S. HRG. 111–667

CYBERSECURITY: NEXT STEPS TO PROTECT OUR CRITICAL INFRASTRUCTURE

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

FEBRUARY 23, 2010

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

57–888 PDF WASHINGTON : 2010

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
MARK PRYOR, Arkansas
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
TOM UDALL, New Mexico
MARK WARNER, Virginia
MARK BEGICH, Alaska

KAY BAILEY HUTCHISON, Texas, *Ranking*
OLYMPIA J. SNOWE, Maine
JOHN ENSIGN, Nevada
JIM DEMINT, South Carolina
JOHN THUNE, South Dakota
ROGER F. WICKER, Mississippi
GEORGE S. LEMIEUX, Florida
JOHNNY ISAKSON, Georgia
DAVID VITTER, Louisiana
SAM BROWNBACK, Kansas
MIKE JOHANNS, Nebraska

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
ANN BEGEMAN, *Acting Republican Staff Director*
BRIAN M. HENDRICKS, *Republican General Counsel*
NICK ROSSI, *Republican Chief Counsel*

CONTENTS

WITNESSES

APPENDIX

CYBERSECURITY: NEXT STEPS TO PROTECT OUR CRITICAL INFRASTRUCTURE

TUESDAY, FEBRUARY 23, 2010

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 2:40 p.m. in room SR–253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. Welcome, all. And this hearing will come to order. And members will be coming in.

Before I give my opening statement, I just want to make sure that everybody knows who is testifying. And Vice Admiral Michael McConnell, U.S. Navy, Retired, Executive Vice President of National Security Business, Booz Allen Hamilton. He and I have done a lot of work together, including on FISA, other matters. Dr. James Lewis, Director and Senior Fellow, Technology and Public Policy Program Center for Strategic and International Studies. And Dr. Lewis is there, working on his computer, I think. Mr. Scott Borg, Director and Chief Economist, U.S. Cyber Consequences Unit. And Rear Admiral James Arden Barnett, Jr., Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission. I'm really glad about that. And Ms. Mary Ann Davidson, Chief Security Officer, Oracle Corporation. So, you're going to have some attention focused on you today.

This Nation—is it OK if I proceed? OK. This Nation and its citizens depend enormously on communication technologies in so incredibly many ways every single day. Vast network expansions have transformed virtually every aspect of our lives: education, healthcare, how businesses grow, don't grow, function, and the development of an interconnected, more democratic conversation. Our government, our economy, our very lives rely on technology that connects millions of people around the world in real time and all the time. And yet, these powerful networks also carry great risks which people, for the most part, don't understand—understandably don't understand—but are going to have to come to understand.

In recent years, hackers have attacked numerous Federal agencies, key media outlets, large companies across the private sector, targeting intellectual property, stealing valuable information vital to our national and economic security.

What was it? An article I read in the paper, somebody from DOD says, "We're getting attacked every day, all day, 7 days a week." And that's what they do. And these attacks are coming with increasing regularity and increasing sophistication. A major cyber attack could shut down our Nation's most critical infrastructure: our power grid, telecommunications, financial services; you just think of it, and they can do it—the basic foundations on which our communities and families have been built, in terms of all of their lives and who are trying to have a future.

So, this hearing is a next step in examining the important action we should be taking right now, as a government and as a national economy, to harden our defenses and safeguard critical infrastructure against a major cyber attack. Having said that they're happening all the time, that would seem to be out of order, but, you know, it needs—both need to be said.

Now, I understand it's no secret that cybersecurity is one of my top securities; it isn't a secret, at least, to Olympia Snowe and myself. As the former Chair of the Intelligence Committee, and now Commerce, I know that it's both national security and our economic security at stake. But, obviously, I'm not alone. Many experts, business leaders, public officials, including two of our former directors of national intelligence, have pointed, time and time again, to cybersecurity as this country's chief security problem.

President Obama called cyberspace a strategic national asset. However, this very important point, critical to the challenge we're discussing here today, unlike the other strategic national assets, cyberspace is 85-percent owned and controlled by private companies and individuals. That means that no one—neither the Government nor the private sector—can keep cyberspace secure on their own. Both must work together. All must work together. And that is why the wonderful Senator Snowe, from Maine, and I have introduced comprehensive legislation—the Cybersecurity Act 2009—to modernize the relationship between the Government and the private sector on cybersecurity.

And I have to say that on—there's—it's such a sensitive subject, particularly with the private sector, that I—we were on our fourth draft, because we kept calling in the stakeholders. They kept saying, "Well, this is wrong, this is wrong, this is wrong." And so, we would adjust, and do another one. I mean, we did it the way legislation should be developed.

Our legislation calls for developing a cybersecurity strategy and identifying the key roles and responsibilities of all the players, private and public, who will respond in a time of crisis.

I'm sure you've all heard about last week's Cyber ShockWave exercise. I watched. The process made it enormously clear; if we are serious about responding effectively to real cyber emergencies, we need a very strong top-level coordination. Too much is at stake for us to pretend that today's outdated cybersecurity policies are up to the task of protecting our Nation and/or our economic infrastructure.

We have heard the reassurances and seen the best efforts of the many in the private sector working to secure their networks. But, it's clear that even the largest, most sophisticated companies are not immune from attack. So, we have to do better. And that means

it will take a level of coordination and sophistication to outmatch our adversaries and minimize, as much as possible, the threats. So, it's that simple. We can't wait; we've got to get going on this. We've got to get people educated on it. And it's a massive, massive undertaking.

I want to introduce, to speak first—one, because he has to leave at 4 o'clock and, second, because he's kind of senior around here—Admiral Mike McConnell, who, you know, was NSA, DNI, private sector, and we worked together very closely on FISA and other legislation.

So, I now call upon Admiral—I'm very aware that you have to go——

Admiral MCCONNELL. Yes, sir.

The CHAIRMAN.—and we will work that, and make it work. But, Senator Snowe ranks here today.

No, but I want you to make an opening statement, if you want to.

Well, John, that's a quandary. I mean, you know, Olympia ought to make a little bit of an opening statement. You could take a 3-minute opening statement.

STATEMENT OF HON. OLYMPIA J. SNOWE,
U.S. SENATOR FROM MAINE

Senator SNOWE. OK. Thank you, Mr. Chairman, you're so gracious and generous.

I also want to take this opportunity to commend you for your extraordinary leadership on this paramount issue for the security of our Nation. And I also want to extend my sincere appreciation to our esteemed witnesses here today who represent a combined depth and breadth of knowledge and experience to provide invaluable insight into the multiple facets of this threat posed by cyberintrusion and attack and how we should mobilize as a nation to leverage both the public and the private sector to confront this exceptional challenge.

As Senator Rockefeller indicated, we filed a comprehensive cybersecurity bill, just a year ago, to accomplish that. We have since had multiple drafts. We are trying to bring new, high-level governmental attention to developing a fully integrated, thoroughly coordinated public private partnership, as we see this as the only means to address our Nation's 21st-century vulnerability to cybercrime, global cyberespionage and cyber attacks.

As crossover members of both the Intelligence Committee and the Commerce Committee, Senator Rockefeller and I, are keenly aware of the gravity of these circumstances and the astonishing dimensions of this threat. Moreover, our legislation reflects the recommendations of the Center for Strategic and International Studies' Blue Ribbon Report that was issued to the President. And the bill has undergone a number of revisions, following literally hundreds of meetings with industry and government thought leaders on this vital subject.

We sought to carve a course for our country to embrace a national security policy that will protect and preserve American cyberspace, which the President has rightly deemed a strategic national asset, because it is simply undeniable that the interconnec-

tion and integration of global systems, the very backbone of our functioning modern society, creates myriad opportunities for cyber attackers to disrupt communications, electrical power, and other indisputably essential services. And over the past several years, let there be no mistake, cyberexploitation activity has grown more sophisticated, more serious, and more targeted.

According to the Director of National Intelligence, Dennis Blair, a burgeoning array of state and non-state adversaries are increasingly targeting the Internet, telecommunications networks, and computers. And we're being assaulted on an unprecedented scale by well-resourced and persistent adversaries seeking to gain a glimpse into America's mission-critical vulnerabilities.

In an unclassified setting just 2 weeks ago, the Director testified that the national security of the United States, our economic prosperity, and the daily functioning of our government are dependent on a dynamic public and private information infrastructure that is now severely threatened. As the Director also noted, the recent intrusions reported by Google that appear to have originated in China should serve as a wake-up call to those who have not taken this problem seriously. That's why Senator Rockefeller and I have said that our failure to implement effective policies and procedures to prevent unauthorized intrusions have proven extremely consequential. And if we fail to take swift action, we risk a cybercalamity of epic proportions, with devastating implications for our Nation.

We've already experienced breaches to our supply chains. According to the SANS Institute, there have been several incidents involving infected memory sticks sold in U.S. retail stores. Furthermore, the FBI has alerted the Administration that malevolent actors have actually begun selling counterfeit networking equipment infected with viruses to consumers. Indeed, government agencies, as well as the private sector, are identifying an increasing number of security incidents. According to Verizon, more electronic records were breached last year than the previous 4 years combined, resulting in loss of privacy, identity theft, and financial crimes. Today, hijacked personal computers, known as "botnets" are used to send spam or viruses. And all of this is done without the owner's knowledge.

And just this week, according to a recently released report from NetWitness, hackers gained access to data at close to 2,500 companies and government agencies, from credit card transactions to intellectual property over the last 18 months, in a coordinated global attack. In fact, it was described as one of the largest and most sophisticated attacks, in the Washington Post this month.

Then, according to a report drafted by the chief information security officer of In-Q-Tel, the CIA's venture capital arm, hackers currently charge about a penny for every thousand e-mails of spam, and only $1 for a credit card that includes every piece of information necessary to compromise one's credit.

I commend the President for deeming cybersecurity a top priority and recently naming Howard Schmidt, whom Senator Rockefeller and I met with just a few weeks ago, as the Administration's national cybersecurity coordinator. However, we remain concerned that this position does not possess the institutional heft that it re-

quires. We would prefer and recommend, in our legislation, a Cabinet-level, Senate-confirmed national cyberadviser that reports directly to the President and is directly accountable to the American people.

It is imperative that the public and private-sectors marshal our collective forces in a collaborative and complementary manner to confront this urgent threat and reduce the risk posed by cyberintrusion or catastrophic cyber attack. As part of this effort, we must identify incentives for the private sector. Limiting liability for the companies that improve their cybersecurity posture, improving threat information-sharing, providing a safe harbor for exchanging vulnerability data, as well as tax credits contingent on a company complying with certain security practices, should all be considered.

It is equally urgent that government take proactive steps, always mindful of privacy concerns. The Government should work with the private sector to recognize and promote cybersecurity performance measures and best practices and develop a robust workforce of cybersecurity professionals, promote innovation and excellence in products and services, and institute a campaign, as Senator Rockefeller has indicated, to educate the public about cybersecurity risk, using the Government's purchasing power, as well, to raise standards through procurement.

Ultimately, we must recognize that time is not on our side, and it's clear that our adversaries will continue to change their tactics as technology evolves. Congress must take action.

I look forward to hearing from our distinguished witnesses and working closely with the Chairman and all members of this committee and others, and throughout the Congress, in order to accomplish this goal this year.

Thank you.

[The prepared statement of Senator Snowe follows:]

PREPARED STATEMENT OF HON. OLYMPIA J. SNOWE, U.S. SENATOR FROM MAINE

Thank you, Mr. Chairman, and I would like to take this opportunity to commend you for your extraordinary and visionary leadership on this paramount issue for the security of our Nation.

I also want to extend my sincere appreciation to our esteemed witnesses for joining with us today. All of you bring to bear a combined depth and breadth of knowledge and experience to provide invaluable insight on the multiple facets of the threat posed by cyber intrusion and attack, and how we should mobilize as a nation to leverage both the private and public sector to confront this exceptional challenge.

Indeed, Senator Rockefeller and I filed a comprehensive cybersecurity bill almost a year ago to accomplish *just that*. We sought to bring new high-level governmental attention to developing a fully integrated, thoroughly coordinated public-private partnership as that is the *only* way we can address our Nation's 21st century vulnerability to cyber crime, global cyber espionage, and cyber attacks.

As crossover members of both the Intelligence and Commerce committees, Senator Rockefeller and I are keenly aware of the gravity as well as the *astonishing dimensions* of the threat. Moreover, our legislation reflects the recommendations of the CSIS report to President Obama, and the bill has undergone a number of revisions following literally hundreds of meetings with industry and government thought-leaders on this vital subject.

Senator Rockefeller and I sought to carve a course for our country to embrace a national security policy that will protect and preserve American cyberspace, which the President has rightly deemed a "strategic national asset." Because it is simply *undeniable* that the *interconnection and integration* of global systems—the very backbone of our functioning modern society—creates myriad opportunities for cyber attackers to disrupt communications, electrical power, and other indisputably essen-

tial services. And over the past several years, let there be *no mistake*—cyber exploitation activity has grown more *sophisticated* . . . more *targeted* . . . and more *serious*.

According to *Director of National Intelligence Dennis Blair*, a burgeoning array of state and non-state adversaries are increasingly targeting the Internet . . . telecommunications networks . . . and computers . . . and we are being assaulted on an unprecedented scale by well-resourced and persistent adversaries seeking to gain a glimpse into America's mission-critical vulnerabilities.

In an unclassified setting just 2 weeks ago, the Director testified that "the national security of the United States, our economic prosperity, and the daily functioning of our government are dependent on a dynamic public and private information infrastructure" that is now "severely threatened." As the Director also noted, the recent intrusions reported by Google that appear to have originated in China should "serve as a wake-up call to those who have not taken this problem seriously."

That is why Senator Rockefeller and I have said that our failure to implement effective policies and procedures to prevent unauthorized intrusion has proven *extremely consequential*, and if we fail to take swift action, we risk a cyber-calamity of epic proportions with devastating implications for our Nation.

We have already experienced breaches to our supply chain. According to the SANS (Systems Admin, Audit, Network, and Security) Institute there have been several incidents involving infected memory sticks sold in U.S. retail stores. Furthermore, the FBI has reportedly alerted the administration that malevolent actors have actually begun selling counterfeit networking equipment infected with viruses to consumers.

Indeed, government agencies *as well as* the private sector are identifying an increasing number of security incidents. According to Verizon, more electronic records were breached last year than the previous 4 years *combined,* resulting in loss of privacy, identity theft, and financial crimes. Today, hijacked personal computers known as *botnets* are used to send spam or viruses. And all of this is done without the owner's knowledge.

Just this week, according to a recently released report from Netwitness, hackers gained access to a data at close to 2,500 companies and government agencies, from credit-card transactions to intellectual property, over the last 18 months in a coordinated global attack. Then, according to a report drafted by the Chief Information Security Officer of In-Q-Tel, the CIA's venture capital arm, hackers currently charge about a penny for every 1000 e-mails of spam and only about *$1.00* for a credit card that includes *every piece of information necessary* to compromise one's credit!

As you all know, 85 percent of our vital infrastructure is owned and operated by the private sector, and, according to a 2009 Verizon report which examined data breaches at 45 major U.S. firms in 15 different industries, "the average cost for a data breach reached an eye-opening $6.75 million"—that's the cost to the average large company *every single day.* Cyber attacks represent both a potential national security *and economic* catastrophe.

I commend President Obama for deeming cybersecurity "a top priority" and recently naming Howard Schmidt—whom Senator Rockefeller and I met with a few weeks ago—as the administration's national cybersecurity coordinator. However, we remain concerned that this position still does not possess the institutional heft that it requires, as the coordinator is not accountable to Congress and the American people nor does he does report directly to the President—significantly more can and *must* be done. It is *imperative* that public and private sectors marshal our collective forces in a collaborative and complementary manner to confront this urgent threat and reduce the risk posed by cyber intrusion or a catastrophic cyber attack.

As part of this effort, we must identify incentives for the private sector. Limiting liability for the companies that improve its cybersecurity posture, improving threat information sharing, providing a "safe harbor" for exchanging vulnerability data, as well as tax credits contingent on a company complying with certain security practices, should all be considered.

It is equally urgent that government takes proactive steps always mindful though of privacy concerns. The government should work with the private sector to recognize and promote cybersecurity performance measures and best practices, develop a robust workforce of cybersecurity professionals, promote innovation and excellence in products and services, institute a campaign to educate the public about cybersecurity risks, use the Government's purchasing power to raise standards through procurement, and promote government and private sector teamwork in emergency preparedness and response in the event of a catastrophic cyber attack.

Ultimately, we must recognize *that time is not on our side* and it is clear that our adversaries will continue to change their tactics as technology evolves. Congress must take action—I look forward to hearing from our distinguished witnesses and

working closely with my colleagues to implement a comprehensive cybersecurity strategy for our Nation.

The CHAIRMAN. Thank you, Senator Snowe.

Admiral if you would present your testimony, please, and then we'll go right on through.

I just want to point out that I—was it four years ago? Five years ago?

Admiral MCCONNELL. Three years ago, sir.

The CHAIRMAN. Three years ago——

Admiral MCCONNELL. Yes, sir.

The CHAIRMAN.—that you took the entire Intelligence Committee to an offsite place and spent a whole day on cybersecurity.

Admiral MCCONNELL. Right.

The CHAIRMAN. And you were so intense that day that I don't think any of us were quite the same afterwards. And it was one of those things that, you know, was a wake-up call that we needed. You gave us amounts of information, and now we have people on the Intelligence Committee who are following this subject very closely.

We welcome you, sir.

STATEMENT OF VICE ADMIRAL MICHAEL MCCONNELL, USN (RETIRED), EXECUTIVE VICE PRESIDENT, NATIONAL SECURITY BUSINESS, BOOZ ALLEN HAMILTON

Admiral MCCONNELL. Thank you, Mr. Chairman, Senator Snowe, members of the Committee. It's a pleasure to be here.

Let me first say I not only agree, I fully endorse and verify everything that the two of you said in your opening statements. Based on what I know, at a classified level, my experience since being the Director of NSA in 1992, I've been worrying about this issue and following it, and you're exactly right. And thank you for your leadership as a forcing function.

Now, what I will attempt to do in some very brief comments is put a sharper edge on it and then make some associations, on a historical basis, about what we may need to do.

You asked me to talk to threat, actions to mitigate, and public-private partnership. You mentioned that we're at significant risk; let me make it sharper. If the Nation went to war today in a cyberwar, we would lose. We would lose. We're the most vulnerable. We're the most connected. We have the most to lose. So, if we went to war today in a cyberwar, we would lose.

As an intelligence officer, I'm often asked to make predictions. I want to make three predictions for you:

The first is, we will not mitigate this risk. We'll talk about it, we'll wave our arms, we'll have a bill, but we will not mitigate this risk. And as a consequence of not mitigating the risk, we're going to have a catastrophic event. In our wonderful democracy, it usually takes a forcing function to move us to action. And it is my belief, having followed this from the early 1990s, it's going to take that catastrophic event.

Now, my second prediction is, the Government's role is going to dramatically change. It is going to be a very active role in the future of telecommunications in this country and, in fact, in global telecommunications.

My third prediction is, we're going to morph the Internet from something that's referred to, generally, as "dot-com" to something I would call "dot-secure." It will be a new way of communicating. Because when transactions move billions of dollars, or when transactions route trains up and down the East Coast or control electric power or touch our lives in the way they do at such a significant level, the basic attributes of security must be endorsed. And the first attribute of security is not a scrambled text to protect a secret. The first attribute is authentication; who's doing this transaction. If it's a $10-billion transaction, don't you need to know for sure who's conducting the transaction? The second attribute is data integrity. You didn't move that decimal. The third is nonrepudiation.

Now, the reason I pick it up that way is because, as the Director of NSA, everybody knows the mission is to break code; break the codes of potential adversaries, so we know their secrets. The other mission of NSA is to make the code to protect our secrets. And the attributes of security mostly are in focus when you talk about nuclear weapons. So, if you're—if you ever contemplated using nuclear weapons—heaven forbid, we never do—authentication—order from the President—becomes the single most important feature. Data integrity is the second most important. Nonrepudiation is the third. So, thinking about it that way changes one's perspective.

So, we're not going to do what we need to do. We're going to have a catastrophic event. The Government's role is going to change dramatically, and then we're going to go to a new infrastructure.

Now, let me speak to the Government's role. I wanted to get historical perspective, so I asked some of my associates to do some research. And the astounding thing that we discovered is, there is a technology cycle that runs about every 50 years. Could be closer to 60, or maybe 40, but it's about every 50 years. Every time there's new technology, there's a rush to invest, there's a frenzy, there's a period when there's a bust, then there's strong intervention by the Government, and then it settles out, going forward.

And the first example that I'll use is railroads. United States has been the largest economy in the world since 1880. Most people don't know that. We captured the Industrial Revolution from the British. We laid rail coast-to-coast, and our economy was off and running. What happened? The railroads became so powerful they started to dictate to the Government. So, what was the result? Antitrust legislation; break it up. The Government's role changed very dramatically.

You can extend that argument to automobiles. Same argument. When I was a child, 60,000 people a year died on the highway; the population of the Nation was 150 million. Today, it's 30,000; our population is 300 million. What changed? The Government's role significantly changed. Interstate highways, for safety, guardrails, seatbelts, flashers, all the things that industry was forced to do because it affected so many people. So, in my view, the Internet—global communications, moving money at the speed of light from Tokyo to New York, or from New York to Singapore—billions of dollars—the transportation systems of the world, the electric power grid of the world—that is so significant that the Government's role is going to change very dramatically. And I would predict we will have a different Internet at some point in time.

Now, what are the things we have to do? International agreements with partners and with competitors. Because it's in the interest of China, as an example, to have a Net that's secure, for which there's authentication, for which there's data integrity, for which there's nonrepudiation features built in. You can achieve that with mathematical certainty. It's a simple function of applying the right kind of tools and techniques and encryption. I would argue it's not in China's self-interest to destabilize the U.S. money—money supply.

Now, what I really worry about today is, not a nation-state. If we had a war with a nation-state, we would engage in ground combat, maritime combat, air combat, space combat, and cyberspace combat. That's not likely in our future. But, what is likely in our future is a group that's not deterred, who wishes to destroy the system, who has the technical capability—because the cost of entry is pretty low—has the technical capability to attack something. And I'll use the money supply as an example.

I majored in Economics 101, way back as an undergraduate, and I was astounded to learn there's no gold backing up all those dollars. We left that standard in the 1930s. And then I was astounded to learn that they're not even dollar bills printed; there's—only about 6 percent of the value of the country is actually in dollar bills. So, where's the value? It's an accounting entry. And I believe the right kind of talent could attack the global money supply.

As an example, our gross domestic product, on a yearly basis, is 14 trillion—just over 14 trillion. Two banks in New York move 7 trillion a day. So, if an extremist group with the right kind of tools could scramble that data, they could destroy confidence in global banking. New York is the banking center of the world.

So, that's the risk. Will we be required to experience that catastrophic event before we move to action?

I'll finish with just an example. Nuclear weapons are easy to imagine, because there's the mushroom cloud and the shockwave. When nuclear weapons happened, this Nation took action to put the government in charge. There was a joint committee of Congress to oversee it and fund it, and the law said only the government could own things that were nuclear. Now, that's mitigated over time. That committee was determined to be unconstitutional, and we created the Department of Energy, and it has gone on. We've got commercial nuclear energy and so on. So, we learned over time to adjust to that.

If you take telecommunications and the Internet, it's almost entirely in the private sector, and it's going in the other direction. But, it has become so important and so potentially significant, in my view, it rivals nuclear weapons, in terms of potential damage to the country.

So, the government was hands-off to start. And if you look at the evolution of the 50-year cycles, whether it was building canals or textile machinery or railroads or automobiles, that cycle repeated, where the government had a greater role when it affected more people. And we're reaching that point now. So, either we have a forcing function through a catastrophic event or, hopefully, your bill will be law and we can have the forcing function to deal with this in the way we must deal with it. We must develop a deter-

rence policy, and we're probably going to have to figure out how we engage in preemption, where those that wish us harm cannot be deterred.

Mr. Chairman, that's my warm-up. I look forward to your questions. Thank you very much.

[The prepared statement of Admiral McConnell follows:]

PREPARED STATEMENT OF VICE ADMIRAL MICHAEL MCCONNELL, USN (RETIRED), EXECUTIVE VICE PRESIDENT, NATIONAL SECURITY BUSINESS, BOOZ ALLEN HAMILTON

Introduction

Mr. Chairman, members of the Committee, thank you for the opportunity to speak to the Committee on Commerce, Science, and Transportation today.

First, I want to open with a simple statement:

If we were in a cyberwar today, the United States would lose.

This is not because we do not have talented people or cutting edge technology; it is because we are simply the most dependent and the most vulnerable. It is also because we have not made the national commitment to understanding and securing cyberspace. While we are making progress:

- the President's cyberspace policy review completed last May,
- the appointment of the Cybersecurity Coordinator in December, and
- recent investments in the Comprehensive National Cybersecurity Initiative (CNCI) are moves in the right direction but
- these moves are not enough.

The Federal Government will spend more each year on missile defense than it does on Cybersecurity, despite the fact that we are attacked thousands of times each day in cyberspace and we are vulnerable to attacks of strategic significance, *i.e.,* attacks that could destroy the global financial system and compromise the future and prosperity of our Nation. Securing cyberspace will require a more robust commitment in terms of leadership, policies, legislation, and resources than has been evident in the past.

Seizing Opportunity . . .

The cyber revolution has transformed our economy, enriched our society, and enhanced our national security. The Information and Communications Technology (ICT) sector contributes over $1 trillion to our economy each year; "smart" electric grids promise to transform our energy system; intelligent transportation systems are altering the way we move and the way we manage commerce; electronic medical records and telemedicine promise to reduce costs while improving quality. The global financial sector relies on information technology to process and clear transactions on the order trillions of dollars each day. To put that in perspective, while the U.S. total GDP was just over $14T last year, two banks in New York move over *$7T per day* in transactions.

Meanwhile, major investments in broadband—by both the government and private sector—empowers small businesses and our citizens; digital classrooms are changing the way our children are educated; and "open government" initiatives make government data more accessible and useable for business and individuals alike. Our military and security services have benefited as well. The Department of Defense has aggressively adopted network-centric operations, linking sensors, commanders and operators in near-real time and providing the U.S. a decisive advantage in the battlespace. The intelligence community and homeland security have benefited from cyber technologies by improving collaboration and information sharing across formerly impenetrable organizational divides. In short, the microprocessor and Internet have been as transformative as the steam engine and railroads in the 19th century and as impactful as the internal combustion engine and interstate highway system in the 20th century.

. . . Managing Risk

The reach and impact of cyberspace will accelerate over the next 10 years, as another billion users in China, India, Brazil, Russia, Indonesia and Middle East gain access to the Internet. As a consequence, cyberspace will be much more diverse, distributed, and complex. As cyberspace becomes more critical to the day-to-day functioning of business, society and government, the potential damage from cyber attacks, system failures and data breaches will be more severe.

In the early stages of cyberspace, the threat largely originated from "hackers" who wanted to their test skills and demonstrate their technical prowess. Criminal elements followed, resulting in attacks against financial institutions, credit card accounts, ATMs for personal gain. More sophisticated actors emerged as state-based intelligence and security organizations developed robust exploitation and attack capabilities as part of a larger national security strategy.

Recently, "hactivists"—non-state actors mobilized in support of a particular issue or motivated by patriotic reasons—have entered the fray. Generally speaking, we know and understand these threats—their capabilities and intentions.

However, of particular concern is the rise of non-state actors who are motivated not by greed or a cause, but by those with a different world view who wish to destroy the information infrastructure which powers much of the modern world—the electric grid, the global financial system, the electronic health care records, the transportation networks.

Of increasing concern is that the sophistication of cyber attack tools continues to increase at cyber speed, while the barriers to entry continues to fall as attack tools proliferate in chat rooms, homepages, and websites. The challenges we face are significant and will only grow; our response must equally bold and decisive.

Recommendations for Cybersecurity

Despite the complex and seemingly unprecedented nature of the challenge, there are some immediate actions we can take to secure cyberspace and the future of our Nation.

Cyber Policy—The U.S. needs a long-term cyberspace strategy that spells our specific goals and objectives and clarifies roles and responsibilities across the Federal Government. This should be preceded by a cyber equivalent to President's Eisenhower's "Project Solarium" in the early 1950s in developing the Nation's nuclear *deterrence policy.* Today, we need a full and open discourse with a diverse group—business, civil society, and government—on the challenges we face in cyberspace. This dialogue should result in a strategic framework that will guide our investments and shape our policies, both domestically and internationally.

We need a national strategy for cyber that matches our national strategy that guided us during the cold war, when the Soviet Union and nuclear weapons posed an existential threat to the United States and its allies. Cyber has become so important to the lives of our citizens and the functioning of our economy that gone are the days when Silicon Valley could say "hands off' to a Government role. To offer historical perspective on how the Government's role has increased in every case as emerging technologies effect the Nation and greater numbers of our citizens, I am attaching to this statement a review conducted by my colleagues and I entitled "The Road to Cyberpower."

Cyber Operations—The Cybersecurity challenge to the Nation today mirrors our response to counter terrorism after 9/11—a host of Federal and state and local agencies, each with their own authorities, missions, operations centers and information systems. The risk is that we fail to learn the lessons around counterterrorism information sharing and operations and create more silos by individual agencies, potentially creating an atmosphere of bureaucratic rivalry and duplicative investments. To that end, the U.S. should establish a National Cybersecurity Center, modeled on the interagency National Counter Terrorism Center (NCTC), that integrates elements of DoD's proposed Cyber Command, DHS's National Cybersecurity and Communications Integration Center (NCCIC), FBI's cyber operations, state and local government, *and the private sector.* This center should operate at the highest levels of classification for all members and serve as the hub of information sharing and integration, situational awareness and analysis, coordination and collaboration. Only sharing information across all sectors will we be able to provide incident response across all domains of cyberspace—.gov, .mil, and .com.

Such a center would utilize the legal authorities of each agency while protecting privacy and civil liberties with appropriate oversight by the Attorney General and the Congress. The center also could serve as the information sharing and collaboration hub with our allies and other Cybersecurity organizations, providing a single conduit for outside entities.

Cyber Technology—The U.S. risks being left behind in Cybersecurity technology. Currently, multiple organizations within the government and private sector are focused on developing new technologies to protect our networks, computer systems, data and applications. However, most of the efforts are fragmented and sub-scale. The U.S. should approach this challenge as we successfully addressed to the challenge to our semiconductor industry in the 1980s through a *public-private partnership* focused on Cybersecurity technologies.

The U.S. should establish a Cybersecurity Collaborative Consortia, modeled after SEMATECH, a public-private partnership that supports basic research and development and develops foundational technologies and techniques of common concern—identity and access management, secure networks, intrusion detection, dynamic defense, etc. Such an organization should work closely with the National Institute of Standards and Technology (NISI) and with the National Security Agency (NSA) to define standards for Cybersecurity that could be used for government, business, and individuals in both the public and private sectors because there are no effective boundaries in cyberspace.

Cyber Human Capital—The U.S. needs a Cyber Education and Training Initiative (akin to the National Defense Education Act of 1958 after the launch of Sputnik) to build our national human capital base in math, science and technology, electrical engineering, computer science, and cybersecurity. Recent initiatives by Congress in programs like the Federal Cybersecurity Scholarship for Service and the Information Assurance Scholarship Program are a start, but need to be more aggressively funded to build the expertise we need in cyberspace. As a country, our vulnerabilities will only grow without a highly trained workforce than can respond to the daunting cyber challenges and opportunities of the 21st century.

Cyber Management—Current spending and oversight on Cyber is spread among multiple accounts and dispersed over multiple committees in Congress. It is difficult to understand the current level of investment in cyber and evaluate the effectiveness of our investments given this complexity and lack of transparency. OMB, working with Congress, should identify Cybersecurity investments, develop performance criteria aligned against a national cyber strategy, address the gaps and eliminate duplicative or conflicting efforts, and improve accountability for results. We can not spend our way out of this challenge, prioritization, accountability, management and oversight are key.

Summary

Cyber technologies offer unprecedented opportunities for the nation; however, they also present significant risks to our infrastructure, our financial systems, and our way of life. We prevailed in the Cold War through strong leadership, clear policies, strong alliances, and close integration of all elements of national power—economic, military, and diplomatic—supported by a bi-partisan, national consensus around containment and deterrence. We must do the same with Cybersecurity.

The CHAIRMAN. Thank you, Admiral.

Dr. Lewis.

STATEMENT OF JAMES A. LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Dr. LEWIS. Thank you, Mr. Chairman, and I'd like to thank the Committee for the opportunity to testify.

And I want to congratulate you on the Cybersecurity Act of 2010. This is a very important bill, and if it was passed, it would make an immense improvement to our national security and our economic well-being. The bill provides a broad rethinking of our approach to cybersecurity and the role of government. And a lot of what I'm going to say is going to sound a lot like Admiral McConnell, which may be good, or not.

The people who pioneered cyberspace—the people who originally designed it—they wanted governments to have a limited role. They expected the Internet would be a self-governing global commons. And they argued there were no borders in cyberspace and that technology moved too fast for government to intervene and that the old rules of business and national security didn't apply. None of this was right.

People thought we would get a peaceful global commons. Instead, we've got the Wild West. The Internet was not designed to be secure. The rules and contracts put in place when it was commer-

cialized were not written with security in mind. The result is a very Hobbesian environment; cyberspace is not safe.

So, the issue for me is, How do you bring law to the Wild West? How to move from a do-it-yourself homebrew approach to cybersecurity, and how to secure the digital global infrastructure we now depend on. Legislation like the Cybersecurity Act can play a crucial role in bringing needed change.

You will hear—I think you've already heard—a litany of criticism. You will be told the bill is not perfect. But, I note that the Constitution says our goal is "more perfect," not perfection. This bill would make cybersecurity more perfect.

People will say that we cannot measure or certify cybersecurity. This might explain why we're in such a mess. But, I think we're now at the point where we're beginning to collect data that shows what works; and if we can determine what works, we can teach it and we can certify people to it.

Many will say that we should let the market fix cybersecurity. I'm familiar with this one because I, myself, wrote it in 1996, and I'm still waiting. The government needs to give the market a kick.

There's a desire to say that the President should not have authorities, during a crisis, to respond to the kind of cyber attack that Admiral McConnell was talking about. I call this the Hurricane Katrina approach to cybersecurity. There will be complaints that cybersecurity will get in the way of innovation. But, to build on the car metaphor, requiring safer cars did not kill innovation in the automobile industry, or we would still all be driving 1956 DeSotos.

Some claim the private sector can do a better job defending networks than government. This is like saying we can rely on the airlines to defend our airspace against enemy fighters. Private companies will never be a match for foreign intelligence service or foreign militaries.

But, moving to the policies we need for cybersecurity will not be easy. In the past, when a new technology has come along and reshaped business and warfare in society, it has taken the United States decades to develop the rules it needed; the laws, the judicial precedents, and the regulations that would safeguard society.

The difference now is that we don't have decades to do this. We're under attack every day, as you said. We're losing, every day, vital secrets. We're at tremendous risk. If we had a war, we would lose. So, we can't wait. You know, when it was steam engines or automobiles or telephones, we could take 20 or 30 or 40 years to come up with the rules we needed. But, we don't have that luxury now, right? Prompt action is necessary.

The prospects for growth and improvement in cyberspace remain great, but to obtain these benefits, we need to close the frontier, end the pioneer approach, say the Wild West is over, and bring the rule of law to cyberspace. We need a new framework for cybersecurity, and this bill helps provide it.

The work of this committee has really helped force the debate in this issue, and so I really applaud you for it. People have had to think hard about real serious issues. And I hope, with that, that we see passage of the bill sometime this year.

Thanks again for letting me testify, and I'll be happy to take your questions.

[The prepared statement of Dr. Lewis follows:]

PREPARED STATEMENT OF JAMES A. LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

I would like to thank the Committee for this opportunity to testify and I would like to congratulate it for its comprehensive "Cybersecurity Act of 2009."

This bill is important because it is a broad step to rethinking our approach to the Internet, to cyberspace, and to the role of government.

The pioneers of cyberspace wanted governments to have a very limited role. They expected a self-governing global commons to emerge, and argued that there were no borders, that technology moved to fast, that old rules of business and security did not apply. They expected a global commons; instead they got the wild west. The Internet was not designed to be secure; the rules and contracts put in place when it was commercialized were not written with security in mind. The result is Hobbesian, that is to say nasty and brutish, if not short. So the issue for the Nation is how to bring law to the Wild West, how to move from a do-it-yourself homebrew approach to cybersecurity, and how to secure a global digital infrastructure upon which we now depend. Legislation like the Cybersecurity Act 0f 2010 can play a crucial role.

Cybersecurity has become an important issue over the last decade as the Internet changed to become a significant global infrastructure. The U.S. in particular has woven computer networks into so many of its economic activities that we are as reliant on the Internet as we are on any other critical infrastructure. Networked activities can be cheaper and more efficient, so companies large and small have migrated to the Internet because it can provide competitive advantage. Our national defense relies heavily upon networks. Networks reinforced existing trends in military the realization that intangible factors—greater knowledge, faster decisionmaking increased certainty—would increase effectiveness of our military force.

That technologies designed in the early 1970s have worked so well and have so cleanly scaled to support more than a billion users is an amazing triumph, but anyone with malicious intent can easily exploit these networks. The Internet was not designed to be a global infrastructure upon which hundreds of millions of people would depend. It was never designed to be secure. The early architects and thinkers of cyberspace in the first flush of commercialization downplayed the role of government. The vision was that cyberspace would be a global commons led and shaped by private action, where a self-organizing community could invent and create. This ideology of a self-organizing global commons has shaped Internet policy and cybersecurity, but we must now recognize that this pioneer approach is now inadequate.

There are two reasons for this inadequacy. First, private efforts to secure networks will be always be overwhelmed by professional military and criminal action. The private sector does not have the capability to defeat an advanced opponent like the SRV or the PLA, organizations that invest hundreds of millions of dollars and employ thousands of people to defeat any defense. We do not expect airlines to defend our airspace against enemy fighter planes and we should not expect private companies to defend cyberspace against foreign governments.

Second, absent government intervention, security may be unachievable. Two ideas borrowed from economics help explain this—public goods and market failure. Public goods are those that benefit all of society but whose returns are difficult for any individual to capture. Basic research is one public good that the market would not adequately supply if government did not create incentives. Cybersecurity is another such public good where market forces are inadequate.

We talk about cyber attack and cyber war when we really should be saying cyber espionage and cybercrime. Espionage and crime are not acts of war. They are, however, daily occurrences on the Internet, with the U.S. being the chief victim, and they have become a major source of harm to national security. The greatest damage to the U.S. comes from espionage, including economic espionage. We have lost more as a nation to espionage than at any time since the 1940s. The damage is usually not visible, but of course, the whole purpose of espionage is not to be detected.

This is not cyberwar, Russia, China, and cybercriminals of all types have no interest in disrupting Wall Street, the Internet, or the American economy. There is too much to steal, so why would anyone close off this gold mine. As with any good espionage exploit or mafia racket, the perpetrators want stability, a low profile, and smooth operations going so they can continue to reap the benefits.

There is a potential for cyber attack, but it is so far constrained by political and technological barriers. Terrorists likely do not yet have the advanced cyber capabili-

ties needed to launch crippling strikes. The alternative, that they have these capabilities but have chosen for some reason not to use them, is ridiculous. There are nations that could launch a crippling strike, but they are likely to do son only as part of a larger armed conflict with the United States. These nations do not love jihadis any more than we do, so they are unlikely in the near future to transfer advanced cyber capabilities to terrorists. Presumably, in the case of Russia and China their cyber criminal proxies are also instructed not to take jihadi clients (although there is one incident where it is alleged that Russian hackers served as mercenaries for Hezbollah, against Israel). Should any of these conditions change—the technological constraints that limit terrorists and the political constraints that limit states and advanced cyber criminals - the U.S. is in no position to defend itself against cyber attack.

Short of armed conflict (over Taiwan or Georgia), China or Russia are unlikely to use cyber strikes against the U.S. The political risk is too high—it would be like sending a bomber or a missile against a power plant, and the U.S. response would be vigorous. Our opponents, however, have reportedly conducted reconnaissance missions against critical infrastructure—the electrical grid, for example—to allow them to strike if necessary in the event of conflict. Cyber attack is cheaper and faster than a missile or plane, there is some chance that the attacker can deny responsibility (because of the weak authentication on the Internet). Right now, our opponents have the advantage but it is within our capabilities to change this.

Getting this change requires a new approach. Many of the solutions to the problem of cybersecurity our Nation has tried are well past their sell-by date. Public-private partnerships, information sharing, government-lead-by-example, self-regulation, and market-based solutions are remedies we have try for more than a decade without success. These policies overestimate incentives for private action and misalign government and private sector responsibilities.

Like other new technologies in the past—airplanes, cars, steam engines—the appeal and the benefits are so great that we have rushed to adopt the Internet despite serious safety problems. These problems are amplified by the global connectivity of the new infrastructure, as the speed of Internet connections means that geographical distance provides little in the way of protection. For those earlier technologies, safety came about through innovation driven by government mandates, and by agreements among nations. The same process of development is necessary to secure cyberspace. The Cybersecurity Act of 2009 could play a vital role in this improvement.

This will not be an easy task. The United States does not like to deal with market failure. This has been true since the earliest days of the republic. Steam engines, although notoriously unsafe, had to wait forty years until a series of savage accidents costing hundreds of live led Congress to impose safety regulations. Automobile safety rules took more than half a century and initially faced strong opposition from manufacturers. The initial air safety regulations appeared only twenty-three years after the first flight. There is the recurring hope that "intellect and practical science," to quote a 19th Century Congressional report explaining why regulation was unnecessary for steamboats put it, will lead to improvement via some automatic and self-correcting market process and without government intervention.

Just as cars were not built to be safe until government pressure changed auto manufacturers' behavior, cyberspace will not be secure until government forces improvement. Twelve years of reliance on voluntary efforts and self-regulation have put us in an untenable situation. Some may argue that a move away from the market or a greater emphasis on security or a larger role for government will damage innovation in cyberspace. This argument is in part a reflection of competition among various bureaucracies, advanced to protect turf, but is also reflects a misunderstanding of the nature of innovation. There are grounds to be concerned about the ability of the U.S. to innovate when compared to other nations, but the real obstacles are a weak education system, poorly designed tax policies, damaging immigration rules, and mis-investment that makes it hard to develop new technologies and competitors. Removing these obstacles would be politically difficult and face strong opposition. It is easier to insist instead that keeping the Internet open and anonymous or bringing broadband to undeserving areas will somehow generate growth. Greater security is more likely to increase innovation, by reducing the loss of intellectual property and by increasing demand for more valuable Internet services.

Another reason put forward for not taking action is the supposedly borderless nature of cyberspace. The pioneers of cyberspace wanted their new creation to be a global commons, a shared space that no one owns. The designers of the Internet built the network to reflect their values, which were non-hierarchical and to a degree, anti-authoritarian and anti-government. One of the original cyberspace theorists was also a songwriter for the Grateful Dead, and it was he who issued the fa-

mous Declaration of Independence of cyberspace, saying there was no room or need for governments. Cyberspace would be a global commons where a self-organizing community could invent and create.

This is an ill-conceived notion that continues to distort our thinking. Cyberspace is an artificial construct produced by machines. Those machines are all owned by individuals or organizations and all exist in some physical location that is subject to the sovereign control of some nation.

Cyberspace is like the public space in a shopping mall, a "pseudo commons" or a condominium.

In some instances, of course, such as the Internet Engineering Task Force or the Open Source Software Movement, this vision of an open, nonhierarchical community has worked exceptionally well. But to use a historical analogy, many of the pioneers of the Internet expected Woodstock and the "Summer of Love," instead they got Altamont and the Hells Angels. The combination of unplanned global access, porous technologies, and weak governance makes this newly critical infrastructure exceptionally vulnerable. As our reliance as a nation increases, so does our vulnerability to remote exploitation and perhaps attack.

Cyberspace is not a global commons. It is a shared global infrastructure. There is rarely a moment when a collection of bits moving from one computer to another is not actually on a network that someone owns and that is physically located in a sovereign state. The exceptions might be undersea cables or satellite transmissions, but the action still takes place on an owned facility were the owner is subject to some country and its laws. At best, this could is a "pseudo commons." It looks like a commons but actually is not, as someone owns the resources in question and that someone is subject to the laws of some nation. Cyberspace is in fact a more like a condominium, where there are many contiguous owners.

Governance of this condominium is both weak and fragmented. There are no agreed rules, other than business contracts, and no "condominium board," no process to develop rules. Action in cyberspace takes place in a context defined by commercial law and business contracts. When the United States commercialized the Internet, it chose this legal construct accommodate business activity, but it is inadequate for security, particularly as the Internet spread to countries around the world and to nations with very different values and laws.

The proposed legislation would go a long way to correct these problems. To put the problem in a larger perspective, it is time to move from the policies created in the pioneer phase of the Internet. It is time to close the Wild West. This will require a broad rethinking of American law and policy, and will require adapting to the technologies we now depend on. It will need new kinds of international agreements, new standards and rules for industry, and new approaches to the professionalization of those who operate networks. This is no small task but, judging from experience, it is inevitable. This process has occurred before, often with help from the government. The Commerce Department of the 1920s, for example, encouraged several major industries, including the automotive and radio industries, to standardize, to professionalize, and to create associations and rules that serve the public interest.

A "one size fits all" strategy will not work. We will need to manage international engagement, critical infrastructure regulation, and economic stability all at the same time. Progress faces significant obstacles. There are legitimate concerns over civil liberties. There are strong business interests in avoiding regulation. And there are the tattered remnants of a vision of cyberspace as some kind of utopian frontier. Governance is a central issue for each of these. Governance is the process for creating rules, resolving disputes, and ensuring compliance. Our beliefs about the nature of cyberspace have downplayed the role of formal governance and now we are paying the price. Changing this, as we did for steamboats, cars and airplanes, is part of the long-term process to adjust to new environment created by technological change.

This bill contains many of the essential elements of the new approach we need. A comprehensive national strategy that considers all aspects of national security and puts forward along term vision for cyberspace is an essential starting point for making this new infrastructure secure. It will be essential, of course, to avoid merely repeating the formulas of 1998 or 2003 in a new strategy. We've heard repeatedly that there is a shortfall of individuals with the requisite skills for cybersecurity. The scholarships, competitions and workforce plans outlined in this bill would go a long way to repair this. The legal review and the intelligence assessment are long overdue. The call for the creations of a response and restoration developed with the private sector that the President could implement in a crisis is crucial for national defense.

As with any major piece of legislation, there will be considerable criticism. Some of this criticism is ideological, some reflects self-interest, and some is the result of

a healthy skepticism as to our ability to carry out some of the ambitious measures contained in the bill. There was initially concern that emphasizing the authorities the President already has to intervene in network operations during a crisis would somehow give the ability to shut off the Internet. This stemmed mainly from an inaccurate reading of the bill and perhaps from the desire to preserve the notion of cyberspace as an untrammeled commons where government has little or no role. Frankly, efforts to deny the President adequate authority in a crisis are like expressing a preference for Katrina-like disaster management. I hope we can do better.

No one ever disagrees with the notion of more education, but the more contentious aspect of the workforce development is the requirement for certification and training. Being able to certify that someone has the necessary skill and knowledge is a requisite part of professionalization. We do this for doctors, lawyers, pilots, barbers, plumbers and real estate agents. Some certification requirements are Federal, many are developed by states. Many in the IT industry believe that they are not ready for this step. Certification requires knowing what is useful and necessary and being able teach it and test it. It is on the former that there is disagreement—that we do not know what is necessary for security.

This may have been true at one time but I believe it is changing. In the last few years, as people have been able to collect more data on security problems, to develop metrics, and to identify steps will reduce risk, it is possible to think of a training program for cybersecurity. This is part of a larger move from compliance drive security, which has largely failed, to performance driven security. The concept of a cybersecurity dashboard found in Section 203 reflects this shift to a data driven approach to cybersecurity. The Act, if passed, will accelerate the development and professionalization of those parts of cyberspace that provide critical services to the Nation.

These are all politically difficult issues, but this situation is not new. Every time a new technology has reshaped business, warfare and society, there has been a lag in developing the rules—law, judicial precedents, regulations—needed to safeguard society. Cyberspace is different in its global scope and in the immediate nature of the damage America suffers. Waiting for some natural process or perfect solution not only puts our Nation at risk, it gives our opponents an advantage. We would be well served if Congress passed this bill.

The CHAIRMAN. Thank you, sir.

Mr. Borg.

STATEMENT OF SCOTT BORG, DIRECTOR AND CHIEF ECONOMIST, U.S. CYBER CONSEQUENCES UNIT

Mr. BORG. Thank you for inviting me.

My name is Scott Borg. Oh, I should turn this on. I'm the Director of the U.S. Cyber Consequences Unit. This is an independent, nonprofit, research institute that investigates the economic and strategic consequences of cyber attacks. We supply our results only to the U.S. Government and to the public.

At the USCCU, I've had the privilege of leading an extraordinary team of cybersecurity experts, economists, and other investigators, many of whom have national reputations. This team has included Warren Axelrod, John Bumgarner, Joel Gordes, Ben Mazzotta, Michael Mylrea, Ardith Spence, Paul Thompson, Charles Wheeler, and a number of others.

Since 2004, we have been visiting facilities in critical infrastructure industries, and interviewing employees, to determine what cyber attacks are actually possible and what their consequences would be. We have been given access to the business records of large critical infrastructure corporations so that we could analyze their dependence on their suppliers and their customers' dependence on them. We've developed powerful conceptual frameworks and analytic tools for making sense of this information.

There are three points I would like to make today. First, cyber attacks are already damaging the American economy much more than is generally recognized. Second, the biggest growth opportunities for the American economy all depend on better cybersecurity. Third, in order to get the improved cybersecurity we urgently need, we must fix a number of broken or missing markets.

The greatest damage to the American economy from cyber attacks is due to massive thefts of business information. This type of loss is delayed and hard to measure, but it is much greater than the losses due to personal identity theft and the associated credit card fraud. The reason the loss from information theft is so great is that we really do operate in an information economy. The amount of value a company can create and capture is generally proportionate to the amount of information that it can utilize that its global competitors can't.

Education is economically important because it allows us to create and apply more information. The greater portion of the value, even in most manufactured goods, is not in the materials from which things are made, but in the information they contain. A modern automobile or airplane, from an economic standpoint, is primarily an information product.

To understand what this means, think of how a company makes money. It introduces a new product or a new feature, and collects a premium from it until its competitors start offering something comparable. Even after that, the company will probably still be able to make a profit on that item because it will know how to produce it for less. When a new production facility opens, there will typically be a 5- to 15-percent drop in costs each year for the first 3 to 6 years. This is because the company is learning how to do everything more efficiently; it's about information. The amount by which the company's costs are lower than the costs of its competitors is normally all profit.

Now think what happens if the company's information is stolen. The period during which it can collect a premium will be reduced to almost nothing, because the competitors will be able to offer a comparable product almost right away. The profits due to lower costs will be gone, because the competitors will have all the detailed information that made the greater efficiencies possible. The competitors' costs will actually be lower than those of the victimized company, because the competitors won't have the expense of creating the information. Instead of collecting a healthy profit, the victimized company might now be struggling to survive.

Most of the other factors allowing companies to prosper can also be wiped out by information thefts. To get an idea of the effect of information thefts on the larger economy, imagine this sort of example multiplied thousands of times.

The biggest large-scale growth opportunities for the American economy also depend on better cybersecurity. This is because nearly all the more innovative ways of creating value need information technology to be developed efficiently.

There are eight big growth opportunities that I've been able to identify. I think you've been given a list of them. These include things like the flexible re-allocation of capacity, which lies behind the Smart Grid and cloud computing; mobile information support,

which boosts efficiency of tools like electronic medical records; and smart products, which allow products, such as smart phones, to increasingly contain services. Examining this list reveals that each of these opportunities requires networked computers, and is vulnerable to cyber attacks. Awareness of this is the main thing that is slowing down the implementation of many of these strategies. And most of them could be brought to a screeching halt by a greater awareness of the vulnerabilities they're introducing.

The solutions to these problems are not something that the government can directly legislate into existence. The reason is that both the information technology and the techniques employed in cyber attacks are developing so rapidly. If the government tries to mandate standards, they will be out of date, and an actual impediment to better security, before they can be applied. This is not like fire codes for building constructions, where the big changes take decades. We don't know what the minimum code of cybersecurity should look like 4 years from now.

If there's any area of the American economy that needs creative entrepreneurial problem-solving, it is, therefore, cybersecurity. Yet, our markets are currently not delivering the improvements in cybersecurity at anything like the necessary rate. In some cases, they are not delivering improvements at all.

When markets are not functioning properly, there are identifiable reasons. I think you've got a list of these reasons; there happen to be six of them. Sometimes it's because companies are not being charged for all of their costs or paid for all the benefits they produce. Other times, the individual agents are not adequately motivated to act in the long-term best interests of their company. Still other times, there isn't enough information available for good market choices.

Each of these market problems, each of these market breakdowns, has possible remedies. It's these remedies to the market failures that should be at the center of our discussion of how to improve our cybersecurity.

Thank you.

[The prepared statement of Mr. Borg follows:]

PREPARED STATEMENT OF SCOTT BORG, DIRECTOR AND CHIEF ECONOMIST, U.S. CYBER CONSEQUENCES UNIT

Thank you for inviting me. My name is Scott Borg. I am the Director of the U.S. Cyber Consequences Unit. This is an independent, non-profit research institute that investigates the economic and strategic consequences of cyber attacks. We supply our results only to the U.S. Government and to the public. At the US-CCU, I have had the privilege of leading an extraordinary team of cyber-security experts, economists, and other investigators, many of whom are nationally famous in their fields. This team has included Warren Axelrod, John Bumgarner, Joel Gordes, Ben Mazzotta, Michael Mylrea, Ardith Spence, Paul Thompson, Charles Wheeler, and a number of others. Since 2004, we have been visiting facilities in critical infrastructure industries and interviewing employees to determine what cyber attacks are actually possible and what their effects would be. We have been given access to the business records of large critical infrastructure corporations, so that we could analyze their dependence on their suppliers and their customers' dependence on them. We have developed powerful conceptual frameworks and analytic tools for making sense of this information.

There are three points I would like to make today:

First, cyber attacks are *already* damaging the American economy *much* more than is generally recognized.

Second, the biggest *growth opportunities* for the American economy all depend on better cyber security.

Third, in order to get the improved cyber security we urgently need, we must fix a number of broken or missing *markets*.

The greatest damage to the American economy from cyber attacks is due to massive thefts of business information. This type of loss is delayed and hard to measure, but it is much greater than the losses due to personal identity theft and the associated credit card fraud. The reason the loss from information theft is so great is that we really do operate in an information economy. The amount of value a company can create and capture is generally proportionate to the amount of information it can utilize that its global competitors can't. Education is economically important because it allows us to create and apply more information. The greater portion of the value, even in most manufactured goods, is not in the materials from which things are made, but in the information they contain. A modern automobile or airplane, from an economic standpoint, is primarily an information product.

To understand what this means, think of how a company makes money. It introduces a new product or new feature and collects a premium for it until its competitors start offering something comparable. Even after that, the company will probably still be able to make a profit on that item, because it will know how to produce it for less. When a new production facility opens, there will typically be a five to fifteen percent drop in costs each year for the first three to 6 years. This is because the company is learning how to do everything more efficiently. The amount by which the company's costs are lower than the costs of its competitors is normally all profit.

Now think of what happens if the company's information is stolen. The period during which it can collect a premium will be reduced to almost nothing, because the competitors will be able to offer an equivalent product right away. The profits due to lower costs will be gone, because the competitors will have all the detailed information that made the greater efficiencies possible. The competitors' costs will actually be lower than those of the victimized company, because the competitors won't have the expense of creating the information. Instead of collecting a healthy profit, the victimized company might now be struggling to survive.

Most of the other factors allowing companies to prosper can also be wiped out by information thefts. To get an idea of the effect of information thefts on the larger economy, imagine this sort of example multiplied thousands of times.

The biggest large-scale *growth* opportunities for the American economy also depend on better cyber security. This is because nearly all of the more innovative ways of creating value need information technology to be implemented efficiently.

There are eight big growth opportunities that I have been able to identify. These include things like the Flexible Re-Allocation of Capacity, which is what lies behind the smart grid and cloud computing, Mobile Information Support, which boosts efficiency with tools like electronic medical records, and Smart Products, which will allow material products, such as smart phones, to increasingly "contain services."

Examining this list reveals that each of these opportunities requires networked computers and is vulnerable to cyber attacks. An awareness of this is the main thing that has already been holding back the adoption of practices like cloud computing. More important, nearly all of these economic initiatives, including the smart grid and electronic medical records, could be brought to a screeching halt by a greater awareness of the vulnerabilities that they are introducing.

The solutions to these problems are not something that the government can directly legislate into existence. The reason is that both the information technology and the techniques employed in cyber attacks are developing so rapidly. If the government tries to mandate standards, they will be out of date—and an actual impediment to better security—before they can be applied. This is not like fire codes in building construction, where the big changes take decades. We don't know what the minimum code for cyber security should look like 4 years from now.

If there is any area of the American economy that needs creative, entrepreneurial problem solving, it is therefore cyber security. Yet our markets are not currently delivering improvements in cyber security at anything like the necessary rate. In some cases, they are not delivering improvements at all.

When markets are not functioning properly, there are identifiable reasons. Sometimes companies are not being charged for all of their costs or paid for all of the benefits they produce. Other times, the individual agents are not adequately motivated to act in the long term best interests of their company. Still other times, there isn't enough information available for good market choices. There are six such reasons altogether, and each suggests possible remedies. It is these market remedies

that should be at the center of our discussions on how to save our economy from the destructive effects of cyber attacks.

Thank you.

The CHAIRMAN. Thank you, sir, very much.

And now Mary Ann Davidson, from Oracle, please.

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

Ms. DAVIDSON. Chairman Rockefeller and members of the Committee, I'm Mary Ann Davidson, the Chief Security Officer for Oracle.

I appreciate the opportunity to appear before you today, and I want to commend the Committee for tackling the difficult issue of cybersecurity and for including industry in the drafting process of cybersecurity legislation, since partnership between government and the private sector is critical to secure our common infrastructure.

I have two specific recommendations to address the present and future challenges of securing critical infrastructure. First, we need to change the educational system so that we have a cadre of people who know that critical cyberinfrastructure will be attacked and to design and build accordingly and defensively. Second, we need to stop upping the ante on exposing critical infrastructure to, in some cases, large systemic risk.

Some have proposed that we certify cybersecurity professionals to improve the protection of critical infrastructure. However, you can't secure something that was not designed or built to be secure. Putting it differently, do we certify interior decorators or the people who built the house? It's architects and engineers and contractors who are professionally licensed, not the people who move furniture around and pick out color schemes, as important as that is.

Those who build software used in critical infrastructure do not, in general, design and code defensively, because they're not educated to do it. And yet, too many universities fiddle while Rome burns, or at least fiddle while Rome is being hacked. Several years ago, Oracle sent letters to the top universities we recruit from, telling them that we spend millions of dollars fixing avoidable, preventable coding errors in software that creates security vulnerabilities. We have to train all computer science graduates in how to write secure code, because they were not taught this at universities. Universities need to change their curricula to address this clear and present deficiency. And the security of commercial software has become a national security issue. Oracle received precisely one response to this letter, and that was a request for money. Is there a more tone-deaf response than that?

We must act now to change the educational system for all computer science and computer-related degree programs, including industrial control systems, so they include security throughout the degree program. We should insist that universities submit a plan to alter their curricula, and we should link government research funding to phased change. If parents can tell their toddlers that they don't get any dessert until they eat their peas, the U.S. Government can certainly tie monies to computer-related curricula change.

Something else we can do today is stop making cybersecurity worse by using technology in ways we know very well we cannot secure and that creates huge systemic risk. We need look no further than the recent financial system meltdown in which massive computer programs could quantify all kinds of risk except the most important one: systemic risk.

One such area is Smart Grid, the idea that powerplants can use near-realtime measurements on usage—devices in your home—so we can price power better, be smarter about usage and build fewer plants. Nobody is opposed to doing more with less, unless, of course, the "more" includes a lot more risk.

And here's what we do know. We know we cannot secure millions of IP-based clients; the millions of PCs that have been co-opted into botnets are proof of that. We know that the SCADA protocols used in control systems were not designed to be attack resistant; they were originally used in electromechanical systems, where you had to physically access the control, turn the knob, and so on. Now we are increasingly moving to IP-based control systems and connecting them to corporate networks that, in turn, are connected to the Internet.

We know that some Smart Grid devices are hackable. For example, a prototype worm developed by a security research firm was able, in a simulated attack—thank heavens—to spread from meter to meter to take out power in more than 15,000 homes in 24 hours. We know that terrorists are increasingly interested in targeting utility grids. We know that there are PDAs—digital assistants—that talk SCADA, because it's just so expensive to send a technician to the plant. Dare I say, move the control rods in and out of the reactor? There's an app for that. Will we one day scram a reactor when someone was merely trying to answer the phone?

And last, we know that the people designing and building these systems are not taught secure, defensive programming any more than computer programmers are.

There are two things we can do now, and must do now. We should insist on some standards, through existing standards bodies, of Smart Grid components. NIST, for example, has led a cybersecurity working group that recently released a second draft of Smart Grid Cybersecurity Strategy and Requirements document. Good on them.

Second, we need better transparency on how Smart Grid components are built and of what they are built. There are some mechanisms that can help establish this transparency, such as the Common Criteria, which is ISO-standard, and the Department of Homeland Security materials on improving software assurance and acquisition.

Last, we do not think of the New Testament as a guide to critical infrastructure protection, and yet, Jesus contrasted the man who built his house on a rock with, quote, "a foolish man who built his house on sand." The rain came down, the streams rose, and the winds blew and beat against that house, and it fell with a great crash. The Gospel of Matthew.

This is an apt description of securing critical infrastructure. If our infrastructure builders do not understand the difference be-

tween building on rock and building on sand, our house will collapse in the first good rainstorm.

Thank you, and I'll be happy to take your questions.

The CHAIRMAN. Thank you.

[The prepared statement of Ms. Davidson follows:]

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

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am Mary Ann Davidson, Chief Security Officer for Oracle. I appreciate the opportunity to appear before you today, and I also want to commend the committee for tackling the issue of cyber security—it's a very tough and multi-faceted issue. I also want to thank the committee for including industry in the drafting process of cyber security legislation, partnership between government and the private sector is critical for making our public infrastructure safe and secure.

When many of us were young, we looked up to superheroes: Superman, Batman, Aquaman and Wonder Woman: the people who could do almost anything and were unstoppable (except—perhaps—by Kryptonite). When we grow up, most of us realized that there are no superheroes: many problems are very difficult to solve and require a lot of hard work by a lot of smart people to fix. So it is with the security of critical infrastructure: we cannot shine a signal in the sky and expect SuperNerd to come and save us.

Many intelligent people have proposed a number of ways we can help define the problem of critical infrastructure protection as it relates to cybersecurity, "bound" the problem space and improve it. There are two specific recommendations that may help stem the problems of the present and change the dynamics of the future: both are necessary to help secure not only today's but tomorrow's critical cyberinfrastructure.

First, we need to change our collective mindset so that elements of critical cyber infrastructure are designed, developed and delivered to be secure. We do that in part by changing the educational system so that we have a cadre of people who *know* that critical cyber infrastructure will be attacked—and they build accordingly and defensively. We do not generally think of the New Testament as a guide to critical infrastructure protection, yet consider the parable of the builders, in which Jesus contrasts the man who built his house on rock with ". . . a foolish man who built his house on sand. The rain came down, the streams rose, and the winds blew and beat against that house, and it fell with a great crash" (Matthew 7:24–27). This parable is an apt description of the problems in securing critical infrastructure: if our infrastructure "builders" do not understand the difference between building on rock and building on sand, our house will collapse in the first good rainstorm.

The second recommendation is more straightforward: we need to stop "upping the ante" on exposing critical infrastructure to—in some cases—unknowable risk—and we should walk away from the gambling tables until we both understand the odds *and* the odds are better. What we know now is that we continue to expose critical infrastructure to the Internet in the interests of saving money, which massively increases our attack surface, we do not, in many cases, know how exposed we are, and we have determined enemies. "Doubling down" is not a strategy—except a strategy for catastrophic loss.

Changing the Educational System

One of many cybersecurity risks the Department of Defense is concerned with involves the supply chain of software—more specifically, the risk that someone, somewhere will put something both bad and undetectable in computer code that will allow enemies to attack us more easily. However, that is but *one* type of supply chain risk we should worry about and perhaps not even the most critical one. In fact, "the software supply chain" at a fundamental level includes the people who design, code and build software. We should worry about the supply chain of *people* as much or more than the supply chain of software itself, because those who design, code and build software don't know how to build it securely and the institutions—with some notable exceptions—who educate them either don't know or do not care to know how woefully inadequate their educational programs are. (Some universities, of course, do care about security and have invested in improving their computer science curricula accordingly. Kudos to them.)

If we were having a rash of bridge failures, and we discovered that universities were failing to teach structural engineering to civil engineers, we would not be discussing how to redesign tollbooths and train tollbooth operators, or teach people how

to drive safely on bridges. Similarly, proposals to "certify more cybersecurity professionals" is only a remedy for the cyber threats to critical infrastructure if we understand the problem certifications attempt to solve and ensure that we focus on the *right set of professionals to certify*. This is especially true since "cybersecurity professionals" these days may well include Chad, the 12-year-old who installs anti-virus on his technophobic grandparents' computer.

Several years ago Oracle sent letters to the top 10 or 12 universities we recruit from [1]—more specifically, to the chair of the computer science (CS) (or equivalent) department and the dean of the school in which the computer science department resided—telling them that:

a. We spent millions of dollars fixing avoidable, preventable coding errors in software that lead to exploitable security vulnerabilities;

b. We have to train CS graduates in how to write secure code because they were not taught these skills in computer science programs;

c. We need universities to change their curricula to address this clear and present educational deficiency; and

d. The security of commercial software has become a national security issue.

Oracle received precisely one response to these letters, and that was a request for money to enable that university to create a "secure programming class." In the last 6 months, a representative that same university—at a Department of Homeland Security Software Assurance Forum no less—said publicly (and in apparent reference to the Oracle letter) that his institutions' graduates were "too good" for vendors like Oracle.

It's hard to imagine a more tone-deaf response to a "customer" request for a better "product."

Some have proposed that we certify "cybersecurity professionals" to improve the protection of our critical infrastructure. However, certifying cybersecurity professionals—presuming we could define the term precisely enough to avoid certifying absolutely everybody who touches an information technology (IT)-based system—is too late in the game. You can't secure something that was not designed to be secure or that has holes big enough to drive the QEII through. Putting it differently, in the physical world, do we certify interior decorators or the people who build the house? It's architects, engineers and contractors who are professionally licensed, not the people who move furniture around and pick out color schemes. (No disrespect to security administrators—or interior designers—is intended by this comparison; the fact remains that cybersecurity professionals cannot necessarily secure a system that was not designed to be secure.)

In the physical world, engineering degree programs are accredited and engineering is a profession. Engineering graduates take the engineer-in-training (EIT) exam—proof that they learned and absorbed basic engineering principles in their degree program as part of their career progression. Most who choose to actually practice the engineering profession must become a licensed professional engineer (PE). While it is true—as many academics are quick to point out—that we understand the physics of, say, bridge design, and there are—as yet—no "physics" of computer systems, that does not mean that we should not expect people who are being educated in computer science to know both what we know now, and what we do not know: specifically, how to think about complexity and risk. At any rate, the fact that Oracle and other large software vendors almost universally must teach the basics of computer security to computer science graduates building IT-based infrastructure should give all of us pause.

We know that embedding sound principles in curricula and reinforcing those principles throughout a degree program works: this is why physics is a "core" course for engineers and why civil engineers cannot conveniently ignore physics in upper level classes. We also know that an increasing number of professions involve computers and thus the need for "security"—embedded and reinforced throughout a number of curricula and a number of classes within those curricula—is critical. Control system design, for example, absolutely must include an awareness of sound security principles or we will merely repeat the mistakes we have already made. And yet, too many universities continue to fiddle while Rome burns, or at least, fiddle while Rome is hacked.

A modest proposal in pursuit of curricula change would be to link government research funding to phased educational reform in computer and computer-related de-

[1] A heavily redacted form of this letter is available at *http://www.oracle.com/security/docs/mary-annletter.pdf* and a larger discussion of the supply chain "personnel" issue is available at *http://blogs.oracle.com/maryanndavidson/2008/04/the__supply__chain__problem.html*.

gree programs. That is, cutting off all money until the curricula is fixed is counterproductive (as it penalizes institutions that actually are making positive changes even if they are not "there" yet). But we can certainly demand that universities submit a plan to alter their curricula that includes specific delivery dates for curricula change and insist that they make those changes as delivered—or else. Currently, there is no forcing function to change education. Many university professors are tenured and thus have no incentive to "cure." One of the few market forces we can exert is money—such as grant money. If parents can tell their toddlers that they don't get any dessert until they eat their peas, the U.S. Government can certainly tie research funds to phased curricula change.

There are two additional reasons to—immediately and with some urgency—forcefully impose curricula change on the universities that deliver the pipeline of people building critical cyber-infrastructure. The first is that we are already out of time: when the Soviet Union launched Sputnik, it lit up the skies and lit up our eyes. The U.S. rapidly moved to dramatically improve the science and technology focus of our educational system so that we, too, could conquer space. As regards cybersecurity, we have already had our Sputnik moment: in fact, we in cybersecurity have such moments over and over, every single day. The most damning comment one could make about the recent Google-China headlines is that for those of us in industry, it was merely the exclamation point on a long narrative, not an opening soliloquy.

The second reason is that everybody is looking for expertise to secure what we have today—not to mention, what we are building in our headlong rush to site critical infrastructure upon technical "sand." For example, the Department of Homeland Security has stated that they want to hire 1000 cybersecurity professionals.[2] Where will they find them? The military is standing up cyber commands[3] and it seems increasingly obvious that wars of the future will increasingly take place in the cyber realm. Where are these future attackers and defenders to come from?

In particular, the military views technology as a force multiplier and their information systems increasingly form the background of their ability to fight wars. What possible confidence can the military have that the network elements on which they base their ability to prosecute war can be trusted if the people who built them do not understand at a very basic level that all software can and will be attacked? The people designing and building software do not, in general, think, design and code defensively because they are not educated to do it. We might as well be turning out Marines who don't know that they have enemies, or what a firefight is or what "take the hill" means. The results would be and are predictable. Marines are lethal in no small part because they know there are enemies, and they train to annihilate them.

Slow Our Exposure to Systemic Risk

There is an old saying that goes, "quit while you are behind, and when you are in a hole, don't dig." Nowhere is this truth more evident than in our rush to increase the interconnectedness of critical infrastructure and its exposure to the Internet—an exposure that creates risks that we do not understand and thus cannot mitigate. We embrace the interconnectedness because the benefits—and cost savings—seem clear, but the risks are murky. No sensible person, of course, should say that we cannot do anything that involves risk. Life is about assuming risk.

That said, and as a cautionary tale of assuming risks we do not understand, we need look no further than the recent financial system meltdown in which massive computer programs could quantify all kinds of risk *except* the most important one: systemic risk. The financial superheroes "in charge" and the brilliant "quants" that were their super-sidekicks got it wrong. Nobody really knew the degree to which entity A was exposed to entity B and what would happen if the thread between them was snipped. It turns out; systemic financial risk was the Kryptonite that brought down Superman.

Alas, a lot of technophiles pushing new "problems" we need sophisticated IT-based solutions for, or those eagerly embracing new uses (and abuses) of technology, do not realize that everything—including technology—has limits. The "limits" are not necessarily those of bandwidth, or protocols we haven't invented yet. The most important limitation is our inability to make rational, informed decisions about risk because of complexities we simply cannot fathom.

In the many discussions on what the government can do to fix cybersecurity, including "spend more money on research," and "certify cybersecurity professionals,"

---

[2] *http://www.cnn.com/2009/POLITICS/10/02/dhs.cybersecurity.jobs/index.html.*

[3] *http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=222600639.*

it is worth noting that no single proposal will "save us," and certainly not any time soon. There is, however, one thing we can do today: stop making cybersecurity worse by rushing to use technology in ways we know very well we cannot secure and that create huge systemic, unknown (and thus unmitigateable) risk.

One such area is smart grid. The general idea, we are told, is to allow power plants to: (a) get lots of near-real time measurements on power consumption (*e.g.,* from your house) to better price power consumption accordingly and (b) do remote maintenance of grid elements (*e.g.,* deployed in your house). If we can do better demand pricing we can build fewer plants and be "smarter" about power usage. Nobody is necessarily opposed to "do more with less" premises, with one big caveat: what if the "more" is "more risk"—a lot more? More, in fact, than we can fathom. What we know about smart grid should—if not scare us—at least induce a very large gulp:

- We already know we cannot secure millions of Internet protocol (IP)-based clients: it's hard enough to secure servers. The millions of PCs that have been coopted into botnets are proof enough of that.
- We know that the SCADA (Supervisory Control and Data Acquisition) protocols used in control systems were not designed to be attack resistant: they were originally used in electro-mechanical systems where you had to physically access the control to use it (*i.e.,* turn the knob).
- We know people are increasingly moving to Internet protocol (I P)-based control systems, and connecting them to corporate networks that are, in turn, connected to the Internet. We thus know that people can access controls for things they shouldn't be able to from places they aren't supposed to be able to.[4]
- We know that many of the smart grid devices that have already been deployed are hackable.[5] For example, a prototype worm developed by a security research firm was able—in a simulated attack—to spread from meter to meter to take out power in more than 15,000 homes in 24 hours.[6]
- We know that terrorists are increasingly interested in targeting utility grids and in developing their hacking expertise to be able to do so. [7]
- We know that smart grid concepts are also starting to be implemented in gas and water utilities.
- We know that people have built personal digital assistants (PDAs) that "talk SCADA" because "it's so expensive to send a technician to the plant." (It won't be long before we hear: "Move the control rods in and out of the reactor? There's an app for that!" Some day we may have a power plant meltdown when all someone was trying to do is answer the phone.)
- And, last, we know that the people designing and building these systems were never taught "secure/defensive programming" any more than computer programmers were.

What we can infer from all the above is that the rush to "save money" is being done by people who fundamentally do not understand that they are vastly increasing the potential risk of a cyber attack that can be launched from any home. Against the grid itself. In a way that we do not know how to mitigate. In an increasingly hostile world. If we think saving money on critical infrastructure is more important than protecting it we might as well start sending the Marines into combat with slingshots (so much cheaper than M 16s) and expecting them to secure our Nation. Neither is acceptable, and both will involve needless and senseless loss of life.

Before we keep trying to "do more with less," let's take a deep breath, step back and think seriously about worst cases and how we avoid them in the first place. *Hoping* our enemies won't exploit a big shiny new attack vector once we've deployed is not a strategy. Actually minimizing the attack surface is.

There are a couple of things we can do to slow the lemming-like rush over the smart grid cliff. One of them is to insist on some standards (through existing standard setting bodies)—if not actual certification—of smart grid components. N IST, for example, has led a Cyber Security Working Group that recently released a second draft of "Smart Grid Cyber Security Strategy and Requirements" document.[8] It's a start.

---

[4] *http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf*.
[5] *http://rdist.root.org/2010/02/15/reverse-engineering-a-smart-meter/*.
[6] *http://www.wired.com/threatlevel/2009/10/smartgrid*.
[7] *http://www.scmagazineus.com/critical-condition-utility-infrastructure/article/161689/*.
[8] *http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628Feb2010*.

Second, we need a better transparency around how "smart grid" components are built, and *of what* they are built—given a lot of the underlying components may be commercial software that was not necessarily designed for the threat environment in which it will be deployed. It will also help those building critical infrastructure to know how robust the "building materials" are. There are existing mechanisms that can help establish that transparency, such as the Common Criteria (International Standards Organization (ISO)–15408) and the Department of Homeland Security (DHS) materials on improving software assurance in acquisition.[9]

Without knowing how software was built, and what care was and was not taken in development—we are building a house from components we know nothing about and hoping the resultant structure is sound. It isn't merely that a house built on sand cannot stand, it's that a house built of ice won't survive in the tropics and a house built of some types of wood won't survive in a termite-friendly environment. Without knowing what components are being used in the house, how they were designed and built—and with what assumptions—we have no idea whether even a house built on rock is going to stick around for the long haul. There are, after all, earthquake zones.

It may seem difficult to change the status quo, and yet we have to believe in the capacity for positive change—even if that embraces a clear and abrupt departure from the status quo. As the prophet Isaiah said, "Whether you turn to the right or to the left, your ears will hear a voice behind you, saying, 'This is the way; walk in it.' Then you will defile your idols overlaid with silver and your images covered with gold; you will throw them away . . . and say to them, 'Away with you!'" So be it.

The CHAIRMAN. And, finally, Rear Admiral Barnett, Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission.

STATEMENT OF JAMES ARDEN "JAMIE" BARNETT, JR., REAR ADMIRAL, USN (RETIRED), CHIEF, PUBLIC SAFETY AND HOMELAND SECURITY BUREAU, FCC

Admiral BARNETT. Thank you, Mr. Chairman and distinguished members of the Committee. Thank you for the opportunity to testify on this important topic.

My remarks to you today are focused on the transformation of communications by the Internet and broadband technologies, the cyberthreat that transformation has engendered, and how the role of the FCC to ensure communications is being invigorated to meet the challenge of the cyberthreat.

Advanced broadband communication technologies have dramatically changed to lives of Americans by enriching the way that we communicate, learn, work, and live. Virtually all major communication networks are now connected to the Internet; and, for that reason, those communication networks are vulnerable to cyber attacks.

Most cyber attacks target information systems attached to communication networks—the edge or end-users—not the communications infrastructure itself. Nonetheless, communications infrastructures are not immune to cyber attacks, and they have vulnerabilities. We should not have a false sense of safety. A successful attack on communication networks could have a severe or even catastrophic effect.

The FCC has an important role to play in securing broadband communications infrastructures in conjunction with our Federal partners. We are the congressionally mandated regulatory agency with authority over communication providers and communication

[9] *https://buildsecurityin.us-cert.gov/swa/downloads/SwA__in__Acquisition__102208.pdf.*

networks, and we must face the new reality that cyberthreats now imperil our communication networks.

When I came to—came aboard as the Chief of the Public Safety and Homeland Security Bureau at the FCC, our Chairman, Chairman Julius Genachowski, asked me to convene a working group to examine the Commission's cybersecurity posture and recommend courses of action. This group delivered a report to the Chairman, and many of its recommendations will be addressed in the National Broadband Plan that will be delivered to Congress next month, in March. In the report, and in the National Broadband Plan, we developed a roadmap to fulfill our cybersecurity role and responsibilities. And I'd like to address just a few points in that—from that roadmap.

First, the FCC can provide the Nation a much greater situational awareness of the status and performance of the Internet, including attacks, than it currently possesses. Many of the owners and operators of the backbone of the Internet are communications companies who are licensees of the FCC. One of the reasons why the communications in America are so reliable is that, under FCC rules, those licensees provide us with near-realtime data on network outages and problems, so that we can analyze that data and work on solutions. We also have a successful voluntary program of reporting in times of disasters and emergencies.

If these near-realtime outage and incident reporting systems were extended to the Internet, the FCC could provide the Nation with an enhanced situational awareness of attacks and incidents and provide vital information for defense against attacks and restoration of communications.

Second, there are things that FCC can do to prevent or mitigate the effects of cyber attacks. For example, a previous FCC Federal Advisory Committee, the Network Reliability and Interoperability Council, or NRIC, developed a set of detailed cybersecurity best practices that are intended to be implemented by communication providers on a voluntary basis. We're exploring the creation of a voluntary certification program, possibly using these best practices as criteria to provide network operators with additional incentives to improve their cybersecurity posture. And we're also looking to other voluntary incentives.

In December 2009, the FCC launched a new expert advisory panel called the Communications Security Reliability and Interoperability Council, or CSRIC, to examine and recommend other cybersecurity solutions, such as how to stem the stream of malware that arrives at our networks.

We're increasing our contacts with communication regulators in other nations, since cyberspace and security are not local, but are truly global. We're at the start of a long journey, working with our Federal partners and with industry to secure our Nation's vital infrastructure against new and rapidly evolving threats. And, Chairman, we are determined to do so.

Thank you for your—the opportunity to testify.

[The prepared statement of Admiral Barnett follows:]

PREPARED STATEMENT OF JAMES ARDEN "JAMIE" BARNETT, JR., REAR ADMIRAL, USN (RETIRED), CHIEF, PUBLIC SAFETY AND HOMELAND SECURITY BUREAU, FCC

Senator Rockefeller, Ranking Member Hutchinson and distinguished members of the Committee, thank you for the opportunity to testify on the important topic of cyber security, and thank you for your leadership in holding this hearing to address this urgent problem.

My remarks to you today are focused on the transformation of communications by the Internet and broadband technologies, the cyber threat that transformation has engendered, and how the traditional role of the Federal Communications Commission to ensure communications is being invigorated to meet the challenge of the cyber threat.

Advanced broadband communications technologies have dramatically changed the lives of Americans and others around the globe by enriching the way they communicate, learn, work and live. The Internet, which relies on broadband communications infrastructure, is now a central part of American interaction of all types. However, the manner in which the Internet developed has left it exposed to cyber attacks. Specifically, the Internet, which started as a small research network, has evolved into a global network connecting over a billion people who rely on it for social, economic, educational and political applications, among others. The Internet's core design philosophy was initially based on easy connectivity. The underlying Internet protocols and architecture were not designed to be secure. As Internet usage has increased and has become mainstreamed for everyday life, communications providers have responded by adding features to improve the security of their infrastructure and the services that ride on it.

As the public and private sectors continue to move toward more online usage, bad actors, including criminals, have begun to lurk in the shadows of cyberspace where they can launch costly attacks on end-users. In 2008, the FBI Internet Crime Complaint Center logged $265 million in reported losses for Internet users, the highest loss ever reported. No one is immune from attack, whether consumers, government users or even our Nation's most sophisticated companies. Last year, it was reported that ten to twenty terabytes of data were pilfered from U.S. Government networks by a foreign entity, and in January Google reported that it was subject to a sophisticated attack originating from China. Reports show that at least ten other large companies, including finance, media and chemical companies, have been the targets of similar attacks. As attacks become more persistent, breaching computer systems and establishing a foothold, these attackers are able to compromise personal, confidential and classified information. We have seen the effects of dedicated cyber attacks on Estonia and the Republic of Georgia. Critical infrastructure sectors, such as energy, finance and transportation, can all fall victim to these attacks.

All major communications networks are now connected to the Internet, and for that reason, those communications networks are vulnerable to cyber attacks. Most cyber attacks target information systems attached to communications networks, the edge or end-users, not the communications infrastructure itself. Cyber attackers currently tend to view the communications infrastructure as the necessary superhighway that will carry them to their victim. Accordingly, they are reluctant to make it impassable.

Nonetheless, communications infrastructures are not immune to cyber attacks, and they have known vulnerabilities. Accordingly, we should not have a false sense of satisfaction with regard to the survivability of our broadband infrastructure. A successful attack on communications networks can affect all end-users that rely on broadband infrastructure. For example, as 9–1–1 networks migrate from today's technologies to Internet-based technologies concerns about the vulnerability of these systems to cyber attacks have mounted. A successful attack on such a network could severely obstruct the ability of our first responders even knowing of emergencies.

We cannot allow the absence of a successful attack make us complacent. The FCC has an important role to play in securing broadband communications infrastructures. We are the Congressionally-mandated regulatory agency with authority over communications providers and communications networks. We must face the new reality that cyber threat now imperils our communications networks and therefore our wellbeing and even lives.

With the changing shape of the telecommunications infrastructure and usage patterns, it is incumbent on the FCC to reassess our role in cyber security. When I came aboard as Chief of the Public Safety and Homeland Security Bureau, FCC Chairman Genachowski asked me to convene a ninety-day working group to examine the Commission's cyber security posture and recommend future courses of action. This group delivered its report to the Chairman on November 30, 2009, and many of its recommendations will be addressed in the National Broadband Plan

that will be submitted to Congress in March. Our Working Group report demonstrates the critical role that the FCC has in cyber security, in conjunction with its Federal partners. This report, in conjunction with the National Broadband Plan, leads us to our plan to become further engaged in cyber security. To this end, we have developed a roadmap in which we plan to address cyber security utilizing our past experience, technical expertise and our regulatory relationship with the FCC's licensees to protect the communications infrastructure. I would like to mention six major points from that roadmap.

First, we believe, based on past experience, that many cyber security challenges can be met through public-private partnership arrangements with industry. However, it would be ill-advised to assume that intervention is not needed. In some cases, obligations may be necessary. The Commission has a vital role to play in these situations, and we will be working to craft a regulatory approach to cyber security that strikes the right balance.

Second, we believe there are things the FCC can do to prevent or mitigate the effects of cyber attacks. For example, recently, the Network Reliability and Interoperability Council, an FCC Federal advisory committee consisting of leading industry executives and practioners, developed a set of detailed cyber security best practices that are intended to be implemented by communications providers on a voluntary basis.

We believe the opportunity exists for us to build on these best practices to provide network operators additional ability to improve their cyber security and to increase the adoption of these best practices. A recent survey by PricewaterhouseCoopers found that organizations following best practices experienced significantly lower impact from cyber attacks, something that commercial industry should find attractive. We believe that based on this survey that we should explore methods, such as voluntary certification of compliance with best practices that would create market-based incentives to increase cyber security.

Third, we believe that a significant area for FCC involvement in cyber security is to secure and analyze additional data received from all broadband service providers concerning network and service disruptions. However, our past experience in receiving data from communications providers concerning disruptions in their networks has been proven effective at providing us early warning of potential problems and attacks on the Nation's existing communications infrastructure. This information allows us, working with our Federal partners and the communications industry, to expedite restoration of service. Our work, which is based on a sector-wide view of communications outages, also allows us to spot industry-wide or carrier-specific reliability and security matters. We use this information in conjunction with DHS and communications providers to produce long-term improvements. For example, we recently observed a statistically significant upward trend in the number of events affecting wireline carriers. We worked with industry to establish a team of experts who examined the data in closer detail and developed a set of recommendations. In the intervening months we have measured a 28 percent decline in this category of outages. Obtaining similar information from broadband and Internet service providers would enable the FCC and its Federal partners to work with industry on sustained improvements to Internet-based infrastructure. We are currently examining the best path forward to obtain this information.

A fourth way in which we are exploring more active involvement in cybersecurity is increase our ability to prepare reports which contains situational awareness on broadband communications infrastructure during disasters for use by our Federal partners, such as the Department of Homeland Security (DHS). We currently gather such data for traditional communications, and it has proven invaluable in emergency management and communications restoration. Accordingly, we plan to coordinate with DHS and communications providers in the near future to plan and implement a cyber attack situational awareness system.

Fifth, another avenue we are pursuing is how to best address the constant stream of malware arriving at the network, frequently from end-users who are not aware that their systems are compromised. The Commission has recently established an advisory committee, the Communications Security, Reliability and Interoperability Council, known as CSRIC. An important function of the Council is to examine this problem and to recommend methods that communications providers can implement to protect their networks from malicious traffic. We expect to see reports from this Council in the near-term.

Sixth, and finally, cybersecurity is by nature international. The networks are global, the threats are worldwide, and the human component is universal. Through the State Department, the Commission participates in various international activities and fora such as the United Nations International Telecommunication Union (ITU) in which cyber security is an issue. Cyber security is increasingly raised as an issue

in discussions with foreign regulators and at international meetings and conferences, and the international aspects of cyber security is also a more prevalent topic in the domestic arena. Going forward, there will be increased need and opportunities for, greater FCC participation in activities involving international aspects of cybersecurity—both in the United States and abroad.

My intention has been to describe to you our vision of the FCC's role in cyberspace and what we are doing to secure our critical communications infrastructure in a broadband world. We are at the start of a long journey, working with our Federal partners and industry, to secure our Nation's vital infrastructure against a new and rapidly evolving threat, and we are determined to do so.

Thank you for the opportunity to speak to you today.

The CHAIRMAN. Thank you very much, Admiral Barnett.

Let me ask the first question. The—this is directed to Admiral McConnell and Mr. Borg and to Ms. Davidson.

You all talked, in various ways, about the need to have people understand this at a very early age. You know, this—they say, you know, kids are too fat these days, we ought to do more exercise. Those things are—exercise is being cut out, sports are being cut out, and sort of crowding the curriculum is a really tough thing to do. On the other hand, if people don't understand the threat of cybersecurity, it's all lose from now on.

I made the point, Ms. Davidson, that 85 percent of the critical infrastructure in this country are owned and controlled by the private sector. And we found, as we were—at least I found, as we were drafting this legislation, that companies—I'm not saying Oracle; I'm not necessarily saying big telecommunications companies—but, companies tended to resist the idea of the government sort of getting in the way of what they were already doing, which they felt to be adequate. Now, my experience in general security with large companies, and particularly like powerplants and chemical plants backed up against rivers, and the rivers are patrolled by the Coast Guard, except, of course, that there aren't enough boats or people, so they're really not controlled by the Coast Guard, so they're all vulnerable, but they say they're doing the job, and thus, they—they're—you know, we had a lot of engagement with industry. And so—and I look at your testimony here, Ms. Davidson, and it's interesting, because I'm not sure what you're saying. Your second recommendation, we need to stop upping the ante, as you said, on exposing critical infrastructure—in some cases, unknowable risk—and we should walk away from the gambling tables until we both understand the odds, and the odds are better. Doubling down is not a strategy, except a strategy for catastrophic loss.

Now, what I'm—what I'd like the three of you to comment on is, in that I think we all agree there has to be this coordination between government and the private sector, are you, in a sense, walking away, saying, "We have to let time pass so that people understand this problem better and kids—it's part of their curriculum"? And—or are you not? And, Admiral and Mr. Borg, if you could comment on this problem of how—don't we have to take action really soon? But, then, you've already said, whatever action—I think, Mr. Borg, you did—whatever action we take is going to be outdated in 3 years anyway. So, talk to me a little bit about this business of cooperation, what we do. Is legislation any good? What do you propose?

Admiral.

Admiral MCCONNELL. Sir, let me use an example that touched me personally. I'm old enough to remember Sputnik. And that happened in 1957. And shortly after, the—an Act was passed. I don't recall the exact name, something to the effect of the National Defense Education Act. I went to college on that Act, and it's likely I would not have gone to college except for that Act. So, when I talk about an education bill—you heard in my opening comments, I think the Nation reacts to two things: crisis and money. Crisis will move us to act, money will move us to act. So, if there is a bill that invests in the youngsters of this Nation to make them smart about cyber and cyber issues, and safe code, and secure code, and so on, I think we will start to mitigate this problem.

I'll use an example. One of my colleagues is Gene—Dr. Gene Spafford, at Purdue. Early mover, wonderful program, struggling to keep it alive, because there's no interest or funding in it. So, I think, since we react to crisis or money, that it's going to take an investment, probably something on the order of the National Security Education Act of 1958, for us to address this problem. And if we do that, I think we'll make progress.

The CHAIRMAN. Will we make progress simply because people grow up and go into business and go into government and, therefore, work things out? Or——

Admiral MCCONNELL. It's——

The CHAIRMAN.—it's a necessary starting point, no matter what happens.

Admiral MCCONNELL.—it is a necessary starting point. And, for me, the example is, we put a man on the moon in 10 years. So, Sputnik happened, the bill was passed, lots of engineers and scientists and physicists, and so on, that were educated. And when President Kennedy set it as a goal, then, 10 years, we actually did it. So, for me, it's a necessary step to get us started so we have the skill sets.

Now, one of the things I'm worry about is, we are significantly outnumbered, in terms of population in China, in India, and other places. So, we don't have a birthright to intelligence. I mean, there are smart people all over the world. It's an even distribution. And others are investing in this in a major, major way. So, if we're going to compete and be competitive and influence the world for a global standard in cooperation in this arena, in my view, we have to produce the electrical engineers, computer scientists, and other technical talents that will allow us to do this.

The CHAIRMAN. OK. So, we—that is stipulated. I think there would be no argument on that at all.

In this matter of cooperation between government and business, and the point I raised, Ms. Davidson, about "How do I interpret what you said?"—I know that it was basically the business community that came in and say, "Look, we're fine. We know what we're doing on this." I'm simplifying a little bit, obviously. But, "We don't need the government involved in this." The Admiral and others are saying that the government has to be involved in this, or else nothing really is going to happen. And so, I don't—when you say "walking away," I want to know what you mean.

Ms. DAVIDSON. What I meant by that was, there's an expression, "Quit while you're behind, and when you're in a hole, don't dig."

And the reason I use Smart Grid—and I was very careful there; I didn't say, "Oh, let's not do anything that's insecure." You know, everything in life is about assuming some risk. My concern is our failure to understand systemic risk and going forward. And based on what we know now—and all of those comments had footnotes to external reports—what we see here is—this looks like we're assuming an asymmetric risk we don't understand. I didn't say, "Let's not do more with less."

The CHAIRMAN. But, you did say——

Ms. DAVIDSON. "Let's not make use of technology."

The CHAIRMAN.—doubling down is not a strategy, except a strategy for catastrophic loss.

Ms. DAVIDSON. I did say that. And my comment was that we continue to look at more ways we can use an IP-based backbone, when we know, today, we cannot secure clients. And that's, on a technical level, saying, "OK, if I have to physically go in a plant to turn a knob to do something bad, that's something I can limit." If I'm now putting a device in everyone's home that may or may not—that's the question mark—be appropriately designed for a threat environment, you know, then I'm basically saying, "OK, now I've got a million ways to get into something." Now——

The CHAIRMAN. Well, my——

Ms. DAVIDSON. So, what I'm saying is——

The CHAIRMAN.—my time is——

Ms. DAVIDSON.—is, let's understand—try to understand the systemic risk. Let's look at how we actually impose enough order that we understand what kind of risk we're assuming. Right now, some of these devices have been hacked. We don't know how they're built. We don't know whether—there is no certification program for the devices. I have concerns about that——

The CHAIRMAN. All right. Look——

Ms. DAVIDSON.—based on just what I know.

The CHAIRMAN.—my time is out, OK? My time is out, and you have to respect the rules of this committee.

I want to come back to you, because I don't think you've answered the—my basic question. I think you've reaffirmed my concern, "Until people understand everything, or until everything is prepared, don't act." Now, you do say you're going to act in two ways, but I want to get back to that.

In the meantime, Senator Snowe.

Senator SNOWE. Thank you, Mr. Chairman.

I guess it gets back to the question about, What will be effective incentives for the private sector? I mean, if the private sector owns and operates 85 percent of the infrastructure, then obviously we have to concentrate on providing the essential incentives for them to adapt.

What do you think would be effective private-market incentives, and is that the appropriate focus? Should we compel them? Should we create incentives, in terms of adopting best practices versus mandating standards? What approach do you believe we should take that would be the most effective in that regard?

Admiral McConnell?

Admiral MCCONNELL. What I attempted to do in my opening remarks—to make the analogy that in those historical cycles, we go

through this each time. So, if we were having this discussion about railroads and robber-barons, you know, way back in the 1880s, those that were in the railroad business would argue very strongly, "We don't want the government involved." So, what we did was have legislation to break it up and regulate it, and so on.

So, the way I would think about it is, the current system is not secure; and so, without prescribing exactly what the answers are, it is a requirement to make it more secure. Now, there is talent that exists to have that dialogue, and in a constructive way. It will introduce tension in the system. There will be those that argue that we shouldn't do this. There will be those that say the Government's going to spy on its own citizens, and so on. But, it is setting an objective to make it secure, to achieve the basic elements of security—the basic elements of making something secure, which I tried to highlight, with authentication and so on. Those things are essential when the transactions are of such significance they affect a broad portion of the population.

So, I think, properly framed, we could create such a framework that would cause us to move forward in that direction. But, it would be required; it would be mandated. Because industry is not going to embrace this unless they're forced to do it.

Senator SNOWE. Yes. Dr. Lewis? Dr. Borg?

Dr. LEWIS. Let me—I was a regulator for 3 years, right? And what I found is that most companies will try and do the right thing, and some companies will always do the right thing, and some companies will never do the right thing; and so, if you don't compel them, you're not going to get the right thing. And since this is a network, and they're all connected, if 10 percent don't do the right thing, then 100 percent could be vulnerable.

So, incentives are great, but what I'd also say is, How do you ensure compliance? And that leads me to a mandatory approach.

Senator SNOWE. Yes. Dr. Borg?

Mr. BORG. Yes, I urgently would like to talk about this, but I hardly know where to start.

I think the government urgently needs to do something. I think most of the things in your bill, broadly speaking, need to be done. However, we have a lot of things here that aren't working in the markets. Government intervention is needed to help those things to work.

The sheet that I waved—that I held up—lists 21 things that you could consider doing to help markets function better. Some of those things you're already proposing to do; some of them are already in your bill. But, there are many other ways in which these markets are not working.

There's a tendency, left over from the Cold War, to think that we have two choices where markets are concerned. One is to be the commissar and dictate from the government what everybody should do, and the other is to go, "Whoopee, let's hope the markets will do it on their own."

In fact, markets are engineered into existence, and the way they work is greatly shaped by government policy. Things that the government decides about what kind of information should be made available can hugely shape the way a market functions.

In this area, we have a number of markets where there's insufficient information for any of the participants with the best intention in the world to do the right thing; there is just no way they can make the right choices, where cybersecurity is concerned.

We have other situations where there are financial impediments to them doing the right thing. I completely agree with James Lewis, that we have a lot of people out there who would do the right thing, but we shouldn't be penalizing them for doing so.

We have other situations where people are ready to jump in and supply the kind of security that is needed—supply products that will provide the right security, but there are economic impediments for them doing that.

So, there's a whole area here that needs to be—opened up for discussion, a whole area of possible government action that's really not being addressed.

Senator SNOWE. Ms. Davidson, would you care to comment, or Admiral Barnett?

Ms. DAVIDSON. So, there are lots of ways to correct markets—market imbalances. And, you know, we can talk, as a public policy issue, about, Is this more effective or that more effective, or is it regulatory or something else? One of the things I have pushed for, because I think it could be effective, is—and I believe I talked about this in the context of Smart Grid, but I talked about it in a much larger context—is a little more transparency around how people build their software. Why is that important? Because at least the people who are taking a piece of software that may not have been designed for some particular purpose, but is general-purpose software, need to understand what was done and not done. You know, we know more about used cars than you do about a lot of pieces of software that are used in really large systems. So, at least forcing some transparency, which is what DHS was trying to get at, would require someone to show, What did you do, and not do, in development? My entire group—purpose in living is to enforce compliance around our own organization which is that transparency. You know, which groups do, and do not do, particular things. And how we build software goes to a security oversight board and it goes to our chief executive officer. So, we know, at any point in time, here's where we are, in terms of complying with our own development processes. We state it is—what we believe are to be best practices.

Now, is that perfect? No. Does it mean that somebody, maybe in the Defense Department, who's buying a piece of software and going to deploy it in some system we have no knowledge of, understands what they're getting and not getting?

Forcing transparency, by the way—it's a strange analogy—it's the bathing-suit test. When someone puts on a bathing suit around March, and they know they're going to go out in the water in June, by and large, they're going to look at themselves and say, "I look terrible. I need to get a trainer, cut out the carbs. I want to look good next to the three other people at the beach." So, forcing more transparency actually does elevate people's performance, in that you're probably going to do no—more if you know that someone's looking over your shoulder. It's not perfect; it won't cure everything, but I think that, as part of that correcting that market im-

balance, is—people need to understand, "You gave me a piece of software. What does it do, and not do? How well does it do it? And what did you engineer into this? And what were your assumptions about how it was going to be used and who is going to attack it?" That's not perfect, but it's a good start.

Senator SNOWE. Thank you.

Ms. DAVIDSON. And the government could enforce that, through procurement.

Admiral MCCONNELL. Senator, could I offer one other——

Senator SNOWE. Yes.

Admiral MCCONNELL.—quick comment—example. In the late 1960s, early 1970s, the United States dominated the semiconductor industry. At a point in time, we went from 80 percent to 20 percent. So, we had to do something about that, because it was so vital to us. So, what we did was create a public-private partnership. It goes by the name of Symantec. And Symantec—I think, it—I don't get the—remember the exact numbers, about 250 million on the government side, about 250 million on the private-sector side. We recaptured the semiconductor industry. That's the kind of thing that we could invest in here, with regard to cybersecurity. It would create the transparency that the case has been made well for. If——

So, there are a series of things that could be done to put us in a position to create the kind of infrastructure that we need that's secure enough to do the Nation's business.

Senator SNOWE. That's an interesting analogy.

Thank you.

The CHAIRMAN. Thank you, Senator Snowe.

Senator Ensign.

STATEMENT OF HON. JOHN ENSIGN,
U.S. SENATOR FROM NEVADA

Senator ENSIGN. Thank you, Mr. Chairman.

I agree with you, in how important and how critical these issues are to our Nation's economy and our national security; it's very important that we have this hearing today and that we explore it going forward into the future. And I appreciate the input of our witnesses today on an incredibly complex issue.

Admiral McConnell, I have a great deal of respect for you, but when you're talking about security in other industries, the Internet and technology today is changing so much more rapidly than any of those other industries ever did. And also remember that with railroads we came in much later. The airline industry, as well. I mean, can you imagine if the government would have come in too early, for instance, in the airline industry, before it became a mature industry?

The question is somewhat about balance. We do want to make sure that innovation occurs, as well. But, cybersecurity is very, very important for all of us; for all of our personal identities; for our financial security, where somebody could steal the money out of your bank account; for protecting some of these critical systems that we have, like Smart Grids; and for all of the other things that you all have laid out today.

Getting to a question, I would ask each one of you to succinctly talk about what you believe is the single biggest cybersecurity vulnerability that we have today. If you could tell this committee just one thing, what would you say the government should focus on?

Admiral MCCONNELL. I'll go first, if that's all right.

Senator ENSIGN. Yes. Just right down the line.

Admiral MCCONNELL. The area would be the financial system, because it—as the comments, I made earlier, about it being vulnerable. And the issue is, the authorities for dealing with it are divided by statute, and it's compartmentalized in boundaries. So, as a nation, cyber respects no boundaries; and so, it's going to take some action on the Hill for various committees who oversee pieces to address it more holistically for the integration of the problem.

So, if you think about it as communications, exploitation of communications, attack of communications, or defense of communication, different statutes, different departments, different committees, and it's, How would you put that together in a way that you can ensure the effect of successful communications while doing the things that would allow you to gain insight of a potential adversary and then mitigate the risk at network speeds, which are milliseconds? So, that's the challenge.

Senator ENSIGN. Dr. Lewis?

Dr. LEWIS. We, in our report of December 2008, said that the one thing you ought to focus on is securing cyberspace. And there were three components to that: the financial grid, as you've heard; the electrical grid; and the telecommunications networks.

And so, I would say you need to think about, What is it that gives us this wonderful capability to do things over the Internet? And you need those three things. Focus on them.

Senator ENSIGN. OK.

Mr. Borg?

Mr. BORG. Three of us here were on the Cyber Commission and heartily endorse that report that Jim wrote.

It's—the center of all this has got to be, however, critical infrastructure industries. That's what we mostly need to protect. That's what could do us the greatest damage. That's where the government needs to be focusing its attention.

Right now, if an electrical company wants to improve its cybersecurity, it can't get permission to pass on the minute rate increase that that requires; it can't get permission from the local regulatory organizations.

With the best desire in the world to improve security, the impediments to these companies doing the right thing are really great. So, one of the first things to do is to remove the impediments and make sure that there is a positive incentive to take care of these urgent issues.

Senator ENSIGN. OK.

Ms. Davidson?

Ms. DAVIDSON. I would certainly echo what my colleagues have said, but I also want to distinguish between something that is important but not urgent. And that—it still gets back to this educational system, particularly college systems. We don't send Marines out to take the hill who don't understand that there are enemies—they will attack them—what weapons to use and how to se-

cure the perimeter. And yet, we are training—the people who build IT systems are building infrastructure. They don't understand that they're building infrastructure, with all that that implies, and they particularly do not understand the difference between things—you know, good input, bad input, and evil input. Until we change the mindset of people to understand their systems will be attacked, and to build and design accordingly, we're not going to change the structure. We might address it today or next year, but the next generation coming forward will not understand that we're continuing to build infrastructure, and the responsibilities. We have to invest, today, in changing the mindset, and that's the educational system.

Senator ENSIGN. Admiral Barnett, before you answer—Ms. Davidson, you mentioned the government hanging carrots out there. We give them a lot of money from the Federal Government to tie in certain things. Remember, however, the private sector also has great influence. I know Oracle is trying to get the universities included. But, collectively, the private sector could have greater influence, because there's a lot of money that comes from private donors to the universities, as well, and I would encourage you all to get together, and especially with some of the larger donors who understand the critical importance of what you were just talking about, to encourage the universities to change what they're doing. And so, maybe we could hit it from both sides.

Ms. DAVIDSON. Thank you.

Senator ENSIGN. Thank you.

Admiral Barnett?

Admiral BARNETT. Senator Ensign, it may be somewhat a parochial answer, but, obviously, coming from the FCC, we see making the telecommunications networks and infrastructure secure to be a primary focus. We—you know, of course, going back to Senator Snowe's question, as well, the front line, of course, are private companies—the commercial things. But, there may be a role for regulation in such things as Admiral McConnell mentioned earlier, such as authentication, identity management, that could help secure—and you can't have piecemeal answers to that. A regulatory framework may be able to help bolster the private companies in protecting our telecommunications infrastructure.

Senator ENSIGN. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much, Senator Ensign.

Senator Pryor.

STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairman, and thank you for holding this hearing.

Admiral Barnett, I'd like to start with you, if possible.

And when I think of the FCC——

The CHAIRMAN. Incidentally, Senator—I mean, Admiral McConnell has to leave in about 5 minutes, so if—particularly if anybody has questions for him.

Excuse me. Go ahead.

Senator PRYOR. OK. Thank you.

When I think of the FCC, I think of, you know, your role of regulating, say, telecommunications, for example, and making sure there's competition and consumer protection, and all those types of things. But, are you saying that there—FCC does have a role in protecting our communications and our Internet?

Admiral BARNETT. Senator, what I would say is that we have a role in making sure that we have the best policies and best practices to ensure. I mean, our traditional role in—under the Communications Act is to ensure and promote that there is a vast, reliable, nationwide, global wire and radio communications system. To the degree that the Internet is now connected to our communication networks, the FCC has a role in doing that. And so, what we have to do as we go forward is make sure that we are continually looking at those policies and making sure that we are bolstering our networks. So, yes, sir, we do have a role.

Senator ENSIGN. Ms. Davidson, let me ask, if I may. We've heard a lot today about the public sector and the private sector. I think, obviously, we all need to do a better job of working together to come up with smart policies, in a lot of different ways, to make all this happen like it should. But, right now, can the private sector talk amongst themselves about what's going on out there, and can you share information? Or when you start doing that, do you start to get into an antitrust problem or another environment that companies either can't do legally or are just reluctant to do because of competition?

Ms. DAVIDSON. You know, I think some of that's out of my area of expertise. I have been told that there are sometimes some challenges. A lot of the—a lot of it has to do with—at some point, it's knowing who you're dealing with. People talk a lot about information sharing, and I'm all for that, but we need to remember, information sharing is a tactic, not a strategy. So, it gets down to information sharing about what, for what purpose, with whom, and how is that going to be used? So, I'm sorry I can't give you a better answer. I'll be very happy to research it and get back to you to make sure I'm giving you a more precise one.

Senator ENSIGN. Admiral Barnett.

Admiral BARNETT. Senator, if you don't mind me jumping in on that. But, that is one of the things that I think the FCC can help. Right now, we've had a very—a great deal of success in the traditional communications world by getting information on outages and problems in the communications network. Because companies are not—competitors are not going to be willing, nor is it proper for them, to share that information with each other. And yet, at the FCC, it's confidential. We can look at it; we can analyze what's happening across the entire network—analyze it and work on solutions. It's been very effective for our legacy communications systems.

One idea is to explore, Could that be extended to the Internet, and could we obtain the same success in getting situational awareness of what's happening?

Senator PRYOR. Good. Thank you.

Admiral McConnell, let me ask you—I know you need to leave in just 5 minutes or so. You gave a very strong opening statement, and your insights have been very interesting to the Committee

members. But, you know, you focus pretty much solely on U.S. policy. Is there a need for an international policy here that, you know, the U.S. either leads or the U.S. plugs into? I don't know that we've talked a lot about international policy.

Admiral MCCONNELL. And, sir, my view is, it can't be solved without an international approach. And I don't—I apologize for being the history buff here today, but I go back to think about the face-off between the United States and its allies and the Soviet Union in the cold war. So, it was an international dimension of NATO and the other allies that brought that to a successful conclusion, from our point of view.

So, I think this is a global problem, and it will require interaction and agreement at an international level, probably starting with the nations that already have alliances, and so on. But, at some point, it's going to have to—in my view—it will have to migrate to nations that we currently see as, if not adversaries, certainly competitors.

Senator PRYOR. Dr. Lewis, let me ask you—and this may be my last question, because I may be out of time—but, just for the media and for laymen, like myself, can you describe—can you give us two or three scenarios of what a cyber attack might look like? I mean, we talk about this, but what does that mean to the—you know, the average Joe out there in this country? Tell us what a cyber attack might look like.

Dr. LEWIS. Sure. And I think we need to divide it—it's a great question—need to divide it into two parts. The first is, then, as you've heard from Scott and from Admiral McConnell and from everyone else on the panel, we're attacked every day, and we're successfully attacked, and it's the economic damage that we have to worry about.

So, what would a cyber attack look like? It would look like being bled to death and not noticing it. And that's kind of what's happening now. All right? So, the cyber attack is mainly espionage, some crime. We've seen a good one. I don't know if you saw it, but a couple months ago a bank, over a 3-day weekend, had $9.8 million extracted from its ATMs. That was a good cyber attack. Caught some of the guys who did it. The mastermind probably lives in Russia, not under attack.

I don't worry too much about terrorists, and I'll tell you why. Because terrorists are nuts. If they had the ability to attack us, they would have used it, right? So, the notion that they're waiting for Christmas or something—they know how to do it. Eventually, they will get it, right? Eventually. And they will not be constrained.

There are people who could attack us now: Russia, China, some others. Our military—potential military opponents. Sorry. And we know they've done reconnaissance on the electrical grid. So, could they turn off the electrical grid in the event of a conflict over Taiwan or Georgia? Sure. That's what it would look like. Could they disrupt the financial system? They might, if they thought that they were either in really desperate straits or if they thought it wouldn't hurt their own bank accounts, right? But, I think that's what you want to look for.

Right now, huge losses through espionage, growing losses through crimes, and the potential of tremendous damage to critical infrastructure if we get into a fight.

Senator PRYOR. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Pryor.

Senator Begich.

STATEMENT OF HON. MARK BEGICH,
U.S. SENATOR FROM ALASKA

Senator BEGICH. Thank you very much, Mr. Chairman.

And I'll try to be quick with these, because I have to be somewhere at 4 o'clock.

But, let me ask Admiral Barnett, if I can. I was listening to your response to Senator Pryor in regards to, kind of, the role the FCC is now playing or will play in the future. I sit on the Armed Services Committee, and we've gotten briefings on DOD issues around cybersecurity. Can you, from your perspective—who do you think, within the general government—I know Homeland Security, to some extent—but, who has the full authority—for example, if you have recommendations of things that should be done, who pulls the trigger?

Admiral BARNETT. Well, I don't know that we have any triggers to pull. We're a regulatory agency.

Senator BEGICH. Right. I understand that.

Admiral BARNETT. But, we work very closely with the National Communications Systems, with DHS, and that's where we have most of our conversations, our information sharing. The information that we do get is applied to the National Communications System, on outages and network problems. We would see that being extended to other types of problems that we're talking about today.

So, primarily focused on DHS, although we work with a lot of our Federal partners, including DOJ. We're a part of the Joint Telecommunications Resource Board that advises OSTP.

Senator BEGICH. Do you think, just—in your experience at this point, do you think they're well coordinated among the agencies?

Admiral BARNETT. Well, as far as I can tell, we have good communications, we have good relationships and good information flows. We have—I'm not positive, while I've been in office, we've been tested on that. And for that reason, we participate in exercises to make sure that there are good information flows. Our most recent one was back in January, a tabletop conducted with——

Senator BEGICH. Right.

Admiral BARNETT.—OSTP and Joint Telecommunications Resources Board.

Senator BEGICH. What's the—do you think the agencies that you're working with have the resources they need to do the work to make sure—or are there gaps that have been identified, or you can identify?

Admiral BARNETT. You know, Senator, I'm not positive I could speak for those agencies. I can say that, after Chairman Genachowski asked us to do our own review, part of the things that we came up with is that we needed to increase our talent pool with regard to cybersecurity, and consequently, we launched a program to do that, to make sure that we have the talent that we need.

It goes back to the question that the Chairman was talking about earlier, is that we need to make sure that there's an educational pool out there. One of the things that I've been, even before coming to the FCC, concerned about is the precipitous drop in computer science majors that this country has been producing since 2000. I mean, I think it's like a drop of almost 40 percent. It may have ticked up in the last year, because I haven't looked at it, but it's very concerning.

Senator BEGICH. Do you have—and let me, if I can, kind of move into that arena. And anyone can answer this after I make this question—and that—or ask this question—and that is, Do you think our ability to buy that talent—pay, compete against companies like Oracle—do you think we have that capacity?

Admiral BARNETT. Once again, I can only speak for the FCC. One of the amazing things—it's just like when I was Active Duty in the military—it's amazing to me that Americans are willing to come forward, because of their belief in the country and what we're doing. I'm positive that we'll be able to find those folks, if we can educate them.

Senator BEGICH. Anyone else want to comment on that?

Admiral MCCONNELL. There—I'm familiar with the current talent pool, particularly in this area, particularly around Fort Meade, over in Maryland, and there's just not enough resources. So, my comments about educational bases—we're going to have to do that. If I could offer another, sort of, historical context, what was referred to a moment ago, the NCS—the National Communications System—resulted from the Cuban Missile Crisis. The President couldn't communicate with the Cabinet officer. We had a single carrier—AT&T—so, a—an arrangement was made. We had guaranteed communications for all Cabinet officers, under any circumstances. That held until Judge Greene's famous decision, which broke it up.

At that point—the question was—asked by Senator Pryor, was exactly the key issue: Can the industry members come together and have a discussion out of fear of the antitrust legislation? And they couldn't do that. So, a secondary organization was created, called NSTAC—National Security Telecommunications Advisory Council. But, it's only focused on telecommunications. That served the Nation well for 30 years. It resided in Defense. It now is over in the Department of Homeland Security. But, it's a public sector—U.S. Government—and a private sector, and they collaborate, coordinate for keeping communications working.

What—DHS, who under law has the authority for this mission—defense—has proposed a construct patterned after NCS NSTAC. It's called CPAC—Critical Infrastructure Protection Advisory Council. Three chairs: Secretary of Defense, the DNI, and the Secretary of Homeland Security. Three co-chairs. You pick the largest segments of industry—critical infrastructures—to come together. You have to have public meetings, with government participation, with minutes that are published to the public——

Senator BEGICH. Sure.

Admiral MCCONNELL.—and you talk about the issues, like technology or policy or operations, to address these issues. Now, that has been proposed. My sense, that it hasn't gotten the traction that

it needs. Perhaps that would—may be something that you could consider, in your bill, to put some energy behind it.

Senator BEGICH. Yes, that's a good question.

My time is up, but, Dr. Lewis, I saw you—maybe you could do a quick response.

Dr. LEWIS. Sure. Just—I wanted to come back to the educational point. And it's not a fluke that we have two admirals sitting here, because the Navy's paid a lot of attention to that—to cybersecurity and to cryptology. They're coming up with a scholarship program. There's something called U.S. Cyber Challenge, which CSIS has been a little involved in, and it's an effort to get kids interested in cybersecurity, in hacking contests. It's really good.

There's a chance to rebuild the university programs. And Admiral McConnell mentioned the National Defense Education Act of 1958. And what that did is, we said, "Hey, the Russians are ahead of us. We need a lot of engineers and mathematicians and foreign language specialists." Five years later, we had them. So, yes, you can fix this, with the right sort of investment.

Senator BEGICH. Thank you very much, Dr. Lewis.

I—my time is up, Mr. Chairman. Thank you for the opportunity.

The CHAIRMAN. I've got to stick with that, Admiral.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much.

And do you have to leave, Admiral McConnell? Is that correct?

Admiral MCCONNELL. I do, and I want to offer a last comment. But, I——

The CHAIRMAN. Please.

Admiral MCCONNELL.—a little over time—just offer my last comment.

The CHAIRMAN. Yup.

Admiral MCCONNELL. Something that hasn't been mentioned; I want to make it harder. We've talked about cybercrime and cyberwar, and on and on. I'm thinking about a new idea, and I will call it "Insidia." Insidia means that an adversary builds into our infrastructure. They do what they're doing now, in terms of taking our intellectual capital, and now they harm the infrastructure for competitive advantage, if and when they choose to do so. That is possible today.

So, let's say that a—you pick it—country X is going to introduce a new product, and they want achieve dominance in a market. They could cause things to happen in our infrastructure, that we don't even recognize, that would disadvantage us in a competitive way.

So, it's early in my thinking, but I'll just leave the thought with you. Insidia. Just something I made up, but it could happen today. And the reason I know it could happen today is, I know we could do it, if we chose to do so.

The CHAIRMAN. The great question, "If we chose to do so."

VOICE. We've been investigating that for the last several years, so I can give you background, if you'd like.

The CHAIRMAN. Great.

Senator KLOBUCHAR. You know, just following up on some of the issues raised about the lack of expertise and not enough computer science majors. I'm a former prosecutor, and I always remember how difficult it was when we even had simple computer crimes and the police would show up, we didn't—and they'd press a button, and then all the porn would vanish from the screen, and we'd lose the computer evidence. And that's a really tiny example, compared to what we're dealing with here.

What do you think about the ability—just as you're concerned about computer science degrees—of law enforcement right now? Because I've always said we need to be as sophisticated as the crooks we're trying to pursue, whether it's internationally or whether it's domestically. What do you think needs to be done there? I'm a member of the Judiciary Committee, as well.

Mr. Borg?

Mr. BORG. When we were looking at it, we discovered that actually the law enforcement is getting increasingly sophisticated about handling their evidence, but, they're not very sophisticated about their own vulnerabilities. We looked at the crime labs and discovered that we could, or somebody could, hack into most of the crime labs that we've looked at, alter evidence, if they chose, do all kinds of mischief. So, we've got some huge issues there.

Senator KLOBUCHAR. OK.

Mr. BORG. Think if somebody for hire could tamper with just the chain of evidence for any prosecution that depended on physical evidence. That's the situation we're in right now.

Senator KLOBUCHAR. Right. Well, and part of what I think is just the training, again, and being able to hire people who have that kind of computer forensics experience.

Yesterday, the Federal Trade Commission issued a report that revealed widespread data breaches by companies, schools, and local governments whose employees are engaged in peer-to-peer file sharing. The software was also implicated in a security breach involving the President's helicopter, and other cases. I'm actually working on some legislation along these lines, that we're going to be introducing soon. But, could you talk a little bit about how this could be a national security threat, and what can be done about the human element in all this, about employees even inadvertently sharing confidential files?

You want to talk about peer-to-peer?

Dr. LEWIS. Well, you know, we're coming to a—sort of a—we're at the early days of, I think, new thinking about cybersecurity, and that's where the work of this committee's been really valuable.

I talk to a lot of companies. What they've—what I've learned is that some of them have fabulous best practices, right? Now, usually they've been companies that have already been hit, right? So, I talk to a giant oil company, they had a—they were hacked, and lost millions of dollars, and now they do everything right. One of the things they do is, they severely limit the ability of employees to use this kind of software.

We can think of many examples. It's fun, if you think about some of them, you can type in "tax return" and it will, for systems that are not set up, show you people's tax returns. But, we now are be-

ginning to identify practices that work in improving network security, and this is one of them.

So, the question is, How do we populate industry with those best practices? How do we tell them what they are? How do we get them all to do the right thing, when it comes to file sharing?

Senator KLOBUCHAR. Very good.

On February 16, the Bipartisan Policy Center sponsored the Cyber ShockWave exercise, which brought together former high-ranking national security officials to evaluate how they acted when there was a realtime cybersecurity emergency. And one of the problems the simulation exposed was the lack of clarity regarding government authority to regulate private-sector-controlled infrastructure systems, such as telecommunication networks and the electrical power grid, during such an emergency. Do you have any views on what steps should be taken to clarify the ability of government to assume temporary control of infrastructure during a cybercrisis?

Dr. LEWIS. Well, I think, I'm—I don't want to talk too much; I'll let somebody else jump in, too, but—there's a provision in the bill that I think could be very helpful. And one of the things that we need to think about is, In an emergency, do we want the President to have the things he needs to do to protect the American people? And I'm not sure the scenario got it right. I'm not sure that the President wouldn't scrounge around—they have some very smart lawyers over there—and maybe under the International Economic Powers Act or—pardon me—International Economic Emergency Powers Act, or some other act, we could come up with a solution. But, I think the ability to intervene in a crisis is essential, and giving the President that authority clearly is going to be essential for national defense in what's become a new kind of warfare.

So, in that sense, the provision in the bill, which I understand has gone through many changes, really could be quite helpful in making the Nation more secure.

Senator KLOBUCHAR. Mr. Borg, in your testimony, you stated that cyber attacks have already done damage to the American economy, much more than is generally recognized, due to massive thefts of business information. Could you talk about some of the examples of what you most see with business information thefts, and what was, or not, done by individual corporations, what you think they could do better?

Mr. BORG. It's very tricky to talk about this, because we've been warned by lawyers that if we even hint about an actual example, we will be sued by everybody involved—the company——

The CHAIRMAN. Could you say that again?

Mr. BORG. Is that—what?

The CHAIRMAN. Could you say that again?

Mr. BORG. We've been warned by lawyers that if we even hint at a real example, so that somebody could begin to identify it, we will be sued by everybody involved, because the business leaders who let this happen will face shareholder lawsuits, they will—their companies will feel obligated to sue the beneficiaries, who will countersue, claiming libel, and so on. So, the whole thing is, legally, a mess. As a consequence, nobody wants to talk about this. This is huge.

Senator KLOBUCHAR. Right.

Mr. BORG. This is just gigantic.

Senator KLOBUCHAR. Well, but there's—sometimes there are publicly known examples that maybe you could——

Mr. BORG. There aren't for this one.

Senator KLOBUCHAR. OK.

Mr. BORG. We do have companies that had very, very extensive intrusions that coincided with similar facilities being built in Southeast Asia. The facilities in Southeast Asia are ones that nobody is allowed to visit—we think, because they would suspiciously like the facilities here that they are replicating. They were, when they opened, able to function very efficiently, offer very low prices, with no particular strain on the corporation that was running them. So, we think whole factories are being replicated in other parts of the world.

Senator KLOBUCHAR. Wow.

Mr. BORG. The economic consequence is that whole industries are potentially going to be stolen over time. It happens gradually. It's being slowed down by certain obstacles right now, the chief one of which is, there aren't enough people in some of the countries and areas of the world that are receiving this information to sort it all out; there isn't enough expertise in American ways of doing business to utilize all the information they've got. But, potentially, we're looking at the viability of entire industries being undermined over time. And the thing is just going abroad.

Senator KLOBUCHAR. And so, if they had the appropriate people, they would just be able to basically replicate a company, is what you're saying?

Mr. BORG. Yes, that's right. Except without the expenses of having to do the R&D, to go through the learning curve, to do all the other things. You can open a facility, and, on the day you open, have a level of efficiency that it took the American market leaders 6 years to get to.

Senator KLOBUCHAR. Anyone else?

Dr. LEWIS. Let me give you a real quick example. I don't care if anybody sues me, but—I heard an example I thought was astounding. It was about a small furniture company, right? A couple hundred employees, you know, not a big revenue—they make wooden furniture. They got hacked, and somebody stole all the designs for the wooden furniture. Now, you all know that there are countries in the world that are good at making low-cost furniture, right? And now they have the designs, the intellectual property. They have the newest styles, and they can get it on the market faster—as Scott said, on the market faster, at a lower price. That American company has really been hurt, right? And that's what we're looking at.

But, the notion, to me, that it's worth this—how pervasive is this, if you're going to be hacking small furniture companies that make wooden furniture? It's amazing. We don't realize what's happening to our country.

Senator KLOBUCHAR. OK.

Mr. BORG. Something else here that's very important, that's not understood, is that all of the information for all the pressures, temperatures, switches for an entire factory, and all the schematic diagrams, can be stolen. We're not talking about stealing the formula

for Coca-Cola. We're talking about sucking all of the information out of a company.

Senator KLOBUCHAR. Well, thank you very much. It sounds like we have a lot of work to do here.

The CHAIRMAN. Kind of, yes.

Senator Thune.

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you, Mr. Chairman. And I want to thank you and the Ranking Member for holding today's hearing on a very important and oftentimes overlooked subject, cybersecurity, which, as we've heard, has great consequence for our security and our economy. And I think we have to remember that we're under constant attack. Our critical infrastructure and the Internet backbone of our economy remain extremely vulnerable to these cyber attacks. And there was a recent GAO report that states that cyber attacks could cost our economy $100 billion annually in the near future. And so, I think it's important that this committee give the appropriate, sufficient attention to this important subject.

I know some—the questions have been posed—Senator Klobuchar and I are working on the peer-to-peer issue, and some legislation with regard to that. But, I—what I'd like to do is just ask a couple of questions to the panel and whoever would like to respond to these.

The Wall Street Journal recently reported that hackers in Europe and China hacked into computers in over 2,500 companies and government agencies. And what's probably even more shocking is that they infiltrated these systems for several months before they were being detected. How do we improve the identification of these attacks, to stop the activity before they do additional damage?

Mr. BORG. One of the problems is that we focus so exclusively on perimeter defense that once somebody has penetrated the system, we don't have adequate devices to spot what's going on. One of the things that we urgently need to develop is industry-specific, sometimes even business-specific, monitoring capabilities that will set off alarms when these systems are being misused and when information is being improperly moved about.

Dr. LEWIS. You know, the *Journal* article was interesting. I think it's the third or fourth time I've heard of something like this—massive penetrations; hundreds, if not thousands of companies. It's an ongoing program. It's a nice program, because you're not going to get caught. And even if you do get caught, there are no consequences.

So, one of the things we want to think about is, When we see people committing a crime, what are the consequences? And right now, if there's zero consequence, there's almost zero risk.

I've talked to a few of the big financial companies and said, "Do you have trouble telling who is doing bad things to you?" And what they usually say is, "No." They can follow the money, they see where it goes, they know who's doing it to them. But, right now, we don't have any way to go to these other countries and say, "Hey, some of your citizens are committing crimes in our country. Would you do something about it?" And so, whether this is something for

the World Trade Organization, whether it's for the World Intellectual Property Organization, whether it's for INTERPOL, we need to start going after people who do these things. And right now, they've gotten a free ride.

Senator THUNE. I'm just trying to think about what our role is, in terms of a worldwide problem. And if you don't have the capability of enforcing or imposing some sort of penalty or punishment on people who do this, you're right, there's no consequence to it. I don't know what would keep them from continuing to do it.

The question I have, dealing with the first response, which said coming up with some industry-specific or even company-specific mechanisms of dealing with that, Do you see some role for the Congress in that process? I mean, it seems to me that the companies that are impacted by this are, maybe, better positioned to do that.

Mr. BORG. When I've talked about the need for this kind of tool, this kind of software, to people in the security industry, they have regularly said, "Oh, yes, we're really eager to jump into that market as soon as it's pioneered. We don't want to be the first mover, we want to be ready to—once the market is formed." So, there's a huge opportunity here for the government to seed that market, to be a guaranteed customer, to, in some cases, be an initial supplier, providing some prototype tools. And then, I think, once that is set up, the security industry will be ready to move into it. But, it's another example of a market that's not working properly, that could be fixed by government intervention.

Ms. DAVIDSON. If I can echo that—and I'm sorry Admiral McConnell is no longer here, because he was using the railroad industry as an example. There is a role for the government in promoting the use of standards. And why do we care about that in this context? Part of what would make it easier for people to not only have better situational awareness, but to be able to connect these types of dots, is having standards around what type of records or censor records you need to keep in a system, and the way in which that is expressed. And the reason for that—why do the railroads tie into that? Because, a long time ago, the railroads didn't have a standard train gauge. And the reason it's—I think, 4 feet, 8-and-a-half inches, is because the government stepped in and said, "We want to build a transcontinental railroad—that's a public good—and we're going to tell you what the train gauge is going to be, so we can put the pieces together, and you can get on a plane on the East Coast and go all the way across the West Coast." The government could actually promote the use of standards around audit records in such a way that would be not only how the—the nerdy bits and bytes of how they're described, but also what kind of record you have to keep. And by doing that, and promoting it through procurement, you could effectively tell your suppliers, "We're going to change—we're going to tell you what kind of train you're going to build and what the train gauge is going to be."

NIST is very good at getting industry to participate in that, and that could actually help make—create the infrastructure of security which can help secure critical cyberinfrastructure.

Senator THUNE. And there are multiple government agencies that deal with, and have some role in preventing, cyber attacks. You've got Defense, Homeland Security, Commerce, FCC, FBI. And

this was actually going to be a question more for Admiral McConnell, but I'm interested in knowing, from your observation, how the coordination—level of coordination is between those various agencies, and is there anything that this committee could do to ensure that they're working in a more efficient and coordinated manner to prevent cyber attacks?

Admiral BARNETT. Senator, from the FCC's perspective, we—Chairman Genachowski is focused on making sure that we have good communications with our Federal partners. And that's not just for cybersecurity, but emergency management and other responsibilities that we have. So, there's certainly a focus on this. I mean, I think there's a desire to make sure that we do the best. And for that, there's a lot of communication, I would say, with regard to the exercises that you're seeing. I can't say that there may need to be some more, and I can't speak to all agencies, but there certainly is communication going on about the threat.

Dr. LEWIS. You know, we want to recognize that progress has been made in the last year, or even a bit longer. So, there is more cooperation than there used to be, and more coordination. And hopefully the appointment of a new cybercoordinator at the White House will help that.

But, you're all familiar with what happened on December 25th in Detroit. And that was a—in some ways, a problem with coordination among Federal agencies. Again, on the counterterrorism side, we're much better off than we were 9 years ago. But, you can still see problems, and I'd say, in cyberspace, the coordination is not as good as it is in the intelligence community and the counterterrorism community.

So, good progress, but still a long ways to go. And that's where congressional attention, measures like this bill, can help encourage the Federal Government to move in the right direction.

The CHAIRMAN. Thank you, Senator Thune.

Senator Snowe.

Senator SNOWE. Thank you, Mr. Chairman.

Dr. Lewis, I wanted to ask you about the cybercoordinator position and the appointment of Howard Schmidt, as you mentioned, being a coordinator, rather than a Senate-confirmed position. And, for example, he is not able to testify before this committee on this issue. So, how important is it to have a Senate-confirmed position on this question?

Dr. LEWIS. Well, I think, in the long run—and hopefully the long run won't be more than a few years—we're going to need something like USTR, right? Or maybe some of the other agencies that exist. We're going to need a specific agency that will be appropriately staffed and have the right authorities to do this. And that position, just as the USTR positions are confirmable, would make sense. So, I think, good first step there, appointing a coordinator. We're on the right path, but we've got a long ways to go.

Senator SNOWE. Yes.

Dr. LEWIS. And, you know, when you think about it, this is a new infrastructure—you've heard that from everyone—that we depend on. But, we haven't adjusted the government to that. And moving toward that Senate-confirmable position would probably be a good idea.

Senator SNOWE. Does anybody else have an opinion on that question?

Ms. DAVIDSON. Well, I can't comment on the structure, but I can certainly comment on the individual. I think Howard Schmidt is probably the very best possible person who could have been chosen for that position, who commands tremendous respect in industry, and his sole agenda is to make things better. And because of his—because of who he is, there will—people who will line up to do things for him because it's Howard asking. I think it was an outstanding appointment. You just could not have had found anybody better. It will be a very difficult job, but if anyone is up to it, it is—he is absolutely the right person for that.

Senator SNOWE. Well, I just think it's—given everything that we've discussed here today and, obviously, the significance of this issue and the fact that, as the President described, it's a strategic national asset, I think it should be elevated so we have that conversation, and that—more importantly, that he reports directly to the President of the United States. I mean, I think that that sends a very critical message, frankly. And that relationship should be developed at the outset, as we're beginning this process and, hopefully, getting legislation in place. That's going to be absolutely critical in that regard; otherwise, we're not going to have the benefit, other than in private meetings, to have those kind of discussions, when, in fact, they should be part of the public arena.

I would just like to ask you, Are you familiar with the NetWitness report, by any chance? And how would you characterize the extent of that attack?

Dr. LEWIS. Interesting company. The fellow who runs it is a guy named Amit Yoran. Like Howard, he has tremendous respect, long experience. And so, it's good that they came out with this.

Interesting report, but, for me, it wasn't a big surprise. I mean, this is sort of the normal business, here. How many times have we seen this in the past: "Somewhere in Eurasia, there's a group of hackers, and they've penetrated hundreds or thousands of American companies." You know, it's just—this one wasn't particularly sophisticated.

One of the things to bear in mind is that we have more sophisticated opponents than the fellows we stumbled across here. The NetWitness report just helps reinforce the kind of pressure we're facing.

Senator SNOWE. Dr. Borg?

Mr. BORG. There were a couple of things about it that were a little bit interesting. One is just the scale of it, and the other is that it used two botnets in conjunction. Each time we have one of these, they're a little more sophisticated, they have another little new twist, something here or there. So, it's a sign of an ongoing process of attackers just getting better and better, more talented.

Senator SNOWE. Getting increasingly sophisticated? Yes. And how do we keep pace with that sophistication?

Mr. BORG. Well, one of the ways we're not keeping pace is by having departments of cybersecurity where, in the graduate programs, there are no Americans. A lot of our leading programs literally have no American students at the Ph.D. level, or sometimes

even the master's level. We're training a lot of the world in cybersecurity better than we are our own people.

Senator SNOWE. What accounts for that? Is there any reason for that, or does it just happen to be the way it is?

Mr. BORG. If you're Indian——

Senator SNOWE. By——

Mr. BORG.—or Chinese——

Senator SNOWE. Yes.

Mr. BORG.—or from some other part of the world, there is greater motivation and a bigger gain from getting a degree in cybersecurity than if you're American.

Ms. DAVIDSON. Well, and to that point, a lot of the—you know, how do we keep up with it? I actually have a team of hackers who work for me. They're ethical hackers; their job is to break our software before someone else does. They are also the ones who author our coding standards: How do you write secure code? And those are in a constant state of revision, not only for new things that are publicly known, but new, nefarious ways they find to break our software. And we train all our developers on that. So, it is constant revision, because there is always something else malicious coming down the pike.

Admiral BARNETT. Senator, of course, I have a son who's in computer security, so I'm not going to complain about the American education system; I think we do have the ability to train the people we need. But, there needs to be an emphasis on—it has been a concern of mine—I mentioned the precipitous drop in the number of computer science degrees that we are producing. I might mention the number of women that we are producing, and that has dropped even further. There's a good deal of research of the reasons for that. We need to attack those directly and reemphasize getting American kids ready to go into computer science programs—so, we have to start earlier than college—and then making sure that they're incentivized to do that, and attack all the various reasons, some of which are cultural—there are various reasons, too, that we can provide to you.

Senator SNOWE. Well, that's interesting. And that's something that is part of our legislation that we're focusing on, on the training and the certification of cybersecurity personnel. But, that's clearly an emphasis that we have to make.

So, then would it be very difficult for the Department of Homeland Security to, you know, hire up to 1,000 cybersecurity personnel over the next 3 years? Is that ambitious, or is that doable?

Dr. LEWIS. It's probably doable. They came in with only about a third of their positions filled. They had 1,000 slots, and I think they had about 300 filled. And in the intervening year, I think they've moved that up to about 50 or 60 percent; they've done a good job.

There's three problems. First, the shortfall of trained personnel means DHS is competing with NSA and with DOD, with FBI. And, let's face it, it might be more fun to work at NSA or DOD than DHS, right? So, they've got a competition problem.

Second, a lot of the hiring processes that we have in the Federal Government don't help. And so, somebody gets hired by DHS, and then they're told—and this happens at other agencies, too—"We've

hired you, and in another 6 to 8 months we'll be able to actually bring you on board." And, of course, people can't wait 6 to 8 months for a job. So, a lot of people leave early.

Finally, there's this—again, this shortfall problem, which is that somebody comes to DHS, they get good training, they get some good experience, they get a clearance, and they're suddenly a lot more attractive to the private sector. So, you've got an outflow problem, too. And all these things are not impossible to beat; we've beat them in other agencies. But, while there has been really good work done at DHS, I think they could use some help on the recruitment side.

Senator SNOWE. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Snowe.

Let me kind of close up here by saying, you've been a fabulous panel, all of you. And you, too, Admiral McConnell, wherever you are. I mean, you really know your stuff. You speak with the kind of cold clarity which this subject deserves. Senator Snowe and I are very happy that we've introduced our bill. And when listening to you, you know, you just ask, Is it—was it done in time? Can it make a difference? And the answer has to be yes.

And let me say the things that worry me. One is the whole question of starting kids out. Right now, there's this enormous—which was brought on point—emphasis on STEM—Science, Technology, Engineering, and Mathematics. We desperately need that. Is there a way that—and the kids are so good—my son was—two nights ago he called up, and he's really, really good on computers, and he was doing—he was at war with a hacker, trying to fight back, and, you know, very, very sophisticated stuff. He's 30, so that makes it a little easier. But, the—trying to integrate this somehow—we don't have that choice, do we?—into early education. We do not have that choice. And if boards of education say they don't have that money, we still do not have that choice.

The second thing is that the problem is so pervasive, so overwhelming. We're talking about the public sector and the private sector and all the—your 6- to 8-month vetting, you know, the horrors of the Federal Government and its vetting process, and people just say, "You know, I can't wait." So, you lose good people. The salaries involved. The budget restrictions we're now going through for the next number of years, because of our deficits. And yet, you know, put it in comparison to the dangers of these massive cyber attacks, which are not, you know, unlike another terrorist attack, something of the future, you know, next week, next month, next year; they're all day, every day, as I quoted at the beginning, from a DOD person. I mean, it's just happening all the time, sucking the blood. I think, forensically, it takes 4 minutes to drain the blood out of a person, and, you know, that's not a particularly attractive analysis, but it's a cogent one, that this is a really serious, desperate problem and that bills at any—you know, any kind of effort is going to be important, and we have to, all of us, decide how to do this.

You know, we talk about the Federal Government and the stovepipes that Olympia Snowe and I have dealt with on the Intelligence Committee, and the intelligence community has gotten a lot

better since we had a DNI, but they are by no means cured. People tend to hold on to their territory, and they don't give it up easily. And I—that has to be true in the corporate world, for some, you know, very clear and understandable reasons.

So, how do we make it all work? How do we get people to together? How do we create the sense of urgency, at a broader lever, in which we do things we've just never done before as a country? Which I think is what it amounts to. Yes, we've got to give the President the right to intervene. And that's controversial. That's all—that'll always be controversial. But, Senator Snowe and I believe that needs to be done.

But, let me leave you with one happy thought, just for practice. Last year and this year and the year before, on the two sides, let's say, of American young people looking for careers, one is in the intelligence—the world of intelligence—the CIA, NSA, et cetera—the applications for those agencies, in number and in quality, have never been higher. So, they're swamping these agencies with applications to work there. And incredible—and I've done this, and I'm sure that Senator Snowe has, too—you go and meet some of these young people working for CIA or whatever—they're fantastic. And so, that's national security.

On the other end is the Peace Corps or Teach for America. But, just take the Peace Corps for a moment. They have never had so many applications, ever, and of such high quality.

So, to say, on the one hand, that we don't have enough Americans doing this, that people from other countries—they used to get their degrees and stay here, because it was more profitable. Now, they're being called home, and they're patriotic, and they're doing—I mean, I can't criticize them for what they're doing. It's just that it makes our life more difficult.

So, I think that, with the depth and desperation of the problem, mixed with this sort of hopeful and positive attitude to be engaged in serious matters, cerebral matters, of young people in this country, we've got to find our way out of this. And we won't do it quickly, but we sure have to do it.

So, thank you very, very much, all of you.

The hearing is adjourned.

[Whereupon, at 4:35 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. TOM UDALL, U.S. SENATOR FROM NEW MEXICO

Thank you, Chairman Rockefeller, for again focusing this committee's attention on cyber security.

Since this committee met last year to discuss this topic, we have witnessed a number of alarming cyber attacks and data breaches.

In December, Google announced that they—and probably many other American companies—had been infiltrated by cyber attacks that originated in China. Apparently the hackers specifically targeted Chinese activists who used Google services. However, many other users and companies could be harmed by this type of cyber attack.

In January, we learned that the National Archives apparently lost a hard drive that had over 100,000 Social Security numbers for workers and visitors to the White House.

This month, a cyber war game exercise also illustrated some of the Nation's vulnerabilities to a sophisticated cyber attack and the need for a nimble and coordinated response to protect our infrastructure.

So, I welcome the opportunity to ask a few questions today about how we can do more to protect consumers, companies, and the Nation.

WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO VICE ADMIRAL MICHAEL MCCONNELL

Question 1. What are the key elements of public-private teamwork that are not in place today that should be?

The witness did not respond.

Question 2. Would it make a difference if more senior executives in the private sector were granted security clearances?

The witness did not respond.

Question 3. What about cybersecurity? Are you confident that the everyday American citizen knows the threat that we are under, and knows how to make his or her own home or business safe?

The witness did not respond.

Question 4. Should there be basic cyber awareness and education as part of the normal curriculum in elementary and secondary school?

The witness did not respond.

Question 5. What can the government and private sector do together to solve this labor shortage problem?

The witness did not respond.

Question 6. What can we do to inspire young students to aspire to serve their country by being a cybersecurity professional?

The witness did not respond.

Question 7. What must the government do better? What must the private sector do better? What responsibilities do both have to the public at large?

The witness did not respond.

WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO VICE ADMIRAL MCCONNELL

Question 1. Admiral McConnell, your statement sounds the alarm about threats to our infrastructure. You note that the United States is not doing enough to promote cybersecurity and that the country needs a coordinated approach involving the public and private sectors. Our national labs—which are the crown jewels of our Nation's research system—are active in efforts to promote cyber security. In my home

state of New Mexico, Sandia National Laboratories is engaged in efforts to secure the national electrical grid from cyber attack. Los Alamos National Laboratories is a leader in quantum cryptography. What role should our National Labs have in the efforts you describe to protect our Nation from cyber attack?

The witness did not respond.

Question 2. Some experts say the arrival of "Cloud computing" could be as important and as disruptive as the advent of the World Wide Web. Eric Schmidt, the CEO of Google, has written that, "We're moving into the era of 'cloud' computing, with information and applications hosted in the diffuse atmosphere of cyberspace rather than on specific processors and silicon racks. The network will truly be the computer." How can we be sure to realize the benefits of cloud computing given very real cyber security threats?

The witness did not respond.

Question 3. What is the role of government and private industry in protecting sensitive data as it increasingly moves from desktop devices to the "cloud"?

The witness did not respond.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO DR. JAMES A. LEWIS

Question 1. What are the key elements of public-private teamwork that are not in place today that should be?

Answer. The most effective partnership models are based on small permanent groups of senior business leaders from the corporate headquarters who regularly interact with senior government officials. Only two or three groups (DOD's ESF, DHS's CIPAC and perhaps NSTAC) now follow this model. The key elements are trust and authority—trust comes from regular meetings among the same people and authority comes from the ability to make binding decisions. Many existing groups are not designed to provide trust or authority.

Question 2. Would it make a difference if more senior executives in the private sector were granted security clearances?

Answer. Classified briefings on the nature and extent of the threat are very effective in alerting corporate CEO's to the problem they face. Classified briefings have been one of the most effective parts of the DOD's Defense Intelligence Bases initiative.

Question 3. What about cybersecurity? Are you confident that the everyday American citizen knows the threat that we are under, and knows how to make his or her own home or business safe?

Answer. I do not believe we should make citizens responsible for the national defense. There are some minimal activities (keeping anti-virus software updated) that citizens now need to perform but we would be better served by shifting security to service providers. Nobody has to program their land-line phone or install anti-virus software on it. The same model should apply to the Internet.

Question 4. Should there be basic cyber awareness and education as part of the normal curriculum in elementary and secondary school?

Answer. Wouldn't hurt, although we shouldn't expect too much from it.

Question 5. How can the Federal Government bolster market-based private sector incentives to drive innovation in cybersecurity and raise the bar on cybersecurity standards and best practices?

Answer. The same way it drove innovation in automobile safety: by setting goals and requirements and then letting the companies figure out how to implement them.

Question 6. Does the American public have the right to expect that U.S. private sector critical infrastructure companies are looking out for the safety and security of the American people? Should this interest in public safety an integral aspect of the private market for IT products and services?

Answer. In most other areas of public safety we expect critical infrastructure companies to meet minimal standards. It is time to extend this to cybersecurity. In many cases, regulatory authorities also allow companies to impose a small surcharge to cover the additional cost of safety measures. This too must become part of a national effort to secure networks.

Question 7. What must the government do better? What must the private sector do better? What responsibilities do both have to the public at large? With this in mind, how can we fashion a public-private partnership, based on trust, that allows

for sharing of confidential and/or classified threat and vulnerability information between the government and critical private sector networks?

Answer. National security is the responsibility of the government. We should not assign this function to citizens or companies if we wish to succeed. Government needs to be better organized and have a clear strategy for defense. The best analogy might be to city policing: yes, we want people to lock their cars and doors to buildings, and exercise a little common sense, but at the end of the day it is the responsibility of the city authorities to bring crime rates down. Our current approach to cyber security is like the crime fighting approach in New York City in the 1970s. We need to change that.

Question 8. Would government and private cybersecurity efforts benefit from "vulnerability mapping" of major U.S. networks, public and private?

Answer. Only if the mapping was then tied to some action to either improve defenses or increase resiliency.

Question 9. What are the specific risks to such an activity?

Answer. Since our major opponents have probably already done this, any additional risk is likely to be small.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO DR. JAMES A. LEWIS

Question 1. The recent Bipartisan Policy Center cyber war game exercise examined a potential attack that first affected wireless cell phones. As computing and networking technology become integral to all manner of consumer goods, it seems that new cyber attack vulnerabilities will only proliferate. In today's business landscape, supply chains stretch across the globe and companies often acquire other firms to gain access to new software and technologies for their products. This makes it more difficult to know whether a product may contain cybersecurity vulnerabilities from a single component or piece of software code from an outside supplier or other firm. How is security of the final assembled product affected in an environment in which new links are so frequently added to the product's "chain"?

Answer. Most companies have processes in place for quality control that provides some level of protection. A skilled adversary could bypass these, but it would be expensive to do so. The larger problem is that as manufacturing and invention shift form the U.S. to Asia, our vulnerability to supply chain corruption may grow.

Question 2. How are leading technology companies bringing the security of acquired products in line with their own standards for cybersecurity?

Answer. The most advanced companies buy from trusted suppliers, engage in testing, and rely on their network defenses to identify anomalies (such as effort to exfiltrate large amounts of data) after a new device or program is installed.

Question 3. What is the role of Chief Security Officers or Chief Technology Officers in assuring best security practices are implemented in such cases?

Answer. It varies from company to company. The best practice is for both CSO and CTO to work together to build secure networks.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN ENSIGN TO DR. JAMES A. LEWIS

Question 1. Are there any legal restrictions we should focus on that make it more difficult for industry and government agencies to share the information needed to protect our critical cyber infrastructure? Are there any barriers that Congress needs to eliminate, or any legal flexibility we can provide to foster the necessary sharing while still protecting sensitive or proprietary information?

Answer. The main problems are the need to have personnel with security clearance to receive some information and the perception that the government does not share fully. It may be possible to streamline the clearance process for lower classification levels (Secret, for example).

Question 2. What mechanisms are in place for private companies to report cyber intrusions (either originating domestically or overseas) to the Federal Government?

Answer. Different parts of the Federal Government receive reports of cyber intrusions. DHS, FBI, Secret Service and, in some instance DOD, all get reporting from companies, but the information is not always available to other agencies.

Question 3. What is being done to encourage private companies, particularly those with government contracts, to report cyber intrusions (either originating domestically or overseas)?

Answer. DHS, FBI, Secret Service and DOD have outreach programs, such as FBI's Infragard program

Question 4. Do government contractors have an ethical or statutory obligation to report cyber intrusions (either originating domestically or overseas)?

Answer. DOD has begun to require reporting from companies in the Defense industrial base and in some instances companies have reported breaches in their SEC filings, but there is no consistent requirement.

Question 5. Do government contractors with classified information on their servers and individuals with security clearances on their payrolls have a statutory or ethical obligation to report cyber intrusions (either originating domestically or overseas)?

Answer. This requirement may be part of their contract of part of DOD acquisitions regulations—the DFAR.

Question 6. When Request For Proposals (RFPs) are put out for contracts that involve sensitive or classified information do all of these RFPs require that bids include the number of successful and unsuccessful cyber intrusions committed by domestic or foreign entities (either originating domestically or overseas)?

Answer. I do not know of any specific requirement.

Question 7. In your opinion, if a private company believes that it has been the victim of a cyber intrusion (both originating domestically or overseas), which is the appropriate agency that it should report this intrusion to?

Answer. The FBI.

Question 8. In your opinion, if a government contractor believes that it has been the victim of a cyber intrusion (both origination domestically or overseas), which is the appropriate agency that it should report this intrusion to?

Answer. The FBI and the contracting agency.

Question 9. In your opinion, if a government contractor that is working on a sensitive or classified project and believes that it has been a victim of a cyber intrusion (both origination domestically or overseas), which is the appropriate agency that it should report this intrusion to?

Answer. The FBI and the contracting agency.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO SCOTT BORG

Question 1. What are the key elements of public-private teamwork that are not in place today that should be?

Answer. The public and private sectors should be discussing how to engender the sort of market environment that will allow the creative potential of American corporations to be turned loose on our collective cyber-security problems. This hasn't happened yet.

Instead, our ability to tackle the challenges of cyber security is being severely limited by established interests and obsolete ways of thinking. Even the threat of government regulation and the promise of big profits from government contracts or subsidies are not solutions, but serious impediments to real cooperation. Both get corporations thinking in terms of lobbyists and public relations, rather than problem solving.

Question 2. Would it make a difference if more senior executives in the private sector were granted security clearances?

Answer. Giving more senior executives security clearances would be of little help. The population that needs to be reached is much larger than the group to whom it would be practical to grant clearances. What is needed, instead, is a set of better incentives for declassifying information and an improved system for circulating it, while respecting its sensitivity.

In general, the whole system of government security clearances is ill-suited to protecting the sort of private-sector-based information relevant to cyber defense. It has been a serious impediment to communication, yet does not offer sufficient security.

It is important to understand that the most sensitive and dangerous information regarding the possibilities of cyber attacks on critical infrastructures is not possessed by the government. It is generated and owned by private sector corporations. Much of this information is far too sensitive to be entrusted to everyone with a given level of security clearance. This information is seldom shared with the government, in part, because there is a widespread belief that the government can't be trusted with it.

Question 3. What about cybersecurity? Are you confident that the everyday American citizen knows the threat that we are under, and knows how to make his or her own home or business safe?

Answer. It is obvious to virtually all cyber-security experts that most Americans have no idea of the threat we are under and little idea of how to make their home and business computers safe.

Question 4. Should there be basic cyber awareness and education as part of the normal curriculum in elementary and secondary school?

Answer. Yes, cyber-security education is essential, but it should not be used as an excuse for failing to create more secure information products and services. When systems are badly designed, there is a great temptation to blame the users. But systems that make great demands on users are simply badly designed systems. In addition to education, it is urgently important to address the question of why information systems are so badly designed from a security standpoint.

Question 5. How can the Federal Government bolster market-based private sector incentives to drive innovation in cybersecurity and raise the bar on cybersecurity standards and best practices?

Answer. I have offered a list of six basic reasons why markets are not delivering the needed levels of cyber security: (1) Companies are not being charged for the increased risks they cause or paid for the risks they reduce; (2) Individual executives are not being motivated to act in the long term interests of their companies where cyber security is concerned; (3) People don't have adequate information to take account of cyber security in their market choices; (4) Markets for many urgently needed cyber-security products and services haven't been created yet; (5) Switching costs are too great to allow companies to shift readily to more secure choices; and (6) Entry barriers have kept out alternative products and services that would be better from a security standpoint.

For each of these six market problems, there are several market remedies that should be considered. One of the possibilities, for example, for remedying the lack of information needed for market choices is a government-facilitated system for rating the cyber security of software products. If people don't have any reliable information on which software products are safer, they can't choose the safer products. Putting rating labels on software, the way we put already rating labels on everything from cars to cookies, would make it possible for the markets to deliver safer software.

Talk of "raising the bar" and "bolstering incentives" misses the point. The markets that determine cyber security are broken and need to be fixed. Government mandates and subsidies won't do the job. The government measures that are needed are actually less heavy-handed and less expensive, but they need to affect the mechanisms that allow markets to function.

Question 6. Does the American public have the right to expect that U.S. private sector critical infrastructure companies are looking out for the safety and security of the American people? Should this interest in public safety an integral aspect of the private market for IT products and services?

Answer. The American public should be able to assume that its interests are being safeguarded, especially where monopolies like electric power are concerned. But government intervention in these areas needs to handled very carefully, because the technology is changing so rapidly. If the government tries to dictate security measures to the critical infrastructure industries, these measures will probably be out of date and counter-productive before they are finished being officially formulated.

Question 7. What must the government do better? What must the private sector do better? What responsibilities do both have to the public at large?

Answer. The government needs to get over the idea that its choices are to throw out the market and dictate what should be done or, alternatively, to do nothing and hope some market will somehow solve things. Instead, the government needs to understand that properly functioning markets need attention and engagement.

For its part, the private sector needs to recognize that properly functioning markets provide better opportunities to make money for any companies that are delivering real value. They should work with the government to make these markets happen.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO MARY ANN DAVIDSON

Question 1. What are the key elements of public-private teamwork that are not in place today that should be?

Answer. The information flow still seems to be one way. With the exception of the UK government (through CPNI, a part of MI5), industry almost never hears of threats the government—or some in the government—know about. In some cases, there may be legal restrictions that prevent this information sharing. It is (obviously) not the case that everyone should know everything, but if there is a material threat that affects national security—where that definition also includes economic security—then I think that some of that information should be shared more broadly.

Question 2. Would it make a difference if more senior executives in the private sector were granted security clearances?

Answer. Generally, yes. I still think there is a general lack of awareness among some executives about the extent to which critical systems are vulnerable and the degree to which their data—including intellectual property—is vulnerable. This affects not only national security in the traditional sense but also our national economic security.

Question 3. What about cybersecurity? Are you confident that the everyday American citizen knows the threat that we are under, and knows how to make his or her own home or business safe?

Answer. Absolutely not; that is, I have no confidence that the average person knows how severe of the risks are and what they can do to protect themselves. I am a security professional, yet I still learn new things every day about how technology can be broken, corrupted or used by bad guys against us.

Question 4. Should there be basic cyber awareness and education as part of the normal curriculum in elementary and secondary school?

Answer. It may sound strange to say Yes, but I am old enough to remember the cold war, and how elementary school children would do "duck and cover" drills in schools. We accepted that at the time, because we lived under the threat of a nuclear war. We now live in a world in which there are new threats and—especially given the degree to which schools seem hell bent on using computers at an early age as "educational tools"—they need to emphasize both "responsible use" and "safe use" of those tools.

Question 5. How can the Federal Government bolster market-based private sector incentives to drive innovation in cybersecurity and raise the bar on cybersecurity standards and best practices?

Answer. I do not think innovation is the problem—there are lots of security startups and more all the time. (Of course, there are other disincentives in the sense that Sarbanes-Oxley, for all that it was well intended, has resulted in the curtailment of the market for initial public offerings (IPOS) in the U.S. The "compliance overhead" for becoming a public company is so high and so expensive that a lot of companies will not IPO anymore—their only exit strategy for investors is to be acquired. This was a (clearly) unintended consequence of the legislation but it has nonetheless curtailed innovation.)

I note that there are ways to bolster innovation by helping small innovative security startups tap into the larger market that the Federal Government represents, such as the IT Security Entrepreneur's Forum which is sponsored, in part, by the Defense Department and the Department of Homeland Security. (See *http://www.security-innovation.org/*).

As far as raising the bar on standards and best practices, I have been an advocate for a long time of using procurement power to do that. And the procurement power need not only be the Federal Government but could include other sectors. For example, the multi-state information sharing and analysis center (MS–ISAC) has come up with common procurement language on software development practice. Is it binding on the states? No. Is it a common resource that they can use to contractually "signal" their suppliers that they need to provide better security? Yes.

A no-brainer as far as I am concerned is that any piece of software sold to the government should: (a) provide a secure configuration guide (attorneys frown on the term "best practice"), (b) enable the product to be installed in that configuration (make it easy and cheap for customers to be "secure out of the gate") and (c) either provide a tool to maintain the configuration *or* support a standard (such as those provided via the Security Content Automation Protocol) that enables the configuration to be monitored automatically and re-configured automatically.

The Air Force realized that something like 80 percent of their security vulnerabilities were a result of weak/poor configuration practice. If vendors can do

something *once* that helps secure all their customers, at a lower lifecycle cost, they ought to do it. Procurement can force them to do it.

Question 6. Does the American public have the right to expect that U.S. private sector critical infrastructure companies are looking out for the safety and security of the American people? Should this interest in public safety an integral aspect of the private market for IT products and services?

Answer. The two items are different. Why are they different? Because in the case of critical infrastructure companies, most know they are "critical" and in fact are already regulated (financial services and utilities, to name two). So, there is already awareness that there is a "duty of care" to the public (or they wouldn't be regulated in the first place).

In the case of the private market for IT products and services, realize that while some products are created for vertical markets that may be regulated (*e.g.,* a piece of software that is used in the utilities industry), a lot of software is general purpose (*e.g.,* accounting software). Trying to impose a "worst case" duty of care on all purpose software would be like trying to ensure that, say, any laptop would be required to comply with the battlefield ruggedness the military demands. The Defense Science Board, in considering the foreign influence over the supply chain of software, realized that, while raising the overall assurance of commercial software was necessary, raising it to the level required for all national security applications was unfeasible because the commercial marketplace will not support such high levels of assurance. I think it is a similar argument for general purpose software used in "critical sectors"—it's not clear whether the market will support *high* assurance to the extent that's what those sectors require.

Now what should happen is that critical sectors use their (perhaps collective) purchasing demands to push their suppliers to *higher* levels of assurance. In fact, we are already seeing many regulated sectors or customers tied to those sectors (as suppliers) demanding more transparency in development practice and higher accountability in software development practice because *their* customers (*e.g.,* pharmaceuticals, defense) are demanding it. And I am all in favor of that push since I think customers' being more demanding purchasers (within reason) absolutely is an effective agent of change.

Question 7. What can the government and private sector do together to solve this labor shortage problem?

Answer. Unfortunately, there isn't a simple solution for this. Nobody can major in "cybersecurity" and in fact, security needs to be embedded in a lot of places if we want to change the dynamic. (E.g., we don't use traffic cops to enforce secure driving—drivers all have to take drivers' ed and be licensed to drive or we wouldn't have a prayer of having reasonably safe highways).

As I have noted in my testimony, I think curricula change in universities is a Must Do or we do not have a prayer of changing the battlefield, so to speak. Perhaps the government can bring some pressure on the accreditation bodies for computer and computer-related degree programs? There is a group called ABET which accredits engineering, computer science and technology programs (see *http://www.abet.org/*) and within that there is a group called Computing Sciences Accreditation Board, see *http://www.csab.org/*) which appears to be the sub-group of ABET that accredits computer science, information systems, software engineering and information technology degree programs. I do not know who accredits industrial control systems degree programs (if it is not within one of the above groups).

Question 8. What can we do to inspire young students to aspire to serve their country by being a cybersecurity professional?

Answer. Making being a good guy more glamorous than being a bad guy, as trivial as that sounds. Currently, the press tends to "glamorize" the hacking community. Vendors are almost universally portrayed as evil slugs that deliberately build crummy software because they do not care about their customers (!). Hackers (including those who release exploit code before a vendor can fix a problem) are often given a pass—regardless of the amount of damage they do. One well-known hacker released "proof of concept code" that several months later was the genesis of the Slammer word, which did BILLIONS in damages. He got a pass from the press for that and there were no legal repercussions, either, since releasing proof of concept code is not illegal.

Finding a way to change the dynamic so kids use their technical skills as defenders and securers can be done (I suspect the Marines'—The Few, the Proud, the Marines—is one of the more successful "service-oriented" advertising campaigns there is).

We have a broader societal problem (in my opinion) in that we have generations raised to be very aware of their rights and what is due them, but few are aware

of or seem to care about their responsibilities. Serving your country is a responsibility of citizenship and I think diversifying that message to emphasize other kinds of service (than just using a rifle) could work (*e.g.,* "Uncle Sam is looking for a few good geeks").

I don't think appealing to the wallet is necessarily the first thing to pitch but quite honestly; there is a lot of demand for cybersecurity professionals—and not nearly the supply. This creates scarcity that increases wages, all things being equal. So yes, cybersecurity is also a good career move because the skills are marketable.

Question 9. What must the government do better? What must the private sector do better? What responsibilities do both have to the public at large?

Answer. I think the government can do a number of things better. For one thing, while the military is busy standing up cyber commands, not all the services actually have career paths for plain old information technology let alone cyber-expertise. I note that traditionally, logistics, though not a war fighter discipline, is still a valued career skill and in fact you can make flag rank (general or admiral) in a logistics specialty. Why does it matter? Because Patton understood what would happen if his 3rd Army ran out of oil. Today's information centric armies run on bits and bytes, just as much as oil. Without a clear, recognized and rewarded career path in both "defensive" information technology and offensive cyber war, the military is sending a signal that information smarts is not valued and is not important.

Obviously, the government also needs to lead by example by securing their own networks.

As far as the private sector goes, I do advocate greater emphasis and "governance" around security for private enterprises. Governance is not about being perfect, it is about understanding the threats to your business, prioritizing them in terms of "what do we, as a company, adhere to in terms of security practices to mitigate those risks?" and ensuring that you are doing those things broadly and consistently. Where you are not doing them, you have a reasonably aggressive remediation plan in place to, as they say, "get with the program." If you do not manage risks appropriately, you are not running your business well.

Response to Written Questions Submitted by Hon. Tom Udall to Mary Ann Davidson

Question 1. Ms. Davidson, in your statement, you note that many of the commercial software components used to build a new "smart grid" probably are not designed for such for the level of cyber attack threats that our Nation's electric grid may face. But ensuring that commercial software, or even government computer systems, are safe from cyber attack is a real challenge. The National Institute of Standards and Technology (NIST) maintains a standard for data encryption, the FIPS 140 standard. What other government or industry standards exist for cyber security?

Answer. There are lots of standards—some of them are technical standards that ensure interoperability of components (*e.g.,* public key encryption standards like PKCS (public key cryptography standards) 11, or standards created by consortia such as the payment card industry (PCI) data security standard (DSS) that addresses securing information related to payment transactions. There are some emerging standards that would specifically facilitate higher "situational awareness" for networks, such as the security content automation protocol (SCAP), a cornucopia of standards that enable things like determining what product is running on a network (and what version), what it's secure configuration is, and so on. These standards were developed by NIST or, in some cases, Mitre under contract to NIST.

There are also international software assurance standards (such as the Common Criteria—International Standards Organization (ISO)–15408) to which the U.S. subscribes. The Common Criteria is focused on describing the nature of threats, what technical measures a product needs to address those threats, and how well it does meet them. I note that in many cases an international standard is really better than a market-specific one, because: (a) a lot of security needs are not country specific and (b) if each country (and in some cases if each industry) starts specifying a similar but slightly different way to do X, companies will—ironically—potentially end up with worse security as they spend money not on actual improvement but on meeting hundreds of only slightly different regulatory requirements. For example, if local, city, county, state and Federal bodies all required separate termite inspections for houses, you'd have to pay for four inspections. Your house would arguably not be four times as termite-free as if you just did one pretty good inspection.

In some cases (by industry) there might be legitimate differences. For example, the Defense Department has (legitimately) different requirements for, say, smart

phones that are going to be used in sensitive environments than the average consumer does for his or her smart phones.

Question 2. Should Congress encourage companies and government agencies to develop and use more cyber security standards?

Answer. I think technical interoperability-type security standards the market will take care of—government tends to be too slow to drive those and entities tend to cooperate when there is a common problem (or, where cooperation will actually increase the market size because there can be more uptake of technology *with* a single standard than would be the case if there are dueling standards).

But there are "underserved" markets or areas in which industry is unlikely to develop common standards where government—specifically, NIST—can have an important role. One such area has been SCAP—being able to determine, quickly, what products are on a network, what their configurations are, to what they might be susceptible, and to be able to reconfigure them automatically—is helping to automate defenses. Considering attacks are automated, automating defenses is important.

Another such area (as unglamorous as it sounds) is auditing and auditability. There are a plethora of products in the sector called SIM (security information management) or SIEM (security information and event management) that claim to be able to analyze "events" on networks (by data mining audit logs) and correlate them (*e.g.,* to see attack patterns). However, that assumes a) that events are recorded at all—not all products have robust enough auditing to even record interesting events—and that the events can be expressed in a common format (so they can be more easily correlated). There is an emerging standard (called CEE—Common Event Expression, see *http://cee.mitre.org/*) in this sector but quite honestly, the government could help create the capacity for better "situational awareness on networks" by fostering a standard adoption through procurement policies. Any software product the government buys could be expected to a) have basic auditability as defined by a standard (possibly CEE, assuming it is actually published by NIST and industry is allowed to comment on it) and b) express their audit records in a common format.

Question 3. The recent Bipartisan Policy Center cyber war game exercise examined a potential attack that first affected wireless cell phones. As computing and networking technology become integral to all manner of consumer goods, it seems that new cyber attack vulnerabilities will only proliferate.

In today's business landscape, supply chains stretch across the globe and companies often acquire other firms to gain access to new software and technologies for their products. This makes it more difficult to know whether a product may contain cybersecurity vulnerabilities from a single component or piece of software code from an outside supplier or other firm. How is security of the final assembled product affected in an environment in which new links are so frequently added to the product's "chain"?

Answer. Keep in mind, there are many supply chain risks businesses need to consider that directly affect their business. These are not necessarily the same concerns that their customers have (but are nonetheless important). For example, some software carries so-called "viral licensing" provisions in that, if the software is embedded within another product, the product comes under the same licensing terms (which in many cases, effectively makes it freeware). No vendor wants to embed such third party code that "taints" their code base in such a way that they can no longer sell the resulting product—their revenue model is destroyed. Second, realize that it is *impossible* to detect all vulnerabilities in software even using the best commercially available tools and it is—in particular (emphasis added) *it is impossible to absolutely prevent someone from putting something bad in code that would be undetectable.*

What is reasonable and feasible is that a company should have reasonable practices around their supply chain risk (because it is in their business interests to do that, anyway). Note again that many of these risks will go directly to their ability to operate and will not necessarily be the same risks that a purchaser worries about. A company should also have a reasonable governance structure in place to ensure that they are doing the same things across their lines of business. Having done that, they could disclose their practices to interested purchasers—who were, for example, concerned over how a company takes reasonable measures to prevent someone from corrupting their code base. Reasonable means that, for example, changes to code have attribution, and there are restrictions on access (*e.g.,* not just anybody in the company can make a change to code—and certainly not in a way that cannot be attributed).

I have done a paper for the House Homeland Security Subcommittee on Cybersecurity, Emerging Threats and Science and Technology on supply chain risk that speaks to the above in more detail and I would be happy to provide that, as well, if it is of interest and of use.

Question 4. How are leading technology companies bringing the security of acquired products in line with their own standards for cybersecurity?

Answer. I cannot (obviously) speak for other companies, but Oracle has a structured process for integrating acquired companies into Oracle business practices. My team has the remit for integration of acquired entities into our secure development practices. As part of that, we rapidly ascertain their current practices, use the review to create a compliance plan going forward, and—as with all lines of business—periodically report progress against compliance requirements to executive management via a security oversight committee. The compliance measurement covers the entirety of our secure development practices. In cases where an entity struggles to make compliance we highlight them for special attention and guidance (and the accountability that goes with it). There are other groups that look after integration of our networks, the security policies that go with our business practices, and so forth.

Question 5. What is the role of Chief Security Officers or Chief Technology Officers in assuring best security practices are implemented in such cases?

Answer. There can be several roles. One of them is that to the extent a CTO or CSO is an influencer or purchaser of technology, they can enforce better procurement transparency on their suppliers. That could include specific "disclosure" requirements on their suppliers related to development practice if not compliance with standards (like FIPS–140, or ISO 15408).

Second, to the extent a company develops their own software, they should have internal standards for development practice that at least reflect or include consensus good practice. That can reference "standards"—I use the term loosely—such as BSIMM (Build Security In Maturity Model), or the Build Security In guidance issued by the Department of Homeland Security, or things like the SANS Top 25 coding errors (*i.e.,* to at least ensure that a developer has considered these issues and attempted to avoid them), and so forth. There actually is a lot of material out on what constitutes good, secure development practice, and what common vulnerabilities are (and how to avoid them). It's unconscionable that universities do not educate people who design and build systems on these matters, but that does not mean people who build systems in industry should accept that "educational deficiency" without making every effort to rectify it in their *own* practice.

ATTACHMENT

Supply Chain Risk

The purpose of this document is to outline risk management concerns pertaining to the supply chain of software and hardware. This document may serve as a blueprint for suppliers seeking to ensure they've adequately addressed hardware- and software-related supply chain risk, and for purchasers in the procurement of software. That is, suppliers that want to protect their supply chain should be able to address these questions for their own risk management purposes. Secondarily, suppliers should be able to *disclose* their supply chain risk management practices so that a purchaser can make better risk-based acquisition decisions.

While supply chain transparency alone will not ameliorate risk, it will level the playing field to the extent that supply chain assurance "disclosure" becomes the norm, and thus customers have the ability to use supply chain risk mitigation as a—but not necessarily *the only*—purchasing criterion. Furthermore, it is likely that disclosure will lead to some upleveling of security practices to the extent vendors are not already addressing supply chain risk *and* more customers evaluate supply chain risk prior to purchasing. That is, to the extent more purchasers demand transparency around supply chain risk mitigation, suppliers not already addressing this risk will be compelled by market forces to do so.

Scope

The scope of this paper is supply chain risk for commercial off-the-shelf (COTS) software and hardware, not custom code or government off-the-shelf (GOTS) software and hardware, which may be a combination of COTS components and either government-developed or third party custom code. GOTS could include custom applications (built by cleared individuals) that run on COTS components, for example. This document does *not* address supply chain risk related to industrial policy (*i.e.,* a country may wish to ensure that they have one or more domestic suppliers of a

critical component—such as microprocessors µ la the Trusted Foundry Program—to avoid supply chain disruption caused by war or other geopolitical upheaval).

Constraints

There are a number of practical constraints that bound the "supply chain risk assessment" problem as it pertains to COTS software and hardware. These constraints are important because they set the framework for what can reasonably and feasibly be asserted about the supply chain of commercial software and hardware. Any such "reasonability" discussion must of necessity bound efforts to reduce or mitigate supply chain risk for COTS. In particular, COTS is *not* GOTS: it is no more reasonable to purchase commercial, general purpose software and hardware and expect it to have the assurance (*e.g.,* extensive third party validation, "cleared" personnel, robustness in threat environments it was not designed for) of custom, single purpose software and hardware as it is to purchase a Gulfstream V and expect it to perform to the specifications of an F–22 Raptor.

Constraint 1: In the general case—and certainly for multi-purpose infrastructure and applications software and hardware—there are no COTS products without global development and manufacturing.

Discussion: The explosion in COTS software and hardware of the past 20 years has occurred precisely because companies are able to gain access to global talent by developing products around the world. For example, a development effort may include personnel on a single "virtual team" who work across the United States and in the United Kingdom and India. COTS suppliers also need access to global resources to support their global customers. For example, COTS suppliers often offer 7x24 support in which responsibility for addressing a critical customer service request migrates around the globe, from support center to support center (often referred to as a "follow the sun" model). Furthermore, the more effective and available (that is, 7x24 and global) support is, the more likely problems will be reported and resolved more quickly for the benefit of all customers. Even smaller firms that produce niche COTS products (*e.g.,* cryptographic or security software and hardware) may use global talent to produce it.

Note that global development may include outsourcing of development staff resource (use of contracted third parties to develop code modules that are sold separately, or integrated into larger product suites), as well in-house developers (employees) of a global enterprise that are located in development centers around the globe. For example, some enterprise software providers build some modules in-house while being an open source distributor for other modules. In addition to including development groups in multiple countries, global development may also include H1B visa holders or green card holders working in the United States.

Hardware suppliers are typically no longer "soup to nuts" manufacturers. That is, a hardware supplier may use a global supply network in which components—sourced from multiple entities worldwide—are assembled by another entity. Software is loaded onto the finished hardware in yet another manufacturing step. Global manufacturing and assembly helps hardware suppliers focus on production of the elements for which they can best add value and keeps overall manufacturing and distribution costs low. We take it for granted that we can buy serviceable and powerful personal computers for under $1000, but it was not that long ago that the computing power in the average PC was out of reach for all but highly capitalized entities and special purpose applications. Global manufacturing and distribution has helped make this happen.

In summary, many organizations that would have deployed custom software and hardware in the past have now "bet the farm" on the use of COTS products because they are cheaper, more feature rich, and more supportable than custom software and hardware. As a result, COTS products are being embedded in many systems—or used in many deployment scenarios—that they were not necessarily designed for. Supply chain risk is by no means the *only* risk of deploying commercial products in non-commercial threat environments.

Constraint 2: It is not possible to prevent someone from putting something in code that is undetectable and potentially malicious, no matter how much you tighten geographic parameters.

Discussion: One of the main expressions of concern over supply chain risk is the "malware boogeyman," most often associated with the fear that a malicious employee with authorized access to code will put a backdoor or malware in code that is eventually sold to a critical infrastructure provider (*e.g.,* financial services, utilities) or a defense or intelligence agency. Such code, it is feared, could enable an adversary to alter (*i.e.,* change) data or exfiltrate data (*e.g.,* remove copies of data surreptitiously) or make use of a planted "kill switch" to prevent the software or hard-

ware from functioning. Typically, the fear is expressed as "a foreigner" could do this. However, it is unclear precisely what "foreigner" is in this context:

- There are many H1B visa holders (and green card holders) who work for companies located in the United States. Are these "foreigners?"
- There are U.S. citizens who live in countries other than the U.S. and work on code there. Are these "foreigners?" That is, is the fear of code corruption based on geography or national origin of the developer?
- There are developers who are naturalized U.S. citizens (or dual passport holders). Are these "foreigners?"

It is unclear whether the concern is geographic locale, national origin of a developer or overall development practice and the consistency by which it is applied worldwide. For example, non-US staff working outside the U.S. would appear by definition to be "foreigners," yet they are often subject to U.S. management oversight and their work on code may be peer and manager reviewed before it is accepted. In the sense that a U.S. manager "accepts" responsibility for a "foreigner's" code work, is this still a concern?

Similarly, there are presumably different levels of concern for different foreign countries. How is a COTS vendor expected to know which countries are of more concern than others? Should work by staff working in or citizens of traditional U.S. allies be accepted as similar to that of U.S. staff?

COTS software, particularly infrastructure software (operating systems, databases, middleware) or packaged applications (customer relationship management (CRM), enterprise resource planning (ERP)) typically has multiple millions of lines of code (*e.g.,* the Oracle database has about 70 million lines of code). Also typically, commercial software is in near-constant state of development: there is always a new version under development or old versions undergoing maintenance. While there are automated tools on the market that can scan source code for exploitable security defects (so-called static analysis tools), such tools find only a portion of exploitable defects and these are typically of the "coding error" variety. They do not find most design defects and they would be unlikely to find deliberately introduced backdoors or malware.[1]

Given the size of COTS code bases, the fact they are in a near constant state of flux, and the limits of automated tools, there is no way to absolutely prevent the insertion of bad code that would have unintended consequences and would not be detectable. (As a proof point, a security expert in command and control systems once put "bad code" in a specific 100 lines of code and challenged code reviewers to find it within the specific 100 lines of code. They couldn't. In other words, even if you know where to look, malware can be and often is undetectable.)[2]

Constraint 3: Commercial assurance is not "high assurance."

Note that there are existing, internationally recognized assurance measures such as the Common Criteria (ISO–15408) that validate that software meets specific (stated) threats it was designed to meet. The Common Criteria supports a sliding scale of assurance (*i.e.,* levels 1 through 7) with different levels of software development rigor required at each level: the higher the assurance level, the more development rigor required to substantiate the higher assurance level. Most commercial software can be evaluated up to Evaluation Assurance Level (EAL) 4 (which, under the Common Criteria Recognition Arrangement (CCRA), is also accepted by other countries that subscribe to the Common Criteria).

Regarding the supply chain issue at hand, what is achievable and commercially feasible is for a supplier to have reasonable controls on access to source code during its development cycle and reasonable use of commercial tools and processes that will find routine "bad code" (such as exploitable coding errors that lead to security vulnerabilities). Such a "raise the bar" exercise may have a deterrent affect to the extent that it removes the plausible deniability of a malefactor inserting a common

[1] For example, a trivial way to introduce a backdoor in a way that would be undetectable by automated tools would be to create a package or function (that is, a piece of code that does something specific) that is "called" within a piece of software but that does—nothing. Nothing that is, unless the package is called with a specific argument—that is, a piece of data (*e.g.,* an input string) that triggers the package to do something very specific and malevolent. While some automated tools scan for "dead code"—code that is never executed—this package *would* be executed in the sense it is called by many other pieces of code—but doesn't do anything, or doesn't do anything bad, except when called with a particular "triggering" input. Manual code review might catch this, but as noted earlier, manual code review is unlikely for every change to a large code base that changes constantly.

[2] The expert related the story while serving on the Defense Science Board task force analyzing the mission impact of foreign influence on DOD software, referenced later in this paper.

coding error that leads to a security exploit. That is, in the absence of using these tools, a malefactor could insert a back door implemented as a common coding error. If the error is found, the malefactor has plausible deniability that, after all, he made a coding error that many other developers make, such as a buffer overflow. Using automated vulnerability finding tools, in addition to improving code hygiene, makes it harder for someone to deliberately insert a backdoor masquerading as a common coding error because the tools find many such coding errors. Thus, a malefactor may, at least, have to work harder. (A side benefit is the overall lower cost of ownership of software to the extent code quality improves and customers do not have to apply so many after-the-fact security patches.)

That said, and to Constraint 1, the COTS marketplace will *not* support significantly higher software assurance levels such as manual code review of 70 million lines of code, or extensive third party "validation" of large bodies of code beyond existing mechanisms (*i.e.,* the Common Criteria) nor will it support a "custom code" development model where all developers are U.S. citizens, anymore than the marketplace will support U.S.-only components and U.S.-only assembly in hardware manufacturing. This was, in fact, a conclusion reached by the Defense Science Board in their report on foreign influence on the supply chain of software.[3] And in fact, supply chain risk is not about the citizenship of developers or their geographic locale but about the lifecycle of software, how it can be corrupted, and taking reasonable and commercially feasible precautions to prevent code corruption.

The lack of market support for "higher assurance commercial software" is *particularly* ironic given the recent policy change[4] by the National Information Assurance Partnership (NIAP) that negates much of the value of existing assurance mechanisms (*i.e.,* Common Criteria evaluations). While they are not perfect, Common Criteria evaluations do establish the assurance of commercial software and—at commercial assurance levels—includes an assessment of the security of the software development environment. In other words, it is ironic that there seems to be increased interest in software assurance (or, the supply chain aspects of assurance) at the very time the U.S. government is undercutting the market for evaluated products.

Constraint 4: Any supply chain assurance exercise—whether improved assurance or improved disclosure—must be done under the auspices of a single global standard, such as the Common Criteria.

This document is proposed as a potential "disclosure questionnaire" for both suppliers and purchasers of software and hardware. Any such disclosure requirement needs to ensure that the value of information—to purchasers—is greater than the cost to suppliers of providing such information. That is, the information needs to result in significantly more "informed" purchasing behavior than would otherwise be the case. To that end, disclosure should be something that is standardized, not customized. Even a large vendor would not be able to complete per-customer or per-industry questionnaires on supply chain risk for each release of each product they produce. The cost of completing such "per-customer, per-industry" questionnaires would be considerable, and far more so for small, niche vendors or innovative start-ups.

For example, a draft questionnaire by the Department of Homeland Security as part of their software assurance efforts asked, for each development project, for each phase of development (requirement, design, code, and test) how many "foreigners" worked on each project? A large product may have hundreds of projects, and collating how many "foreigners" worked on each of them provides little value (and says nothing about the assurance of the software development process) while being extremely expensive to collect. (The question was dropped from the final document.)

---

[3] Report of the Defense Science Board Task Force on the Mission Impact of Foreign Influence on DOD Software (*http://www.acq.osd.mil/dsb/reports/2007-09-Mission_Impact_of_Foreign_Influence_on_DoD_Software.pdf*).

[4] See *http://www.niap-ccevs.org/* Prior to October 2009, procurement policy as it related to software assurance was governed by Department of Defense (DOD) 8500, which stated that national security systems must have an international Common Criteria (ISO 15408) evaluation or, for cryptographic modules, Federal Information Processing Standard (FIPS) 140–2 cryptographic module validation. (Note: DoD 8500 and NSTISSP #11 are due to be modified to reflect the new NIAP policy.) As of October 2009, the NIAP policy has been changed such that only products for which the U.S. government has an approved "protection profile" (a description of the threats a specific class of product faces and the technical remedies for these threats) must be evaluated. (The only other "exception" is in the case where an agency indicates to NSA by letter that they need another class of product—without a protection profile—evaluated.) While the intent of the policy is to make evaluation more "relevant" to the stated needs of the U.S. Government, as a practical matter it has undercut the market for evaluated products. Vendors are already reassigning their evaluation personnel in response to this "market signaling."

More specifically, given that the major supply chain concerns seem to be centered on assurance, we should use international assurance standards (specifically the Common Criteria) to address them. Were someone to institute a separate, expensive, non-international "supply chain assurance certification," not only would software assurance not improve, it would likely get worse, because the same resources that companies today spend on improving their product would be spent on secondary or tertiary "certifications" that are expensive, inconsistent and non-leverageable. A new "regulatory regime"—particularly one that largely overlaps with an existing scheme—would be expensive and "crowd out" better uses of time, people, and money. To the extent some supply chain issues are not already addressed in Common Criteria evaluations, the Common Criteria could be modified to address them, using an existing structure that already speaks to assurance in the international realm.

Terms

Like the Indian fable of the six blind men and the elephant, each of whom described a totally different animal based on what part of it they were touching, the definition of "supply chain risk" often varies depending on who is describing it. The assurance that stakeholders may wish to have around *supply chain risk* may vary depending on their perspectives. For example, vendor concerns may include a heavy emphasis on intellectual property (IP) protection since IP is typically one's "corporate crown jewels" and, should it be compromised (*e.g.,* stolen or tainted) the firm may be out of business or crippled in some markets. For customers, the concern tends to focus on the aforementioned "malware boogeyman" which is a subset of a larger discipline known as software assurance.

Counterfeiting is a risk that is perceptually greater for hardware than for software. The concern from a supplier's side goes to both their brand and their intellectual property since a hardware component has to both look like and perform like the genuine article but may not be as good a quality as the genuine article. The customer concerns over counterfeiting include getting what you pay for in terms of performance characteristics (*i.e.,* not failing at a critical juncture) and the customer ability to service the product.

Software assurance (SwA) is defined by the Department of Homeland Security as "the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner."

Source code is raw computer code in uncompiled form. Typically, vendors deliver compiled code (also known as binaries or executables) to customers, so that all the customer can do is execute—"run"—the code. While much software is configurable, the executable typically limits the amount of customization or configuration a customer can do to what is designed in (*e.g.,* a customer of an ERP application can typically configure approval hierarchies or the chart of accounts, but cannot change the basic logic of the application). Therefore, most threats to the supply chain are threats to source code to the extent that it is source code that must actually be modified (maliciously).

There is another risk to the extent that some code allows execution of other binaries that are "linked in"—allowed to run with the executable. That is, a software developer that downloads or purchases binaries to run with their code without an understanding or vetting of what that code does could be allowing "bad code" to execute with or within their product. Much software (such as browsers or wiki software) is explicitly designed to allow such third party "plug-ins." Despite the fact that the basic software usually "warns" users of the dangers of allowing unvalidated plug-ins to run, most users just "click through" such warnings because they want the features of the "cool" plug-in.

Supply Chain/Source Code Questions

The following questions outline concerns that a software or hardware manufacturer should address in regards to protection of source code throughout its lifecycle. It also includes questions related to hardware-related intellectual property and assembly. By addressing these concerns, a software or hardware manufacturer should be able to:

- Identify the ways in which they are addressing risks (and the "owners" for those areas).
- Document what is being done—and not done—to protect their source code throughout its lifecycle.
- Identify remaining unmitigated risk and propose ways to reduce that risk.

- Create a governance structure around the protection of source code—and other intellectual property, such as hardware designs—to ensure that policies are followed consistently across lines of business, and consistently over time.

Note: many below questions that are geared toward intellectual property protection of source code may be equally applicable to the intellectual property associated with hardware designs (*i.e.,* limiting access to source code or hardware designs to ensure employees—with or without "need to know"—do not commit IP theft).

Acquisition

Many companies grow by acquisition and incorporate code sets from those acquisitions into other products. Ultimately, the processes and policies that a company implements around supply chain risk need to be reasonably consistent (that is, if there is an exception or a policy "difference," there should be a reason for it and an explicit approval of that difference).

A1. Do you do any pre-acquisition screening of source code prior to an acquisition (*e.g.,* to ascertain what it does, the "content" or other characteristics of the code)? The general concern is, "Do you know what you are getting in an acquisition?"[5]

A2. Are you consistent across all acquisitions, or do you do different "source code due diligence" depending on the acquisition?

A3. Are acquired code bases integrated into your other software development practices? How quickly, and how often is this progress measured?

Development

Software development encompasses much of the lifecycle of code. This may include incorporation of third party code (*e.g.,* open source, licensed libraries), the core development of new code, the ability to maintain it through its lifecycle, granting access to source code to third parties (*e.g.,* for a security assessment or for other reasons) and escrowing the code.

Personnel

D1. What screening or background check do you do of employees who get access to source code throughout its life cycle?

D2. Is the screening consistent (in terms of quality) across employees, geographic areas and product divisions?

D3. Do you differentiate among some products or product areas that are deemed more critical (and thus do more stringent checks)? Which ones?

Third Party Code (not Open Source Code)

D4. What controls do you have around third party code incorporation into the code base (to ensure, for example, that a random piece of code without approval, appropriate licensing and oversight is not introduced into source code)?

D5. In cases where you do incorporate third party code, are you incorporating source code in all cases, or are there some object libraries?

D6. What if any security checks do you do on third party code, and is it consistent across product lines and across "homegrown" and "third party" libraries? (That is, any code shipped with a product should in general comply with the same standards of quality, testing, and so on.)

D7. Are the security checks done via manual code review, static analysis or other analytic tool, or via another means?

D8. Are the same checks done on patches and updates? That is, if a third party provider gives you a "patch" to a problem in their libraries, are there any security checks done on the patch?

D9. How consistently are the above checks done across third party libraries and across lines of business?

Open Source Code

D10. What processes and policies do you have around incorporation of open source code into your product (to ensure, for example, that you do not incorporate viral licenses, or "back-doored code" or an otherwise "tainted" open source code into your code base)?

D11. Are the same checks done on patches and updates? That is, if a third party provider gives you a "patch" to a problem in their libraries, are there any security checks done on the patch?

---

[5] One reason to do such pre-acquisition screening is to identify so-called "viral licenses" wherein inclusion of the code in a larger code base changes the licensing terms, potentially "tainting" the larger code base and one's ability to generate revenue from it. There are automated tools (*e.g.,* from Black Duck) that can scan code bases looking for such "viral license" code.

D12. How consistently are the above checks done across open source libraries and across lines of business?

Development Access Control

D13. Have you identified all employees who get access to source code throughout its life cycle (*e.g.,* developers, quality assurance (QA), support personnel) as apropos? (That is, access to source code should be reasonably restricted to those with a need to access it, not open to all. While the ability to modify code (write) is one concern, the ability to read code (that is read but not modify) may also be a concern for purposes of intellectual property protection.)

D14. Do you deploy source control systems to govern access to and modification of source code?

D15. What is the granularity of access? (That is, can a developer get access to, say, an entire product's code base or a much smaller subset?)

D16. How often is this access control reverified? For example, if an employee is transferred, how quickly is source code access modified or restricted accordingly?

D17. How consistent are your access controls? (That is, are these controls implemented consistently across all product areas, or is there a lot of disparity on granularity depending on product access?)

D18. Are the servers on which source code is stored regularly maintained (*e.g.,* do you apply critical patches—especially security patches—in a timely manner?)

D19. Are there baseline secure configurations enforced on the servers on which source code is stored and how often are these checked? (The concern is whether someone can bypass source code controls by breaking into the source code server through, say, a poor configuration or an unpatched system.)

D20. Do you have any special carve outs on source code access beyond "by product/by developer"—for example, are there greater restrictions on accessing security functionality like encryption technologies (*e.g.,* for Export Administration Regulations (EAR) reasons) or other geographic restrictions?

D21. Do you review, validate (or "pen test") your source code access controls to ensure that your controls are adequate? How often?

D22. Do you do any proactive checking (*e.g.,* through a data loss prevention tool) to look for source code leaving your corporate network (*e.g.,* through someone e-mailing it)?

D23. What if any auditing do you have on who accesses source code in development and does anyone ever review those logs? How often?

D24. What if any native logs are there in the source control system itself and how far back can you attribute changes to code?

D25. Are code changes attributable to individual developers?

Security Testing

T1. Do you use automated (or other) tools—such as static analysis—to actively look for security vulnerabilities in code?

T2. How broadly is the tool deployed within a product? (*E.g.,* is it run against all libraries associated with a product, just a few, or something in between?)

T3. How broad is the code coverage of such tools across all products and lines of business?

T4. Are defects found via such tools logged and tracked?

T5. What policies do you have around fixing defects you find either during development or afterwards? Do you keep metrics around how quickly issues are fixed?

T6. What kind of access control or restrictions do you have on access to information about unfixed security vulnerabilities? (The concern is that a malefactor could find information about exploitable defects by accessing a record or database of such information if access is not suitably restricted to those with "need to know.")

Manufacturing and Distribution

M1. What processes do you have to ensure that your code is not corrupted in between development and delivery to customers or external parties (*e.g.,* escrow agents)? For example, do you use checksums or other mechanisms to ensure that the code "as developed and released to manufacturing" is what is delivered to customers?

M2. Are these processes consistent across product divisions and products?

M3. What are your processes regarding backing up (that is, secure storage) of source code, to include length of time for which you store it (*e.g.,* escrowing), security controls around the secure storage (*e.g.,* encryption) and any auditing or "spot checking" of these controls?

M4. Do you use a third party to escrow source code? If so, what controls are there on source code as it is transmitted to the firm (*e.g.,* is it encrypted and/or sent by trusted courier, other?)

Third Party Access to Source Code

P1. What policies do you have around providing access to source code to third parties and how are they enforced? (There are many reasons an entity might provide such access: for example, a third party might be doing a "port" of the code to an operating system that the company does not have in-house resources to do.) What kind of access is provided and how is it provided? (Does the third party have access to corporate networks for purposes of accessing code, or other?)

P2. Is there any "master list" of where such access has been approved and provided, to whom, for what products and so forth?

P3. What policies and processes do you have in place to ensure, for example, that random third parties (to include customers and third party research firms acting on their behalf) do not get access to source code for purposes of security analysis? (While companies may wish to contract with third parties for such purposes, allowing a third party to access source code for security analysis purposes allows that third party to amass a database of unfixed security vulnerabilities which, if compromised or sold, could put all customers at risk.)

Hardware

The following section addresses hardware-specific supply chain risks.

Manufacturing

HM1. To what degree is your manufacturing outsourced?

HM2. If all or part of your manufacturing is outsourced, what steps have you taken to mitigate intellectual property theft (*i.e.,* by not having a turnkey "outsourcer" that provides all components to specifications and that also does final assembly, or by selecting locales based on "country risk?")[6]

Testing

HT1. What kind of testing do conduct of a) components during manufacturing and b) final component assembly?

HT2. Is testing done by the outsourcer or is there a "check and balance?" wherein testing is done by an entity other than the manufacturer?

HT3. How broad and deep is the testing (Each component? Each final assembly?)

HT4. Does testing[7] include verification that there are no components or functions that should not be there?

Counterfeiting/Fraud

HC1. What procedures do you have in place to ensure that components used in hardware manufacture are authentic (that is, not counterfeited)? How broad (*i.e.,* against the spectrum of components) and deep (*i.e.,* frequency) is your verification?

HC2. What procedures do you have in place to provide component verification for customers (that is, to establish that hardware ostensibly of your manufacture actually is authentic and not a knockoff?)

HC3. Do you actively look for fraudulent "suppliers" of your product?

Other

HO1. Are any hardware components used and resold[8] wiped to ensure that no data—or non-standard programs—are installed when they are delivered to customers?

HO2. Is this verified to ensure that data is truly non-recoverable?

HO3. Are hardware components used operationally wiped before being scrapped or resold to ensure that data is non-recoverable?

---

[6] The degree to which manufacturing can be outsourced in sections is a function of the amount of expertise one wants to retain in-house and also an assessment of risk of putting all one's eggs in one basket, in particular, country-specific risk. Some locales have not only a higher reputation for intellectual property theft but much less legal protection of IP.

[7] Note: as with software, hardware testing can establish that hardware performs to specifications but cannot necessarily establish what it does *not* do.

[8] Some companies use their own hardware components for testing or development purposes for a period of 90 days or less and then sell them to customers (tax laws allow this). It's critical to ensure that there is no data or non-standard programs on the hardware for the protection of both the supplier and customers. This is a different issue than wiping corporate data (or intellectual property) prior to disposition.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN ENSIGN TO MARY ANN DAVIDSON

Question 1. Ms. Davidson, Mr. Lewis of the Center for Strategic and International Studies states in his testimony that public-private partnerships, information-sharing, self-regulation, and market-based solutions in the cybersecurity space are "well past their sell-by date" and have not been successful. He argues that strong government mandates are required to spur the cybersecurity innovation that our country needs. As the only witness on the panel who has any hands-on cybersecurity experience in the private sector, do you agree with Mr. Lewis that we have exhausted the potential of market-based solutions to improve cybersecurity? If not, what specific steps can we take to improve cooperation and coordination between industry and the government?

Answer. With all respect to my esteemed colleague, Mr. Lewis, I do not agree with him on this issue. To take these points separately, I do not think that market based solutions have been fully explored in areas where they could help harvest low hanging security fruit. To give one such example, the Air Force (under then-CIO John Gilligan) realized that some 80 percent of their serious security vulnerabilities (as identified by NSA) were the result of poor desktop configurations. They worked with one of their major suppliers (Microsoft) and NSA to craft a more secure desktop configuration and then—as a condition of procurement—required Microsoft to ship products to them in the secure default configuration. They estimated they saved millions of dollars over the life of their contract and dramatically improved their security posture. That configuration became the basis of the Federal Desktop Core Configuration (FDCC), which the Office of Management and Budget (OMB) required all suppliers to be able to comply with (that is, suppliers who ran on a Microsoft desktop needed to assert that they supported /could run on an FDCC-compliant Windows desktop).

While the way the program was implemented can and should be improved, as a general construct, it was an important and needed effort. The U.S. government could help themselves—and other market sectors—by requiring any product sold to them to: (a) deliver a secure configuration guide, (b) allow the product to be installed by default in the secure configuration, and (c) provide either tools to maintain the configuration OR make the security-specific configuration parameters machine readable in a standard format (such as Security Content Automation Protocol (SCAP)). It is a "no brainer" to require suppliers to do something once that enables all customers to: (a) be more secure out of the box, (b) maintain their security posture easily, and (c) lower their lifecycle security costs. Yet, it has never been broadly adopted as a procurement requirement. There is a lot of low hanging fruit like that that has never been planted, let alone harvested. (Note: Oracle, like many large vendors, has instituted "secure by default" as part of their development process. We do this because we, like many vendors, run our own company on our own software and thus it lowers our own IT security costs and improves our IT security posture as a company, not to mention that of all other customers. Providing good security at an attractive price point is also a competitive advantage for us. In short, we have market incentives (lower cost of operations) to deliver secure configurations.)

No vendor can or should argue that doing something once as a vendor, that improves security for all customers, and lowers their lifecycle costs, "can't be done" or "shouldn't be done." It does work, it can work, it must work. It makes too much economic sense not to work (and does, indeed, correct a market inefficiency).

I am leery of "information sharing" being thrown out as a security cure-all, because information sharing is a technique, or a tactic; it is not a strategy. Specifically, it is not always easy to ascertain what information is useful, with whom it should be shared, what the desired result would be of such information sharing, and so on. Absent some concrete "for instances," it's ineffective for everyone to share everything with everybody as a cure for cybersecurity problems. Furthermore, information sharing (in the general sense) typically imposes costs on those sharing the information that may "crowd out" other—more useful—security activity. Not to mention, many businesses are global entities, so it is difficult to share information with one entity (the U.S. government) and not others (*e.g.,* other governments).

Back to the procurement idea, what would actually facilitate information sharing, and enable better situational awareness as well as more automated defenses is continuing to push the elements of SCAP through the standards process (ideally, as an international standards organization (ISO) standard) and then requiring suppliers to support SCAP as a condition of Federal procurement. Why? Because currently, nobody can answer the following questions real time: what is on my network? who is on my network? what is my state of (security) readiness? and what is happening that I should be concerned about? SCAP does not speak to all of these, but absent

being able to automate discovery of what's on the network—what products, what versions—what is the security configuration of those elements—what vulnerabilities are present? and so on, there is no way that defenses can be automated. And, being able to have a common language to express the above would take the scarce resources we now employ in purchasing and deploying multiple one-off tools—which cannot communicate with all networks elements, which cannot express "readiness" in any way that is actionable—and apply them to other areas of network defense. Better intelligence at a lower cost: voila!

Automated and actionable information sharing for which the information has a specific purpose and distinct benefit is more effective than "give us all your information."

In short, the government *can* and *does* change the market through their procurement policies. "You don't ask; you don't get" is not, perhaps, enshrined in the Federal Acquisition Regulations, but it should be. And, working with industry in a public private partnership to talk about how rapidly those requirements can be implemented, what kind of timelines, and so on, could help make procurement an effective instrument of change.

Another example: the Defense Department claims they want to do better risk based acquisitions. One way to accomplish this would be for the U.S. Government to come up with a standard (*i.e.,* "single") set of reasonable questions around software development practices that would help a customer know what was and was not done in the area of security. They should be questions for which the answers: (a) have value, (b) would materially affect the customers' decision to procure and (c) have a specific purpose in mind that (d) should be readily answerable by both large and small suppliers. A vendor could answer these questions once (per product) and the results could be reused by a number of procurement offices. Better information, at lower cost, and more transparency. Transparency also reduces market inefficiencies (*i.e.,* where the seller has more information than the purchaser). This is also a better approach than having multiple, agency-specific or country specific "assessments" that actually crowd out security improvements (just as having 12 termite inspections will not results in a house with $\frac{1}{12}^{th}$ the number of termites, but it *will* result in a more expensive house). I already have had customers asking for such transparency and, where a product group is not doing as well as I would like, I have used the "transparency requirement" to push the problems to a senior level of management. (That is, if you don't want to publicly say you don't do A, B, and C, because you think you will look bad vis a vis your competitors, then the remedy is to start doing A, B and C. This assumes A, B and C are worth doing and materially improve security which, in the case of our company and others who have such software assurance programs, they are.) If it is true that everybody cannot do everything perfectly in security (and it is true), it is also true that most of us can do some things better that are also economically feasible to do better.

Question 2. Ms. Davidson, in your testimony you discuss the need to change our educational system and to slow our country's exposure to systemic cybersecurity risk. You raise a lot of good points, but do you have any other specific recommendations on what this committee can do to harden and protect our critical infrastructure?

Answer. What about starting to require self defending products as part of procurement? The Marine Corps ethos is "every Marine a rifleman." That is, every Marine can fight, and they don't outsource individual defense to the next Marine down the line. They do not assume their perimeters will not be breached, nor that they will never take casualties.

Given the threat environment (and the fact that our perimeters are so porous), we should change our mindset away from "build stronger firewalls" to realizing that: (a) perimeters will be breached and thus (b) we need both "redoubts"—ideally dynamic redoubts—and for each product to be able to defend itself. That is, products already know what good input look likes, how to handle bad input gracefully, It ought also to anticipate "evil input" and be able to share real time information (*e.g.,* events of interest) via a common auditing protocol and format (something NIST could develop and, apparently is developing via a standard called CEE (Common Event Expression). A fire team pinned down by enemies will not last long if it cannot tell the command post they are under fire in language the command post can understand. Systems under attack will not be able to survive if they cannot digitally do the same thing.

Procurement could be used to start "signaling" the marketplace that DOD expects products to natively defend themselves instead of assuming "nobody would ever do that," and "the firewall will save us all" as is the case now.

Networks are—like it or not—battlefields now and we ought to take the lessons we have learned from warfare and apply them to general network defense (and by

that I do not necessarily mean "cyberwar"). By way of example, the late Maj. John Boyd's theories on the importance of maneuverability to air combat (popularized as the so-called observe-orient-decide-act (OODA) loop) found later application to ground combat (*i.e.,* in the first Gulf War) and also in business strategy.

Question 3. Ms. Davidson, in his testimony, Admiral McConnell recommends establishing a National Cybersecurity Center (modeled after the National Counter Terrorism Center) that would integrate private sector participation with interagency cooperation. What are your thoughts about such a center? In your opinion, would the private sector view this as a positive development or just one more layer of government bureaucracy?

Answer. Before undertaking such an activity, I'd want to consider what existing organizations do (and how well) and what the "mission statement" is for such a new organization. We already have industry specific information sharing and analysis centers (ISACs) which are natural focal points for both industry sectors to share information among themselves and to serve as a focal point for interactions with government (*e.g.,* I have been told—but have no way to verify—that the Heartland Payment Systems data breach used techniques that were known and discussed in the financial services industry ISAC (of which Heartland was not a member at the time)).

Question 4. What mechanisms are in place for private companies to report cyber intrusions (either originating domestically or overseas) to the Federal Government?

Answer. As a general comment, I think we need to choose words carefully in terms of what constitutes an intrusion. That is, there may be "general patterns of traffic" that could be of interest, that do not constitute an intrusion. Also, there are "incidents" that, upon investigation, are found not to have merit. For example, if a company has poor processes for terminating the accounts of employees who have left, and a (former) employee accesses their network, should that be reported to the government? I would think "no," in the general case. Now, if the company had evidence that their industrial designs for, say, a new hardware encryption device being built for the Defense Department were exfiltrated by that employee, the answer would likely be "yes."

Question 5. What is being done to encourage private companies, particularly those with government contracts, to report cyber intrusions (either originating domestically or overseas)?

Answer. With all respect, this discussion, doubtless coming on the heels of the Google-China incident, reminds me of the discussions of 8 or 9 years ago, when the Federal Government wanted information about non-public security vulnerabilities in software products (the discussion was typically, "vendors, give us all your vulnerability information"). Leaving aside the fact that a) there is often no remediation for such issues until the vendor issues a patch, b) sharing that information inevitably results in data leaks, which puts everyone at risk. Famously, CPNI (part of MI–5) "shared" such information on a "need to know" basis only (with other UK intelligence or Ministry of Defence entities) and yet it leaked to U.S. COMMERCIAL customers, which led to the actual vulnerability being reported to the vendor who built the software. The vendor, of course, was the only one actually able to remediate the defect. In the meantime, the risk to the vendors' customer base materially increased and the trust of the vendor community toward this particular government materially decreased. (CPNI have since implemented much better information sharing protocols.)

There is a difference between a cyber intrusion where the entity has determined is limited and did no damage and one in which there was material harm. The next question ought to be a consideration of the benefit of sharing that information, the cost of obtaining it, and the positive results that would accrue from it. Just asking people to throw audit logs over the wall to a third party, for example, does not have a clear benefit (and could, if the information were not handled properly, render the intruded upon entity MORE vulnerable in the future).

Question 6. Do government contractors have an ethical or statutory obligation to report cyber intrusions (either originating domestically or overseas)?

Answer. In my opinion, it depends upon the nature of the intrusion.

Question 7. Do government contractors with classified information on their servers and individuals with security clearances on their payrolls have a statutory or ethical obligation to report cyber intrusions (either originating domestically or overseas)?

Answer. See earlier comments. Note that I am not arguing against reporting anything; my concern is that any organization on either the originating or receiving end of information can drown in it if the information is not targeted for a specific purpose. And, if a system is vulnerable, and the vulnerability had not been remediated (which may require an architectural change or operational change), if the informa-

tion about HOW the breach occurred is not protected, the company will be more vulnerable.

Clearly, there are occasions in which an intrusion would have larger ramifications than just the effect on the intruded upon entity. For example, if a contractor is developing a new weapons program, and the designs are exfiltrated to a hostile nation state, which renders the value of the weaponry potentially much lower to the Defense Department. You can't have a technical advantage if the technology is used by everybody.

In short, I think "incident reporting" to be successful would need some clear ground rules for both asker and askee to include what types of incidents or intrusions are material and germane.

Question 8. When Request For Proposals (RFPs) are put out for contracts that involve sensitive or classified information do all of these RFPs require that bids include the number of successful and unsuccessful cyber intrusions committed by domestic or foreign entities (either originating domestically or overseas)?

Answer. I am unaware of any such requirements in RFPs.

At the risk of stating the obvious, you can't count unsuccessful intrusions because there are a lot of attempts you cannot necessarily capture. Also, you cannot count the successful intrusions you haven't found yet, either. What would be unproductive is reporting something like "number of port scans" as a proxy for "unsuccessful intrusions" Firewalls get scanned all the time. Having to collect that data and report it doesn't really accomplish anything besides taking a scarce resource (a good security person) and putting them on a reporting function.

By way of example, about 9 or 10 years ago, after Oracle started running an ad campaign entitled "Unbreakable"—the port scans on our firewall (that is, an attempt to look for open ports, perhaps through which to mount an attack) increased by an order of magnitude in just one *week*. We can pretty confidently conclude that the increase in port scans was from hackers who wanted to be the first to break "Unbreakable." Now, there were no actual intrusions but, in the absence of a precise definition, someone could require these port scans to be reported as an "incident." That would not be a productive use of either a reporter's time or the time of an entity on the receiving end, either.

Question 9. In your opinion, if a private company believes that it has been the victim of a cyber intrusion (both originating domestically or overseas), which is the appropriate agency that it should report this intrusion to?

Answer. The FBI. And in fact the FBI does reach out to local businesses in Silicon Valley (and for all I know in other locations) to engage in dialogue. Dong this proactively is better than hoping a company knows to call the FBI.

Question 10. In your opinion, if a government contractor believes that it has been the victim of a cyber intrusion (both origination domestically or overseas), which is the appropriate agency that it should report this intrusion to?

Answer. The FBI.

Question 11. In your opinion, if a government contractor that is working on a sensitive or classified project and believes that it has been a victim of a cyber intrusion (both origination domestically or overseas), which is the appropriate agency that it should report this intrusion to?

Answer. I think the company ought to be doing an investigation on their own first and in fact, most organizations of size DO have (or should have) an incident response protocol which includes a series of decisions as to whether law enforcement should be contacted (regarding an incident) and under what conditions. For example, if a government contractor experienced a website defacement (which is an "incident" under most definitions), does any Federal Government entity really want that reported to them? (Note that a web page for the company as a whole is likely a different area of the network than a classified program.)

This would actually be a good area for industry-government dialogue—under what circumstances would the government want to know of "incidents?"

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO REAR ADMIRAL JAMES BARNETT JR.

Question 1. What about cybersecurity? Are you confident that the everyday American citizen knows the threat that we are under, and knows how to make his or her own home or business safe?

Answer. I believe that the consumers, on the whole, are becoming more aware of the threats that exist when they use the Internet, but there continues to be room for improved education in this area. Polling data, for example, indicates that citizen

awareness is improving. A March 2009 poll conducted by Harris Interactive indicates that online security awareness among adults 18 and over had "grown tremendously in the past 2 years. The study found that 62 percent are more concerned about their online security."

Nevertheless earlier studies identified significant gaps between perceptions and the realities of America's cyber security and are cause for continuing concern. For example whereas 81 percent said they were using a firewall, expert analysis indicated that in reality only 42 percent had a firewall installed on their computer.[1]

Question 2. Should there be basic cyber awareness and education as part of the normal curriculum in elementary and secondary school?

Answer. Yes. Regardless of the environment in which it is taught, our youngest generation needs instruction at the appropriate time by responsible adults who are knowledgeable on these subjects. According to a poll released February 25, "more than 90 percent of technology coordinators school administrators and teachers support teaching cyberethics, cybersafety and cybersecurity in schools. However, only 35 percent of teachers and just over half of school administrators report that their school districts require cyberethics, cybersafety, and cybersecurity in their curriculum."[2] There are also differing opinions "as to who is or should be responsible (parents vs. teachers) for educating students about cyberethics, cybersafety, and cybersecurity. For example, while 72 percent of teachers indicated that parents bear the primary responsibility for teaching these topics, 51 percent of school administrators indicate that teachers are responsible."[3]

Question 3. What must the government do better? What must the private sector do better? What responsibilities do both have to the public at large?

Answer. Concerning educating the everyday American citizen on cybersecurity issues, the government must speak with a single, clear voice. Hence the FCC is committed to working with other Federal agencies to deliver a coordinated message. The Commission has a unique role on the Federal team protecting the critical communications infrastructure against cyber attacks. Thus, the Commission must coordinate its own focus on the cybersecurity of the communications infrastructure with the end-system and standardization cybersecurity responsibilities that have been delegated to DHS, FTC, NIST, and other Federal agencies. Many broadband service providers are to be commended for making "anti-virus" software and services available to their subscribers, frequently free of charge. These providers should take steps to ensure that their subscribers not only are aware of the availability of such software and services, but, through appropriate communications to them, also take steps to ensure that they understand the perils of not taking advantage of these offerings or ones that offer similar protections.

The government and the private sector must also work together to ensure the cyber security of our Nation's critical infrastructures. For example, they must work together to identify and encourage the implementation of standards and best practices that will enhance the security of our systems. In this regard, the Commission's National Broadband Plan recommended that the Commission explore creation of a voluntary cyber security certification program as a mechanism to encourage the implementation of cyber security best practices by communications service providers. The government and the private sector must also develop a partnership that allows for sharing of threat and vulnerability information.

Question 4. With this in mind, how can we fashion a public-private partnership, based on trust, that allows for sharing of confidential and/or classified threat and vulnerability information between the government and critical private sector networks?

Answer. Our experience working with telecommunications carriers on communications outage reporting and vulnerability analysis suggests that this is possible. The recently released National Broadband Plan recommended that the Commission and the Department of Homeland Security's Office of Cybersecurity and Communications should collaboratively develop an IP network Cyber Information Reporting System (CIRS). As envisioned, CIRS would serve as a mechanism by which the Commission could collect situational awareness information from communications service providers and ISPs, during cyber events as opposed to hurricanes and other types of emergencies. Under CIRS, the Commission would act as a trusted facilitator to ensure that any information sharing is reciprocated and structured in

---

[1] 2008 NCSA/Symantec Home User Study, October 2008, *http://staysafeonline.mediaroom.com/index.php?s=67&item=46*.

[2] Cybersecurity, Safety and Ethics Education Falls Short in U.S. Schools, February 2010. *http://staysafeonline.mediaroom.com/index.php?s=43&item=57*.

[3] *Ibid.*

such a fashion that ISP proprietary information remains confidential. CIRS filers may be in a position to report about downstream attacks, *i.e.,* attacks on customers. Accordingly, relevant privacy issues and other details would need to be addressed.

Question 5. Would government and private cybersecurity efforts benefit from "vulnerability mapping" of major U.S. networks, public and private?

Answer. Yes. Vulnerability mapping typically involves identifying weaknesses in the targeted network infrastructure components and their communications protocols. Many of these weaknesses are already well understood and a greater benefit would come from ubiquitous deployment of known fixes and best practices. Naturally, steps would have to be taken to secure this sensitive information.

Question 6. What are the specific risks to such an activity?

Answer. The most obvious risk of vulnerability mapping is a breach in information security whereby an adversary obtains sensitive information about vulnerabilities in our critical communications infrastructure. I believe this risk can be mitigated with proper safeguards, and I further believe that the benefits of vulnerability mapping outweigh the risks. There's little real security to be achieved through obscurity. Any effort relying on security through obscurity—the idea of not drawing attention to a security problem lessens the potential for a security event—assumes that if flaws are not known, that attackers are unlikely to find them. While this notion may be theoretically attractive as a defense in-depth measure, in the real world where we are dealing with multiple vulnerabilities spread across a substantial infrastructure, which is currently the case, this is not a reasonable assumption. Rather, achieving security by design—where concerted efforts are brought to bear on solving a set of vulnerability risks—would make us more secure.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN ENSIGN TO REAR ADMIRAL JAMES BARNETT JR.

Question 1. Are there any legal restrictions we should focus on that make it more difficult for industry and government agencies to share the information needed to protect our critical cyber infrastructure? Are there any bathers that Congress needs to eliminate, or any legal flexibility we can provide to foster the necessary sharing while still protecting sensitive or proprietary information?

Answer. I believe that the Administration's recent *Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure,* to which the FCC contributed, captures well the current state of information sharing between and among industry and government agencies:

"Some members of the private sector continue to express concern that certain Federal laws might impede full collaborative partnerships and operational information sharing between the private sector and government. For example, some in industry are concerned that the information sharing and collective planning that occurs among members of the same sector under existing partnership models might be viewed as "collusive" or contrary to laws forbidding restraints on trade. [For example, the Sherman Antitrust Act, 15 U.S.C. §§ 1–7 (2004)]. Industry has also expressed reservations about disclosing to the Federal Government sensitive or proprietary business information, such as vulnerabilities and data or network breaches. This concern has persisted notwithstanding the protections afforded by statutes such as the Trade Secrets Act and the Critical Infrastructure Information Act, which was enacted specifically to address industry concerns with respect to the Freedom of Information Act (FOIA). Beyond these issues, industry may still have concerns about reputational harm, liability, or regulatory consequences of sharing information. Conversely, the Federal Government sometimes limits the information it will share with the private sector because of the legitimate need to protect sensitive intelligence sources and methods or the privacy rights of individuals.

These concerns do not exist in isolation. Antitrust laws provide important safeguards against unfair competition, and FOIA helps ensure transparency in government that is essential to maintain public confidence. The civil liberties and privacy community has expressed concern that extending protections would only serve as a legal shield against liability. In addition, the challenges of information sharing can be further complicated by the global nature of the information and communications marketplace. When members of industry operating in the United States are foreign-owned, mandatory information sharing, or exclusion of such companies from information sharing regimes, can present trade implications."

[Obama Administration, *Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure,* May 29, 2009, p.18]

Question 2. What mechanisms are in place for private companies to report cyber intrusions (either originating domestically or overseas) to the Federal Government?

Answer. The FCC currently has rules that require communications providers to report disruptions to circuit-oriented infrastructure and wireline and wireless switched-voice services. Thus, if a cyber intrusion resulted in a circuit-oriented or switched-voice communications service outage that meets certain thresholds, the communications provider must report the outage and the root cause to the FCC. These rules generally cover legacy communications systems and do not cover Internet Protocol (IP)-based communications infrastructure. To address this, the National Broadband Plan proposed that the Commission initiate a proceeding to expand these outage reporting rules to broadband Internet service providers and to interconnected voice over 1P service providers.

In addition, the National Broadband Plan recommended that the Commission and the Department of Homeland Security's Office of Cybersecurity and Communications collaboratively develop an lP network Cyber Information Reporting System (CIRS) somewhat as an analog of the FCC's Disaster Information Reporting System (DIRS). Specifically, the National Broadband Plan states that "CIRS will be an invaluable tool for monitoring cybersecurity and providing decisive responses to cyber attacks.

ORS should be designed to disseminate information rapidly to participating providers during major cyber events. CIRS should be crafted as a real-time voluntary monitoring system for cyber events affecting the communications infrastructure. The FCC should act as a trusted facilitator to ensure any sharing is reciprocated and that the system is structured so ISP proprietary information remains confidential." *National Broadband Plan,* Recommendation 16.8 (available at *http://www.broadband.gov/plan/16-public-safetyntr16–1*).

Question 3. What is being done to encourage private companies, particularly those with government contracts, to report cyber intrusions (either originating domestically or overseas)?

Answer. The packet-oriented infrastructure and packet-switched services such as Internet access are much more susceptible to outages caused by cyber incidents. The FCC has engaged in collaborative efforts with industry, including Internet Service Providers, to enhance industry's own ability to prevent and respond to cyber events through Federal advisory committees, which include private sector representatives. There are currently no requirements for reporting packet-switched service outages or their causes, which would include cyber incident causes.

The FCC's National Broadband Plan has recommended that the Commission's Part 4 outage reporting rules be expanded through a rulemaking proceeding to include ISPs and interconnected VoIP service providers. The Commission would seek comment about reported "causes" and thresholds for reportable events. As with the data received pursuant to the Commission's circuit-oriented outage reporting rules, ISP and VoIP outage data would be analyzed and used to support cooperative efforts with industry to improve security and reliability.

Question 4. Do government contractors have an ethical or statutory obligation to report cyber intrusions (either originating domestically or overseas)?

Answer. We are not aware of any code of ethics or statutory obligation that requires government contractors to report cyber intrusions. Although the Federal Acquisition Regulation (FAR) requires contracts over $5 million to include a clause requiring the contractor to establish a written code of business ethics and conduct, there is no FAR requirement that such codes address the subject of cyber intrusions. FCC Directive 1479.3 (mentioned in the response to question 5), which is included in a small number of FCC IT contracts, requires reporting of "security incidents" regarding FCC IT systems.

Question 5. Do government contractors with classified information on their servers and individuals with security clearances on their payrolls have a statutory or ethical obligation to report cyber intrusions (either originating domestically or overseas)?

Answer. Under the National Security Act, government contractors and their employees with security clearances have a statutory obligation to protect the classified information that comes into their possession. This requires the same reporting of cyber intrusions into systems that involve sensitive information as fall to government employees.

Question 6. When Request For Proposals (RFPs) are put out for contracts that involve sensitive or classified information do all of these RFPs require that bids include the number of successful and unsuccessful cyber intrusions committed by domestic or foreign entities (either originating domestically or overseas)?

Answer. The FCC's information technology contracting procedures require contractors to comply with the security matters addressed in FCC Directive 1479,

which "establishes policy and assigns responsibilities for assuring that there are adequate levels of protection for all FCC information systems, the FCC Network, applications and databases, and information created, stored, or processed therein."

A requirement that the vendor report the number of successful and unsuccessful cyber intrusions is not a standard feature of FCC contracts for information technology systems. However, under current procedures this requirement could be included in the language for those contracts for systems that involve sensitive information at the discretion of the Contracting Officer. The nature of Internet-based cyber attacks is such that careful attention would have to be given to specifying definitions, thresholds and suspected origination of cyber intrusions.

Question 7. In your opinion, if a private company believes that it has been the victim of a cyber intrusion (both originating domestically or overseas), which is the appropriate agency that it should report this intrusion to?

Answer. If a cyber intrusion results in circuit-oriented or switched-voice communications service outages that meet certain thresholds, then the communications provider must report the outage and the root cause (*i.e.,* the cyber incident) to the FCC in accordance with Part 4 of our regulations. As noted above, the FCC's National Broadband Plan has recommended that outage reporting rules be expanded to include ISPs and interconnected VoIP services through a rulemaking proceeding.

More generally, as the GAO has noted, where criminal activity is involved "the Departments of Justice (DOA Homeland Security (DHS), and Defense (DOD), and the Federal Trade Commission (FTC) have prominent roles in addressing cybercrime within the Federal Government. DOD's FBI and DHS's U.S. Secret Service (Secret Service) are key Federal organizations with responsibility for investigating cybercrime. State and local law enforcement organizations also have key responsibilities in addressing cybercrime."

[*Cybercrime—Public and Private Entities Face Challenges in Addressing Cyber Threats*, June 2007, GAO–07–705, p.1]

Question 8. In your opinion, if a government contractor believes that it has been the victim of a cyber intrusion (both origination domestically or overseas), which is the appropriate agency that it should report this intrusion to?

Answer. In my opinion a government contractor should—unless the applicable contract otherwise provides—first report a cyber intrusion to the contracting agency; for example an FCC contractor should report a cyber intrusion to the FCC. If criminal activity is suspected, then the FCC will report the intrusion to the agency or agencies that investigate cyber crime within the Federal Government, such as the Departments of Justice and Homeland Security.

Question 9. In your opinion, if a government contractor that is working on a sensitive or classified project and believes that it has been a victim of a cyber intrusion (both origination domestically or overseas), which is the appropriate agency that it should report this intrusion to?

Answer. Unless the governing contract otherwise provides, a government contractor should first report a cyber intrusion involving sensitive or classified information to the contracting agency. If criminal activity is suspected, then the agency should report the intrusion to the agency or agencies that investigate cyber crime within the Federal Government, such as the Departments of Justice and Homeland Security.

○