GSEs are for-profit), and these quasi-Governmental types are listed in Table 2.

TABLE 2.—TYPES OF QUASI GOVERNMENTAL ENTITIES IDENTIFIED BY CRS

Type	Example
Quasi-Official Agencies	State Justice Institute.
Government-Sponsored Enterprises	Fannie Mae.

[3] The initial private-sector Board members would serve 1-year terms, and then would be replaced through elections. Whether said members would be permitted to seek re-election is not addressed by the legislation.

[4] Generally, see CRS Report RL30533, *The Quasi Government: Hybrid Organizations with Both Government and Private Sector Legal Characteristics,* by Kevin R. Kosar.

[5] CRS Report RL30533, *The Quasi Government: Hybrid Organizations with Both Government and Private Sector Legal Characteristics,* by Kevin R. Kosar.

TABLE 2.—TYPES OF QUASI GOVERNMENTAL ENTITIES IDENTIFIED BY CRS—Continued

Type	Example
Federally-Funded Research and Development Centers	Sandia National Laboratories.
Agency-Related Nonprofit Organizations	(See below):
Adjunct Organizations Under the Control of a Department or Agency.	National Pork Board.
Organizations Independent of, But Dependent Upon, Agencies.	Henry M. Jackson Foundation.
Nonprofit Organizations Affiliated with Departments or Agencies.	National Park Foundation.
Venture Capital Funds	In-Q-Tel.
Congressionally Chartered Nonprofit Organizations	American Legion.
Instrumentalities of Indeterminate Character	U.S. Investigation Services.

Source.—CRS Report RL30533, *The Quasi Government: Hybrid Organizations with Both Government and Private Sector Legal Characteristics.*

As presently proposed, the NISO could be characterized as an agency-related nonprofit organization. NISO would be a non-profit organization and it would have an affiliation with the Department of Homeland Security by virtue of the Secretary's role in selecting a minority of NISO's board members.

However, NISO organizationally would not fit neatly into any of the subtypes of agency-related non-profit organizations above. Rather, it would possess characteristics associated with all three subtypes. Like the National Pork Board and other agricultural check-off entities, it would charge its members fees. As with the Henry M. Jackson Foundation, the NISO would undertake a research agenda that is broadly defined in statute. And like the National Park Foundation, the NISO would be affiliated with a Federal agency and have Federal representatives on its board.[6]

One particularly notable aspect of the NISO as currently proposed is that it would charter itself. Typically, quasi-Governmental entities are chartered via Federal statute; the law itself incorporates the entity. Such charters typically set forth the corporation's: (1) Name; (2) purpose(s); (3) duration of existence (limited or in perpetuity); (4) governance structure (e.g., executives, board members, etc.); (5) powers; and (6) the schema for Federal oversight (e.g., annual reporting).[7]

In the limited time available, CRS could locate only one recent precedent for self-chartering—the Semiconductor Manufacturing Technology (SEMATECH) consortium—an entity established by Congress in 1987 (Pub. L. 100–180, Part F; 101 Stat. 1068).[8]

Congress established SEMATECH in response to the United States' growing dependency upon Japan for semiconductors.[9] Viewing this as a National security vulnerability, SEMATECH was a quasi-Governmental entity comprised of more than a dozen major domestic semiconductor manufacturers, such as AT&T Microelectronics and Intel.[10] SEMATECH was a research and development enterprise whose purposes were to "encourage the semiconductor industry in the United States—(A) to conduct research on advanced semiconductor manufacturing techniques; and (B) to develop techniques to use manufacturing expertise for the manufacture of a variety of semiconductor products." SEMATECH was affiliated with the Department of Defense (DoD) but was led and staffed by the private-sector stakeholders (not Government appointees and employees).

---

[6] A board comprised of representatives of both the Government and private sector is not unusual for quasi-Governmental entities. The American National Red Cross, which chartered a century ago, is a well-known example. Federal representation on the board of the Red Cross was changed most recently in 2007. Pub. L. 110–26 authorizes the President to appoint one board member and to name the chairman of the board. CRS Report RL33910, *The Charter of the American National Red Cross: Current Issues and Proposed Changes,* by Kevin R. Kosar.

[7] CRS Report RS22230, *Congressional or Federal Charters: Overview and Current Issues,* by Kevin R. Kosar, p. 1.

[8] A copy of SEMATECH's legislation is attached to this memorandum.

[9] CRS Report 92–749 SPR, *SEMATECH: Issues in Evaluation and Assessment,* by Glenn J. McLoughlin. (Archived report available from the author of this report.)

[10] CRS Report 91–831 SPR, *SEMATECH Facts,* by Glenn J. McLoughlin. (Archived report available from the author of this report.) SEMATECH also had an adjunct organization, SEMI/SEMATECH, comprised of approximately 130 U.S. equipment suppliers and materials suppliers.

The costs of SEMATECH were shared between the Federal Government and the private sector—the Federal Government funded SEMATECH via grants authorized by the Secretary of Defense, and SEMATECH charged its members annual dues.

While NISO and SEMATECH share some organizational attributes, there are at least two considerable differences (Table 3). First, SEMATECH's legislation required the DoD and SEMATECH operate under a memorandum of understanding (MOU) that provided the DoD with certain authorities over SEMATECH, such as the authority to participate in the development of SEMATECH's annual operating plan. Additionally, SEMATECH's statute created an Advisory Council on Federal Participation in SEMATECH. This 12-person panel was comprised of both Federal stakeholders and Presidential appointees from the private sector.[11] The panel advised "Sematech and the Secretary of Defense on appropriate technology goals for the research and development activities of Sematech and a plan to achieve those goals," and conducted annual reviews of its progress.[12] The draft legislation for the NISO does not include similar provisions.

TABLE 3.—COMPARISON OF SELECTED NISO AND SEMATECH ORGANIZATIONAL ATTRIBUTES

Similarities	Differences
Self-chartering.	MOU between SEMATECH and DoD.
Affiliated with a Federal agency.	Advisory Council on Federal Participation in SEMATECH.
Funded by the Federal Government and private sector.	
Private sector leadership and employees.	

QUASI-GOVERNMENTAL ENTITIES: RATIONALES, ACCOUNTABILITY, AND NISO

Benefits and History

Congress has been establishing quasi-Governmental entities since the Nation's founding. For example, Congress chartered the First Bank of the United States in 1791 (1 Stat. 192, Section 3) to stabilize the Nation's currency and provide a safe depository for funds and serve as a source of credit. The bank was a hybrid entity—it was capitalized through a stock offering, and both the Federal Government and private investors purchased shares. The bank's debt was the Nation's debt. Private shareholders elected most board members, and the Treasury Department was authorized to inspect the bank's accounts.

The creation of Federal quasi-Governmental entities has increased since the 1960s. Many arguments have been advanced to support the creation of these hybrid organizations. However, the current popularity of the quasi-Government option may be traced to the following impetuses:

1. the desire to avoid creating another Federal "bureaucracy;"
2. the current controls on the Federal budget process that encourage Federal agencies to rely less on annual appropriations;
3. the desire to make Government operate more like a private-sector organization; and
4. the belief that management flexibility requires entity-specific laws and regulations, and thus exemption from Government-wide management statutes (e.g., Administrative Procedure Act; 5 U.S.C. 551 et seq.)[13]

[11] The members were: The Under Secretary of Defense for Acquisition, who served as chair; the Director of Energy Research of the Department of Energy; the Director of the National Science Foundation; the Under Secretary of Commerce for Economic Affairs; the Chairman of the Federal Laboratory Consortium for Technology Transfer; and seven Presidential appointees who were to include four members "who are eminent individuals in the semiconductor industry and related industries;" two members "who are eminent individuals in the fields of technology and defense;" and one member "who represents small businesses."

[12] Additionally, SEMATECH's legislation required annual independent audits of SEMATECH and Comptroller General review of these audits. SEMATECH had to submit its audits to Congress and the DoD Secretary. No reporting or audit requirements are including in the draft legislation for the NISO.

[13] CRS Report RL30533, *The Quasi Government: Hybrid Organizations with Both Government and Private Sector Legal Characteristics,* by Kevin R. Kosar, p. 1. On the Federal Government's management laws, see CRS Report RL30795, *General Management Laws: A Compendium,* Clinton T. Brass, Coordinator.

Many quasi-Governmental entities exist, and many have been considered to be successful. The National Park Foundation, for example, annually raises significant private support for the Nation's public parks.[14]

Cost

With quasi-Governmental entities there also may come a cost—reduced accountability to Federal Governmental direction.[15]

An organization's institutional structure can affect its accountability to Congress and the President. In simplest terms, the more tightly yoked to Legislative and Executive Branch authorities an organization is, the more responsive to those authorities the organization can be expected to be. Hence, if organizations are considered as existing on a spectrum—with a wholly-Governmental agency on one end and a wholly-private firm on the other—the former would tend to be the most accountable and responsive to Federal direction, while the latter the least.

This organizational responsiveness to Federal direction comes through a number of means, including: (1) Federal involvement in the appointment of the organization's leadership; (2) the organization's location within or outside the Government; (3) requirements for annual auditing and reports to Federal authorities (Congress, the President, and agency heads); and (4) the organization's reliance on appropriated funding.[16]

Assessed on these criteria, NISO might be expected to behave independently of the Federal Government (Table 4).

TABLE 4.—ORGANIZATIONAL ACCOUNTABILITY AND NISO

	NISO
Federal appointees	Minority; 5 of 15 directors would be Federal representatives; the board would choose its chair and co-chair, who cannot be Federal representatives.
Location within or outside the Government.	Private sector; not explicitly placed within a Federal agency or branch of Government.
Annual auditing and reporting requirements.	None.
Reliance on appropriated funding	Low Federal contribution (not more than 15% of annual operating costs).

Organizational accountability to overseers, it has been noted, is not an unalloyed good. A frequent criticism of Federal Governmental entities (such as agencies) is that they are too responsive to diverse Federal oversight authorities. Their efforts to satisfy the demands of diverse stakeholders may result in underperformance of an agency's general or National policy objectives.[17] As noted above, one of the arguments for establishing a quasi-Governmental entity is the intention that it operate less like a Governmental entity and more like a private firm.[18]

Additionally, an aspect of organizational accountability is predictability, that is, that the entity created will behave as its creators expect. When Congress establishes an entity, Governmental or quasi-Governmental, it inevitably includes in the statutes the "purposes" of the organization and provides the organizations with authorities to attain its purposes.

In public administration parlance, there is a principal-agent relationship, wherein Congress (the principal) has established an agent (the entity) to execute the law. Quasi-Governmental entities sometimes behave unpredictably should they be estab-

[14] National Park Foundation, 2011 Annual Report, at *http://www.nationalparks.org/files/about/financials/annual-report-2011.pdf.*

[15] Jonathan G.S. Koppell, *The Politics of Quasi Government: Hybrid Organizations and the Control of Public Policy* (New York: Cambridge University Press, 2003); and Ronald C. Moe, "The Emerging Federal Quasi Government: Issues of Management and Accountability," *Public Administration Review,* vol. 61, iss. 3, May/June 2001, pp. 290–312.

[16] An organization that is required to be self-financing will have a strong incentive to act in its own self-interest, possibly at the cost of fully pursuing its statutorily-prescribed goals or complying with Government-prescribed operational rules.

[17] For example, Congress established Base Realignment Commissions in order to close unneeded DoD facilities. CRS Report 97–305, *Military Base Closures: A Historical Review from 1988 to 1995,* by David E. Lockwood and George Siehl.

[18] The presumption is that a private firm will perform more optimally than a Governmental one.

lished with starkly competing organizational imperatives. Governmental entities are to pursue policy objectives (e.g., National defense, poverty reduction, etc.); private firms pursue private objectives (e.g., profit, financial self-perpetuation, etc.) Arguably, the Government-sponsored enterprises, Fannie Mae and Freddie Mac, serve as examples of the unpredictability of entities driven by competing Governmental (diverse housing policy goals) and private-sector imperatives (maximizing private shareholder value).[19]

Whether NISO would face strongly competing organizational imperatives is unclear.[20] Unlike the GSEs, the NISO would be a not-for-profit organization and would not have stockholders. Its objective is a collective good—improving security against cyber threats, an end which each stakeholder has an interest in but cannot attain alone. NISO's board would have both Governmental and private-sector representatives, whose interests may or may not coalesce.[21]

The legal framework within which organizations operate can greatly influence their behavior by setting incentives and expectations for operations.[22] Quasi-Governmental entities sometimes behave unpredictably due to their ambiguous legal nature. When Congress establishes a fully Governmental entity, such as an agency, many of entity's attributes are set by default. That is, absent statutory provisions exempting the agency from Federal laws and regulations, the agency is subject to them.[23] The Federal Government-wide management laws are many, and include statutes such as the aforementioned Administrative Procedures Act, the various civil service employment and compensation statutes (5 U.S.C. 101 et seq.), and the Lobbying with Appropriated Monies Act (18 U.S.C. 1913).[24] Government agencies' actions also are bound by various Constitutional limitations. Oppositely, when a private individual or group establishes a corporation, this private entity will not be subject to the general management laws that are applicable to Federal agencies.

The United States, then, "has two distinctive forms of law: public law, which governs the activities of governmental bodies in their capacities as agents of the sovereign . . . and private law, which governs the relations of private parties with one another."[25] Thus, when Congress creates quasi-Governmental entities that are not clearly Governmental nor private sector, confusion may result as to which laws

---

[19] These GSEs' statutes contain five different public policy objectives. CRS Report R40800, *GSEs and the Government's Role in Housing Finance: Issues for the 112th Congress,* pp. 2–3. See also Koppell, *The Politics of the Quasi Government,* chapter 5; and Congressional Budget Office, *Controlling the Risks of Government-Sponsored Enterprises* (Washington: GPO, 1991), chapter 1.

[20] As NISO resembles SEMATECH, Congress may find value in reviewing the performance of SEMATECH.

[21] Determining the alignment of interests among the board's Governmental and private-sector board interest goes beyond the scope of this memorandum and would involve cybersecurity policy and other considerations.

[22] Thomas H. Stanton, "Assessing Institutional Development: The Legal Framework That Shapes Public Institutions," in Robert Picciotto and Ray C. Rist, eds., *Evaluating Country Development Policies and Programs: New Approaches for a New Agenda* (Jossey-Bass, 1995), pp. 55–68.

[23] Ronald C. Moe, "The Importance of Public Law: New and Old Paradigms of Government Management," in Phillip J. Cooper and Chester A. Newland, eds., *Handbook of Public Law and Administration* (Jossey-Bass, 1997), p. 46. To be clear Congress may exempt a Governmental or quasi-Governmental entity from coverage by a particular Government management statute. For example, in 1995 the Supreme Court considered the issue of distinguishing between a Governmental and private corporation. The National Railroad Passenger Corporation (AMTRAK) established by Congress (45 U.S.C. 451), and enumerated under 31 U.S.C. 9101 as a "mixed-ownership corporation" (e.g., it was owned by both the private and Governmental shareholders), was sued by Michael Lebron for rejecting, on political grounds, an advertising sign he had contracted with them to display. Lebron claimed that his First Amendment rights had been abridged by AMTRAK because it is a Government corporation, and therefore an agency of the United States. AMTRAK argued, on the other hand, that its legislation stated that it "will not be an agency or establishment of the United States Government" and thus is not subject to Constitutional provisions governing freedom of speech. The Court decided that, although Congress can determine AMTRAK's Governmental status for purposes within Congress's control (e.g., whether it is subject to statutes such as the Administrative Procedure Act), Congress cannot make the final determination of AMTRAK's status as a Government entity for purposes of determining Constitutional rights of citizens affected by its actions. *Michael A. Lebron* v. *National Railroad Passenger Corporation;* 513 U.S. 374 (1995). The AMTRAK Reform and Accountability Act of 1997 (Pub. L. 105–134; 111 Stat. 2570) removed AMTRAK from the GCCA list of mixed-ownership Government corporations.

[24] CRS Report RL30795, *General Management Laws: A Compendium.*

[25] Moe, "The Importance of Public Law: New and Old Paradigms of Government Management," p. 42.

apply to the quasi-Governmental entity.[26] To cite just four examples, quasi-Governmental entities have found themselves in legal disputes involving questions as to which courts may hear suits against them, which Government-wide management laws apply to them, to what extent they need to respect a private citizen's First Amendment rights, and the constitutionality of prohibiting the removal of their directors except for cause. [27]

It is difficult to anticipate how predictably the proposed NISO would behave due to its ambiguous nature. The draft legislation for NISO does not explicitly state whether it is a Governmental entity or a private-sector entity. By virtue of the provision that the entity should charter itself (presumably under State law), it might be assumed that it is intended to be private. The legislation also exempts the NISO from the anti-trust provisions of the Clayton Act (15 U.S.C. 12), a statute which apply to private-sector firms.

However, the draft legislation also would make non-applicable to NISO two Government management statutes, the Freedom of Information Act (5 U.S.C. 552) and the Federal Advisory Committee Act (5 U.S.C. Appendix). Furthermore, as NISO would be designed to serve as an "information-sharing" venue regarding cybersecurity issues, the draft legislation does provide for the protection of this information. It would forbid "any officer or employee of the United States or any Federal agency" from knowingly disclosing information regarding a cyber threat. Violators could be removed from their positions, fined, and imprisoned. Whether such information protections would apply to all NISO directors and employees is unclear.

Mr. LUNGREN. Thank you very much for the testimony of each member of the panel. I appreciate you staying within the time limits assigned. We will have a round of questions and I will start with 5 minutes.

Dr. Nojeim, thank you—or Mr. Nojeim, thank you very much for your testimony. I wonder if you might elaborate on why it is important that the DHS is the lead agency in charge of civilian cybersecurity. We generally speak about the notion that under our Constitutional Governmental structure, it is both explicit and implicit that there is civilian control of the military. This administration engaged in a memorandum of understanding between DOD and DHS so that you have some cross-fertilization there, but I think they have done a pretty good job of making sure that we don't violate the notion of civilian control of the military. We happen to think it was important in this bill to make it clear that DHS was in charge of civilian cybersecurity. But I wonder if you would elaborate a little bit on that issue.

Mr. NOJEIM. Thank you for the question. I agree, the bill does cement DHS as the lead for civilian cybersecurity operations. That is important because those operations need to be transparent, and they need to be transparent because the private sector controls about 85 percent of the critical infrastructure that needs to be protected. It needs to be able to trust that information it shares will

---

[26] Statutes establishing quasi-Governmental entities often include provisions exempting the entity from a particular Government management law. SEMATECH, for example, was exempted from the Freedom of Information Act (5 U.S.C. 552). Yet, this effort at clarification may lead Federal overseers to question whether the statute's silence regarding other Government management laws implies that they are applicable to the entity. Currently, Congress is considering whether the Freedom of Information act ought to apply to the GSEs Fannie Mae and Freddie Mac since they are in Federal receivership and effectively Government-owned. See CRS Report R42080, *Fannie Mae, Freddie Mac, and FOIA: Information Access Policy for the Government-Sponsored Enterprises,* by Wendy Ginsberg and Eric Weiss.

[27] Respectively, see Michael T. Maloan, "Federal Jurisdiction and Practice: The American National Red Cross and the Interpretation of 'Sue and Be Sued' Clauses," *Oklahoma Law Review,* vol. 45, 1992, pp. 739–760; *Animal Legal Defense Fund* v. *Shalala,* 104 F.3d 424 (D.C. Cir 1997); *Michael A. Lebron* v. *National Railroad Passenger Corporation* (513 U.S. 374 (1995)); and *Free Enterprise Fund, et al.* v. *Public Company Accounting Oversight Board, et al.,* 561 U.S. _____, 130 S.Ct. 3138, 177 L.ed.2d 706 (2010).

be used for the proper purposes, and it needs to know what is going on because that will encourage the private sector to cooperate.

In a military-led operation, something led by NSA or Cyber Command wouldn't be able to build that trust, because for otherwise legitimate reasons they operate secretly. So I think the administration is right to try to draw on the expertise of Cyber Command and NSA without putting those agencies in control of a civilian program.

Mr. LUNGREN. Directed to both Dr. Shannon and Ms. McGuire, during the both formal and informal discussions we had, both the Republican task force and this committee, and other things that we have done with our Democratic counterparts in the past, there seem to be at least to me a consensus that with the structures we already have, as good as they may be in the different industry sectors, the idea that timely access of information of threat from the Government to the private sector has been an issue, and the issue of trust; that is, that we have not established the mechanism by which the private sector is encouraged to share more of their information in a timely fashion, I guess in some ways because we haven't articulated the limits of the use of that information. Why are you going to self-report if there is some liability on the other end? So on our efforts in coming up with this draft, we came up with a concept of NISO.

Can you give us your thoughts on, if you disagree or if you agree, why this shouldn't be done by already existing structures, or what problems we have with the suggestion we have got in the bill right now? Ms. McGuire.

Ms. MCGUIRE. So first off, I think there is a couple of issues that we see on a regular basis with the current system. One is that we don't see that timely actionable information coming from the Government flowing to industry. So we have a little bit of a chicken-and-an-egg problem here. Industry doesn't see valuable information coming from Government, therefore industry doesn't perceive the need to provide information back to the Government.

But we also see a situation where industry is not necessarily incentivized to provide information to the Government. There is not a clear articulation of what kind of information the Government needs from industry. I have actually sat in meetings where I have had Government folks actually say to me: Well, just give us everything. Well, that is impossible. I don't think the Government has enough data centers to store all the information that industry has, nor do they want it.

Mr. LUNGREN. Nor do you want to give it all to them.

Ms. MCGUIRE. Nor do we want to give it all to them. Exactly. So we have a little bit of that situation. So I think that this notion of incentivizing industry to share more information is a really important concept that is articulated in the bill.

To your question about why current structures in existence shouldn't be used for the NISO, my view is that we already have private industry engagement and buy-in to a NISO-like concept and that we really do need to build on those existing structures and frameworks that we have in place. So if there is a way to articulate this NISO framework that includes those existing struc-

tures, I think you will get a lot more buy-in from industry than trying to set up a separate new entity.

Mr. LUNGREN. Dr. Shannon.

Mr. SHANNON. Thank you. I have four quick points. One is the notion of sharing information has been evolving for over 2 decades, and the need for timeliness and what information there is, the technologies involved, the players involved, the civil liberties issues involved, have been evolving. So I think that is part of why you see in that second diagram this jumble of links is kind of what has accrued over the decades. This sort of legislation I think is another important attempt to try and get it to the right point.

Incentives are about encouraging the emergence of a capable organization. We are not going to know, a priori, what the right incentives are, so I suggest soft incentives rather than hard incentives, such as tax breaks and such, to encourage people to consider doing the right thing. As you see them doing the right thing, then you can provide for their encouragement for those lagging behind.

As Ms. McGuire mentioned, I think feedback, timely feedback from the Government to private entities is a missing capability, and that really will cement the deal. It is about valued propositions on both sides. Regardless of how much the private industry is paying up front, if anything, the fact is they invest a tremendous amount in cybersecurity on their own, and so any involvement has a price and they want to know kind of how they can benefit from that for the benefit of their shareholders and their customers. Thank you.

Mr. LUNGREN. Ms. Clarke is recognized for her questions.

Ms. CLARKE. Thank you, Mr. Chairman. Thank you to our panelists for your testimony here this morning.

My first question is posed to Ms. McGuire and to Dr. Shannon and to Mr. Nojeim. There is general agreement that enhanced information sharing is key to improving cybersecurity. For DHS' part, it has worked diligently to support sector ISACs as forums for information sharing and has stepped up its cyber operations with the creation of NCIC and US–CERT. There is limited cybersecurity resources, financial and personnel, in the private sector and Government.

If the NISO was established, how do we guard against these limited resources being diverted from existing efforts to the new platform?

Ms. MCGUIRE. Well, I think that your statement about the limited resources is a particularly challenging area for the Department of Homeland Security. As a former employee, I actually was the director for awhile, as well as a deputy director of the National Cybersecurity Division in the US–CERT, with first-hand knowledge and experience of some of those resource challenges. I think they are particularly challenged, though, by a lot of staff turnover amongst their leadership. This is creating a continuity issue there. So the progress that they have made thus far with the NCIC, while I think it is commendable given the current situation, there is still a long way to go. In particular, dealing with private industry, the level of which we are seeing information sharing has not matured to a level where I think it is creating the kind of value proposition that Dr. Shannon just talked about, and that effort really needs a

focused concerted effort by the Department and its leadership if we are going to realize this information sharing. I am not even going to say nirvana, just a progress step forward.

Mr. SHANNON. Thank you. There are two elements. One is that there is a desire to reach a broad spectrum very quickly. Some of the programs that you talked about, the NCIC and the DIB programs, for example, are just beginning to scale and still haven't demonstrated what the challenges are going to be in reaching full scale. So I see the current NISO effort as being—it will help existing efforts by in some sense taking the pressure off and trying to reach a broader audience faster, as opposed to waiting for these smaller efforts to mature.

Mr. NOJEIM. We think that an incremental approach is called for, an examination of why information sharing under the current structures isn't working. Then once those problems are identified, Congress should ask, well, does NISO address each one? If it doesn't, then you are creating a redundant information-sharing entity. But if it does, you are creating one that will solve problems. So that is the approach that we would recommend.

Ms. CLARKE. I fully understand where all three of you are coming from, but the issue, though, is resources, right? So if we are at a point where resources are limited and there is a possibility that there could be some redundancy, how do we sort of reconcile that? You could have a situation where you are spread so thin that no one meets their mission, and I don't know whether that has been a consideration, given the entities that we currently have that are working on these efforts—we are now considering an additional, and how we would make sure that they have what they need to meet their mission.

So I wanted to just sort of get a sense of, you know, is there something innovative that you can think of that would maybe make one of the entities self-funding, I don't know. But it would appear to me that if we have all of these entities out there, many of whom have not fully stood up yet but are going to require a resource in order to meet their mandates, that is something that we ought to consider up front.

Mr. SHANNON. If I might add, setting measures of success and expectations of success I think is important. It goes back to being operationally and scientifically valid, to know what the intention of the organization is and how you will know when that organization's mission is being met. As I mentioned, because of the evolving threat, landscape, and technologies, what works today may not work as well tomorrow. So it is difficult to divine what the right organization is today. So I encourage you to consider multiple efforts such as we do have today, but I would agree that consolidation to the current budget environment is important.

Ms. CLARKE. Thank you, Mr. Chairman.

Mr. LUNGREN. Thank you. The gentleman from Texas, Mr. McCaul, is recognized for questioning.

Mr. MCCAUL. Thank you, Mr. Chairman. Let me commend you for this legislation. I think it provides clarity and guidance as to who should be in charge. For a long time we have talked about who is in charge of cybersecurity in the Federal Government. For a long

time NSA was not coordinating with the Department of Homeland Security, and they are now.

But when we talk about the issue of information sharing, which is critical to protecting these infrastructures, that is where I think this bill really comes into play. Mr. Nojeim, you talked about civilian control, and I agree with that assessment. There is a bill that was passed out of the Intelligence Committee that does not really specify which agency within the Federal Government should be in charge of this effort of information sharing. Some would argue that the NSA, because of the pilot program, the Defense industrial base pilot program, that NSA is the best agency to conduct that.

I tend to disagree with that assessment, because as you mentioned, civilian control is important here. In terms of international sharing of information, I don't think going to the intelligence community is going to be the right answer to this issue.

So with that, I just want to throw that out to the panel. Who do you see is the best agency to be in charge of this critical component of information sharing? I personally think it should be DHS. Tell me why I am right, or maybe why I am wrong, in that assessment.

Mr. Nojeim, if you want to lead on this.

Mr. NOJEIM. I will start. As I said a minute ago, civilian control will promote the transparency that is essential to building cooperation and trust with the private sector. You got to have the private sector involved because they own and operate most of the critical infrastructure.

But thinking for a minute through what the House Intelligence Committee did, one thing they did that seems like a good idea is to unlock the classified information, particularly the classified attack signatures that the NSA has, for the benefit of industry. It is important to accomplish that in legislation. If that legislation stopped there, with this flow of information from the intelligence agencies to private network operators who could then use it to protect their systems, we would support it.

The problem with that bill is that it opens a flow back to the intelligence agencies and to Cyber Command, and to other Governmental agencies that are not specified at all, of information from the private sector that could include regular user communications. It is important to limit that flow back, and I think that your bill, the bill that you are looking at, could do that with some very targeted amendments.

Mr. MCCAUL. Dr. Shannon and Ms. McGuire, what is your assessment in terms of who should be the lead agency?

Mr. SHANNON. I have to say no comment, thank you. We are a Federally-funded research and development laboratory.

Mr. MCCAUL. I understand. Ms. McGuire, you may have the same response.

Ms. MCGUIRE. We believe that a civilian agency is the right and appropriate authority for this entity. As a global private company, it is very difficult for us to operate in a global playing field if we have this kind of interaction direct with some of the other agencies.

Mr. MCCAUL. For a long time we have had the ISACs. The Information Sharing Analysis Centers have been kind of the vehicle for information sharing in the past. I think this bill actually provides again that clarity that I think is needed.

The ISACs have not been totally functional. They haven't worked as I think they were expected to work. I think this is a good opportunity to really put something in place in legislation that can be a real vehicle for information sharing. Do you all agree with that assessment?

Ms. MCGUIRE. While I agree that the NISO as a concept and a framework can seek to accomplish that, I do have concerns about ensuring that those existing entities, such as the ISACs and the sector coordinating councils, that industry has put so much effort and resources into over the last 10 years, do not go by the wayside. I am a firm believer that we have to improve those entities. I think that the information sharing and the direct engagement with Government has not always been, shall I say, as positive between the ISACs and the Government agency of DHS. I would be happy to share some specific examples with you after this hearing when there is more time.

Mr. MCCAUL. How would you recommend merging—I see my time is about expired—how would you recommend merging the existing—you know, the ISACs—with this National information sharing organization?

Ms. MCGUIRE. Well, I think that is something that we need to explore more in depth, because those ISACs for the most part are privately funded, privately incorporated, industry-owned and -operated entities, and so I think we need to have that dialogue of how we would incorporate them into this framework.

Mr. MCCAUL. Dr. Shannon, do you have any comments?

Mr. SHANNON. One comment is, again, going back to measures of expectations. When you stand up, whether it is the ISACs or any other entity over the last couple of decades, there were original intentions about what they should be able to achieve. Some of the things they were able to achieve and some things they were not, for various reasons. So I think doing a critical assessment at the current time of what those needs are would be helpful. I mean that is part of what CERT and the SEI has been involved in in assisting the Government with the DIB evaluations that have gone on. It is excruciating, but I think in the end it was very valuable to policymakers.

Mr. MCCAUL. We look forward to your comments following up on how we can best merge these entities. Mr. Chairman, my time is expired. Thank you.

Mr. LUNGREN. Thank you. Mr. Walberg is recognized for his questions.

Mr. WALBERG. Thank you, Mr. Chairman. Living in a delegation who has the dubious distinction of having the Chairman of the Intelligence Committee in our delegation, with a perverted sense of just giving us enough information about cybersecurity potential attacks and causing us to not sleep as much as he, I think that is a challenge that we have. So I appreciate your efforts here and I appreciate the panel being here today as well.

Mr. Kosar, let me ask you, is there anything in the draft language regarding the structure of NISO that in your opinion would prevent the NISO from accomplishing its mission?

Mr. KOSAR. It is difficult to say. I think one underlying requirement for the organization to be functional is that organizations

have to feel it is going to be a safe space where they can share information and that the information is not going to get out. I looked over the information protection provisions, and I confess I just didn't quite fully understand whether there were sufficient incentives to ensure that NISO participants did not leak or illicitly share information and cause damage to members.

Mr. WALBERG. How could that be remedied?

Mr. KOSAR. I honestly don't know at this point. I would have to think further about it and consult with my colleagues.

Mr. WALBERG. Okay. You were going on. I apologize for jumping in.

Mr. KOSAR. Oh, sure. No, I think one interesting aspect that I gleaned from looking at this is that if NISO is able to get up and running and to gain a reputation for appearing to be a very sound organization, private-sector members might want to flock to be part of this organization, not only because they could get information from it which is valuable to it, but also because it might kind of create a sort of Good Housekeeping Seal of Approval for companies who are participants. So that might be a pull factor and encourage collaboration.

Mr. WALBERG. Thank you.

Ms. McGuire, you evidently have a lot of personal experience with DHS and its cybersecurity mission. With regard to the authorities provided to DHS in the draft bill, are there any left out?

Ms. MCGUIRE. I don't think so. I mean, I read the draft legislation in detail, of course, in preparing for the hearing and I don't see anything there that—or didn't see anything that was missing, no.

Mr. WALBERG. Well, a credit to the bill sponsor then. Let me follow up and ask you if you could explain what you mean by risk assessment and any examples that you might have where a risk assessment approach has been used to protect against the cyberthreats.

Ms. MCGUIRE. So when we talk about risk assessment we are really looking at what are the threats, vulnerabilities, and consequences of any particular threat vector. With regard to specific examples where risk assessments have been used, the IT sector endeavored in 2009 to develop a sector-wide, not a company-by-company, but a sector-wide risk assessment to look at specific risk to the IT sector at large. We worked in concert, public-private partnership, with DHS to develop that risk assessment and we identified some specific areas in DNS routing, identity management, supply chains, some specific areas that we felt that we needed as a sector to focus some more detail on.

As a follow-on to that work, we developed some specific guidance that was released earlier this year to provide to IT sector companies' owners and operators, to help them focus on particular risks that we saw from a National level to the sector. Interestingly enough, what that risk assessment, though, demonstrated was that we as an industry were largely resilient because we had a lot of redundancies and processes in place to deal with incidents such as cybersecurity attacks and things of that nature, but there still were areas that we need to improve on.

So from a risk assessment standpoint, we believe that that allows companies to focus in their resources and efforts on what they should potentially be protecting according to that National-level risk.

Mr. WALBERG. Thank you.

Mr. Nojeim, how important do you think it is for the Department of Homeland Security to identify sector-specific cybersecurity risks?

Mr. NOJEIM. I think that having a sector-specific approach helps DHS modulate its level of regulation of cybersecurity information systems. So, for example, you wouldn't want, as Cheri said earlier, you wouldn't want a situation where the same kind of security performance standard is applied to a nuclear power plant as is applied to something that is much less dangerous but it fits within a definition of covered critical infrastructure. So DHS needs to have the flexibility to adopt a risk-based approach, and I think that the bill gives it that flexibility.

Mr. WALBERG. Thank you.

Mr. LUNGREN. We have time for a second round. So I just remember the old deal about tomato-tomahto, we now have "NESO" and "NISO." I asked my staff what is it, and they said, Well, since you wrote the legislation you can say. We will wait until later until we figure that one out.

Mr. Nojeim, we talked about protection of privacy and civil liberties, how important they are. Would limiting the type of information that is shared with the NISO and then limiting how that information can be used by members, including the Federal Government, address your concerns; and how would you define that?

Mr. NOJEIM. I think NISO can be nice to civil liberties. The way it could do that, I would define it as, first, I would start with attack signatures. Everybody agrees that cyber attack signatures ought to be freely shareable. There may be a need also to define cyberthreats with reference to actually overcoming a technical control, something that is in place to stop unwarranted access to a database. We think that this information can be defined, we think it can be defined broadly enough to permit the share of information that is necessary, and we have provided some language to your staff and we will continue to work with your staff on that language.

Mr. LUNGREN. Ms. McGuire and Dr. Shannon, if NISO is going to be successful, there has to be some value there for the private sector as well as for the Government. But we are the Government setting this concept up, so I suppose we should be appealing to the private sector. So it has got to be value.

So as I think, Ms. McGuire, you mentioned, it has got to be something that is unique or something that they can't get otherwise, because otherwise why buy into this?

On the other hand, in terms of the participation of the private sector, we could set up rules, as suggested by Mr. Nojeim, to say this is the limitation on the use of the information by the Government that has been given to them by the private sector.

But does the concept of subsequent liability protection come into play, or is that something we don't have to discuss? If I'm making a decision for myself or my company as to whether I should share this information with the Government, even through this entity, I might be dissuaded if I thought that is going to subject me to a

slew of lawsuits. Do we have to deal with that concept? I know there are other things to figure out. Have they followed proper procedures and so forth before they—but is that something that is necessary, or is that a concept that is redundant or unnecessary?

Mr. SHANNON. As I testified back in June, the notion of safe harbor protections I think is important. You want to free the people involved in incidents and collecting using the information.

Mr. LUNGREN. I know it is important. Is it crucial?

Mr. SHANNON. I think it is. You want to enable organizations to do the right thing.

Mr. LUNGREN. Ms. McGuire, is it necessary?

Ms. MCGUIRE. I would agree with that, yes.

Mr. LUNGREN. Mr. Nojeim, do you have any problems with that?

Mr. NOJEIM. I think it is important that there be consequences for breaking the rules. If the rules are followed, I think there should be immunity for people who are following the rules. For people who are breaking the rules, I think there should be consequences. Without them, you put companies between a rock and a soft place.

Mr. LUNGREN. Ms. Clarke.

Ms. CLARKE. Thank you, Mr. Chairman.

Dr. Kosar and Mr. Nojeim, in your testimony, you mention that, as designed in the proposed legislation, it would be difficult to know how the NISO would behave. The lack of predictability, even as the Federal Government invests significant resources, is a concern. Please explain the possible risks to the Government of establishing this quasi-Governmental entity without specificity as to its range of activities and responsibilities to its members; more especially, DHS.

Mr. KOSAR. Well, I guess the first question that I would have is whether or not the NISO would see strong incentives to coordinate its activities with the Department and to be responsive to the Department's needs, or would it have incentives to basically act otherwise?

A second issue or question I would have is: If this organization does not stand up well, will it have long-term negative ramifications for future efforts to do something on this? Will it kind of poison the well in some way, shape, or form? As I mentioned earlier, it seems like this kind of consortium for sharing this information is heavily based upon trust, and if something gets done incorrectly, there could be a lot of very bad feelings all around.

Third is the question of predictability. One thing I noticed in the mission for this organization is that on the one hand it is to be a place where information and advice is to be shared. But it is also a place where there seems to be R&D activities that will be undertaken to develop new technologies to aid in cybersecurity production.

So you have kind of two different operational activities, and I guess the question that entered my head is, these new technologies, are these going to be sold to companies? Will they be given to members of NISO? Will this organization split itself off and create a for-profit side organization?

It is not unprecedented that organizations created by the Federal Government have in the past, without Congress' expecting it, to

have split themselves and have divided themselves into multiple organizations. So I guess those would be my thoughts.

Mr. NOJEIM. I actually think that the bill includes a number of provisions that will allow the Government to protect its own interests in NISO. First, it reserves a number of seats on the board of directors to Governmental entities. Many of NISO's member entities, the ones who receive information, will be Governmental entities, State, and local, and Federal.

It also gives the Department of Homeland Security the ability to partially fund NISO. One could discuss whether 15 percent is enough or not, but it is a significant chunk of money. But the Government has something that NISO members will want. It has classified information about attacks that in a way give it a lot of leverage, maybe more leverage than it ought to have, over NISO's operations.

So I think that as it is structured, there is actually enough—there are enough provisions in the bill to protect the Government's interests in the NISO.

Ms. CLARKE. So in other words, you are saying that the way that the bill is currently constructed it should mitigate risk; is that what you are saying? Because I'm asking about possible risk.

Mr. NOJEIM. I think you were asking about whether the bill, as structured, protects the Government's interests in the NISO. My answer is I think it does, because I think it gives the Government substantial authorities. In fact, if we were drafting the bill, we would probably more limit the Government's participation and make it more clearly a privately-run entity as opposed to a Governmental entity.

One of our biggest concerns is the flow of personally identifiable information to Government members of NISO through the NISO entity.

Ms. CLARKE. Thank you.

Then just a final question. Dr. Kosar, you mentioned that the legal framework within which organizations operate can greatly influence their behavior by setting incentives and expectations for operations. You are a specialist in American Government, and in your opinion how does the legal framework described in this proposed legislation for NISO lend itself to defining the actions, incentives, and goals of the organization?

Mr. KOSAR. Well, I really appreciate the point brought up just a moment ago about DHS possibly having a lever for dealing with the NISO by virtue of its access to classified information policy. I think that is a subtle insight.

This entity, as structured, is primarily private-sector; and so presumably, its incentives lie with the perceived self-interest of the members.

Just going back to the example of SEMATECH, created in 1987, that was an organization—that legislation is substantially similar to this one. It created an organization of kind-of like firms, firms that produced, manufactured, semiconductors here in the United States. It looked at them and said, you have a shared interest in upping your technology and jumping forward, vis-à-vis Japan. This was a shared goal, and you guys can work together on this, you just need a little Government coordination.

Here we have, I think, members that are a little more diverse than those that were participating in SEMATECH. I guess an open question for me is whether or not the individual incentives of these organizations align as neatly as they did with SEMATECH. Because of this organization's success it would seem to me to be largely dependent on the activities of the private-sector parties.

Ms. CLARKE. Thank you, Mr. Chairman.

Mr. LUNGREN. Thank you very much. I think the questions of the hearing have indicated the fact that we are going into a new area here. We are trying to create a platform that makes sense for both the private sector side and the Governmental side. It is creating a mechanism in which there are incentives so that all will cooperate.

We thank you for your thoughts on this. We seek your thoughts in the future as we move forward. We intend to move on this because the issue is one that cannot wait. I am encouraged by the interest that we have received from our colleagues on both sides of the aisle, from people in the administration, from those in the private sector, because I think that is a good sign that while we are certainly not perfect, we are at least moving forward with a concept in an area that needs to be dealt with.

I want to thank all witnesses for your valuable testimony and the Members for their questions.

The Members of the subcommittee may have some additional questions for you. We would ask if we would submit them to you, that you would respond to these in writing. The hearing record will be held open for 10 days.

The subcommittee stands adjourned.

[Whereupon, at 11:25 a.m., the subcommittee was adjourned.]