S. HRG. 111–43

CYBERSECURITY: ASSESSING OUR VULNERABILITIES AND DEVELOPING AN EFFECTIVE RESPONSE

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MARCH 19, 2009

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

U.S. GOVERNMENT PRINTING OFFICE

50–638 PDF WASHINGTON : 2009

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

FIRST 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
JOHNNY ISAKSON, Georgia
DAVID VITTER, Louisiana
SAM BROWNBACK, Kansas
MEL MARTINEZ, Florida
MIKE JOHANNS, Nebraska

ELLEN L. DONESKI, *Chief of Staff*
JAMES REID, *Deputy Chief of Staff*
BRUCE H. ANDREWS, *General Counsel*
CHRISTINE D. KURTH, *Republican Staff Director and General Counsel*
PAUL NAGLE, *Republican Chief Counsel*

CONTENTS

WITNESSES

APPENDIX

CYBERSECURITY: ASSESSING OUR VULNERABILITIES AND DEVELOPING AN EFFECTIVE RESPONSE

THURSDAY, MARCH 19, 2009

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

The Committee met, pursuant to notice, at 10:02 a.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. Good morning, everyone. We have a full quorum present, so we're able to start this hearing.

Good morning, Senator Cantwell.

It's interesting to me, there are 10,000 other Committees meeting, and I hope the witnesses understand that. Nobody ever said we were a sane institution, but we prove it, particularly in the early times, like this, when we're trying to confirm people, and there are too many hearings, and people have to run back and forth, and we've got four votes sometime this morning. Anyway, I'm very glad that you're all here.

I was Chairman of the Intelligence Committee, so I'm familiar with the Nation's cybersecurity threats and vulnerabilities. And what I'd like to say is, very powerful, at least to me. In the last 2 years; under two administrations, two Directors of National Intelligence, before an open world-threats hearing, which is an annual event in which all the Intelligence Committees sort of bring their work together, Mike McConnell, under President Bush, and Admiral Blair, under President Obama, both said that the number-one security threat to the United States of America was cybersecurity, or cyberterror, however you want to phrase it. I regard it as a profoundly and deeply troubling problem to which we are not paying much attention. We have jurisdiction—part jurisdiction in this committee. As do others, obviously. This is not going to be the last of our hearings on this subject; we're going to pursue this subject further.

The problem is, America is unacceptably exposed to massive cybercrime, global espionage, and potential cyberattacks that would very easily cripple our infrastructures. Anyone, anywhere, can launch a cyberattack, for as long as the Internet or other like instruments exist.

We currently have in place very sophisticated systems to protect against cyber espionage, but it's very important for people to know that cybersecurity is not just about protecting our government networks from countries, terrorists, or hackers who want our secrets. It's about protecting our Nation's critical infrastructure from cyberattacks that could severely impact commerce and the economy in absolutely devastating ways. People just don't stop to think about it, don't know about it, don't care about it, don't know what the word means.

For example, private-sector IT systems control virtually all of this critical infrastructure; traffic lights, rail networks. It would be very easy to make train switches so that two trains collide, affect or disrupt water and electricity, or release water from dams, where the computers are involved. How our money moves, they could stop that. Any part of the country, all of the country is vulnerable. How the Internet and telephone communication systems work, attackers could handle that rather easily. If healthcare reform is successful, this is something which is just mind-boggling to me, IT systems will play a critical role in the future of healthcare and will be at risk as well. They can take an IT system and do what they want with it. I'm not sure if they can change prescriptions that doctors prescribe, but I think they can. I know that they can send you to the wrong doctor or cancel your appointments. Attackers can just take things that we do on a common everyday basis, and could wreak havoc, and get into the minds of the American people.

I've always believed that, with all the tragedy of 9/11, that Al Qaeda does not necessarily exist just to bring down tall buildings, but to get into the minds of the American people and to bring them to their knees out of fear as a result of something happening in a small place, or it was prosaic event, but it was crushing and people panic. When Americans panic, not very good things happen.

So, we need to get private-sector leaders and government authorities on the same page on this enormous threat. We cannot do this soon enough. We need a coordinated public-private response. Currently, this does not exist.

President Obama talked about having a cybersecurity advisor. That has not happened.

In broader terms, I think that the homeland security part. This is sort of strange to say, but here we are, fighting in Iraq and Afghanistan, and potentially in other places, disruption is with us for years and years to come, and the wars aren't the point. These cyberattacks can come from anywhere. We tend to say, "Well, what country do they come from?" And people say, "Well, it's China." They say, "It's Russia." Estonia and Latvia both had their power systems shut down. Attackers can disrupt systems for a very short time, they don't have to do it for a week, they could do it for a day and a Nation or a country goes into panic.

The point is that anybody, some kid in Malawi, some kid in the southern tip of Chile who's just mad, can do this. They can and have figured out how to do it. We see regularly on television the TV ad that the Department of Defense is being hacked into, 3 million times a day. My honest assessment is that most Americans see that, don't believe it. The number is too big, and, "Oh, by the way,

it's the Department of Defense, it's not me," is the sort of response that goes on.

There's this monumental disconnect between the American people in many cases, the private sector, and protecting ourselves. Being aware of, getting ready for, being ready to respond to cyberattacks.

How's a small business going to do this? How are they going to know about it? How are they going to afford to figure out what to do? The bigger businesses are pretty good at it, but there are a lot of bigger businesses that aren't very good at it at all. Because the times are rough, and they figure there are other things to do and it won't happen to them, which is they classic American psyche, anyway.

I just want to put myself down as somebody who is very concerned and is determined to make a difference in this Committee on this subject. I've pushed for a national security advisor who reports directly to the President, who would coordinate such an interagency and public-private effort. How do you do that? Well, you've got to have backup groups, advisory groups. And we'll have to do that.

This is not just about providing a new powerful government official, a tsar or anything like that, it's about transforming the way the government, private sector, and the American people tackle something called cyberterrorism, cyberattacks, as a problem, and do it together.

I went over my time, Senator Cantwell, and I apologize, as I do to you, Senator Udall.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman. And thank you for holding this important hearing. I know that your passion and understanding of these issues comes, not just form this Committee, but your former chairmanship of the Intelligence Committee, so we appreciate you calling together such a distinguished group of witnesses. I look forward to hearing their discussion, particularly from Dr. Lewis and Dr. Weiss, about the electricity grid and the security issues related to the electricity grid, and how we move forward with technology that can help us, both on efficiency and security. So, I look forward to those comments.

I look forward to your continued leadership, Mr. Chairman, on this issue with this Committee, from the perspective of continuing to move forward on technology, but to make sure that security concerns are addressed.

And so, I'll stop with that and have questions for the witnesses, but thank you, again, for holding this important hearing.

The CHAIRMAN. Thank you very much.

Senator Udall?

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

Senator UDALL. Thank you very much, Chairman Rockefeller. I, also, want to echo what Senator Cantwell said. I think we're very lucky to have you as Chairman, and this expertise that you've de-

veloped over time as chairman of the Intelligence Committee, I think, is going to be shown here today. It's an honor to be here and be serving with you. Thank you for your dedication.

I come from a State that has two great national laboratories: Los Alamos National Laboratory and Sandia National Laboratories. They work somewhat in both of these areas. So, as you proceed with your testimony addressing these very important issues, I'm going to be asking about the kinds of research you think should be done, either in national laboratories or at academic institutions. It seems to me, at least from what I've learned, talking with our chairman, is that we really need to be ahead of the curve, we need to be out in front of this. Where is it that we generate the new knowledge and getting out on the cutting edge? So, that's going to be one of the things that I talk about.

I also know that there has been some suggestion in your testimony that we collaborate with other countries. And yet, there are dangers in collaborating, and I think, with several of you, I would like to explore that interaction that's there, because clearly it—from my travels, anyway, countries insist that we collaborate, but, at the same time, I know that there are serious issues also facing that particular area.

So, thank you very much for being here, and I'm going to shorten my statement and make sure that we get, Chairman Rockefeller, quickly to the witnesses.

The CHAIRMAN. Good. Incidentally, this is not an Intelligence hearing, this is a Commerce Committee hearing. Every single thing that we're going to talk about here has to do with commerce.

We have a very distinguished panel. We have Dr. James Lewis, Director and Senior Fellow of the Technology/Policy Program with the CSIS, which I don't have to spell out; Dr. Joseph Weiss, Managing Partner for Applied Control Solutions; Dr. Ed Amoroso, who is Chief Security Officer at AT&T, they know something about this. He'll discuss cybersecurity from a network operator's perspective. And Dr. Eugene Spafford, Professor and Executive Director of the Purdue University, Centers Education and Research and Information Assurance and Security. That's a heck of a letterhead.

[Laughter.]

The CHAIRMAN. Dr. Lewis?

STATEMENT OF DR. 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 thank the Committee——

The CHAIRMAN. Yes, it should be sort of an orange.

Dr. LEWIS. OK, I guess it's on. Well, that was a good start.

Thank you. And I thank the Committee. Your opening remarks were, I think, exactly on target.

The nature of our dependency on cyberspace is not always recognized, although I have to say you've recognized it. We tend to think of it is a military or homeland security problem, but the primary vulnerability in cyberspace is economic.

In the 1990s, there was a debate over the value of information technology, and some people said, "We're spending all this money,

and we don't see any return." By the end of the 1990s, the debate was over. There was conclusive evidence that information technology spurred growth.

Why was there a delay? The delay was because there was a lag between the time people bought it and the time they figured out how to use it, how to apply it in new ways, how to reorganize.

Just as companies had to change how they operated and were organized, we must now change the Federal Government. It's no surprise that adjustment takes time, but in this case, the problem is compounded by the nature of the technology.

The Internet was designed to provide survivable communications based on rapid and easy connectivity. It's optimized for easy connection. It's built on implicit trust. It has changed the world, but it is deeply flawed. That flaw is security.

As the Internet is now configured and governed, it cannot be secured. Right now, the attackers have the advantage in cyberspace. As a Nation, we have not brought the full power of the Federal Government to overcome this advantage.

Now, on the bright side, the U.S. has done more than other countries when it comes to cybersecurity. There has been much progress in the last 2 years compared to the previous decade. And the Obama Administration has identified cybersecurity as an important issue for national security.

But, while the United States has done more than other countries, we also have more to lose. The risk is not what some cybersecurity proponents would tell you. We're not talking about explosions or mad hackers or bringing the U.S. to its knees in a few hours. The real risk lies in the long-term damage to our economic competitiveness and our technological leadership.

Cyberconflict can disrupt key services, as you mentioned, as in the case of an opponent who can access control systems. I'm sure we'll hear more about that today. But, the real and immediate damage comes from the theft of intellectual property and the loss of advanced commercial and military technologies to foreign competitors.

Cyberconflict is well suited to providing a competitive edge to other nations. In this competition we are in now, economic strength, technological leadership, and the ability to innovate is as important as military force for national power. A failure to secure America's information infrastructure weakens the United States and makes our competitors stronger.

Changing this requires two sets of actions. The first is to strengthen our national ability to innovate; the more innovative nation is more secure. The second is to secure the networks upon which we rely.

Let me give you two examples, quickly, of the connection between cybersecurity and the economy:

The stimulus bill provides a significant increase in funds for research. This will improve U.S. competitiveness. But, if that research is conducted over insecure networks, we are subsidizing, not only our own industry, but foreign industry, as well.

The Smart Grid that is also in the stimulus bill makes innovative use of advanced technologies to address energy problems, but

if the Smart Grid is not secure, it can be hacked and used to disrupt the delivery of electricity.

In the past, we've viewed cybersecurity as a technical problem. This was a mistake. Cybersecurity requires using all the tools of U.S. power—diplomatic, military, intelligence, enforcement—law enforcement and economic policy. CSIS put out a report in 2008 that laid out a comprehensive strategy. But, more than a comprehensive, a strategy will also need to be coordinated.

Cybersecurity requires actions by many agencies, and our current efforts are not sufficiently coordinated to provide advantage, although the Obama Administration's 60-day review may change this.

Congress can focus Federal efforts on the economic risk, and it can ensure that regulatory efforts by agencies give full weight to cybersecurity, something that is not now the case. It can ensure that the Department of Commerce, which has a key role in this, makes cybersecurity a priority.

Finally, Congress can tackle the daunting task of modernizing our legal authorities, many of which were written for technologies that were in use decades ago.

My testimony has discussed how information technology has brought great benefits, but that these are accompanied by unavoidable risks. We have an opportunity to secure cyberspace and use it to renew economic growth, create more efficient government, and build stronger national security. These are attainable goals, and the Nation that finds new ways to use cyberspace securely will gain competitive advantage.

I thank the Committee for its attention, and I'll be happy to take any questions.

[The prepared statement of Dr. Lewis follows:]

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

I thank the Committee for the opportunity to testify on vulnerabilities and effective defense in cyberspace. As America's dependence on cyberspace grows, and as the scale and pace of conflict in this new venue increases, the need to rethink national strategies has become urgent. The free and secure use of cyberspace has become, like freedom of the seas, a vital national interest for the United States. This Committee can play an important role in developing and guiding an adequate national approach to securing cyberspace.

The nature of our dependence on the use of cyberspace is not always recognized. We tend to think of cybersecurity in military terms, or as a problem of homeland security, but this is inadequate for understanding the scope of the problem. Networked, digital information technology provides the infrastructure for news ways to organize, interact and create wealth—actions that can now take place in cyberspace. Information technology lies at the center of an immense and ongoing transformation in the global economy, in politics and society, and in military affairs. It has transformed how people work, altering business models, supply chains, customer interactions and production. The use of cyberspace has become a central element in both economic and national security.

You may recall that in the early 1990s, there was a debate over the value of investing in information technology. Some economists noted that American companies had spent millions of dollars on information technology without any noticeable gains in productivity. The promise of information technology, they asserted, was a mirage. The excesses and rhetoric of the *dot.com* bubble only contributed to this perception.

But by the end of the 1990s, this debate was over. There was conclusive evidence that spending on information technology brought economic benefit. Information technology made a significant contribution to American GDP growth—perhaps as

much as a third of total GDP growth. It turned out there was a lag, a delay between spending on IT and the increase in growth. The reasons for this delay were that companies had to figure out how to change their organizations and their business practices to take advantage of the new and more efficient processes enabled by IT. New technology layered over old organizations does not provide much benefit.

We can draw two conclusions from this story. First, we are barely into our second decade when it comes to exploiting the advantages that digital network technologies provide. If this story was about cars, we have moved from the Model T, introduced in 1908, to the Model A, which appeared in 1927. This is progress, to be sure, but we are only at the beginning of the story. We have not exploited the full potential of the new technology for recovery and for future growth.

Second, just as there was a lag as companies took time to adjust how they operated and were organized to make use of the new technologies, we are facing a lag in adjusting law, regulation and policy. To continue the car analogy, if the economy as a whole is moving toward the Model A, the Federal Government is still comfortable driving a Model T. The difficult task of modernizing the Federal Government will challenge both the administration and the Congress.

A common element links both business and governmental stories together. That element is security. It is no surprise that a new technology that has immense economic and political effect requires adjusting our security policies, and that we have lagged in doing so, but in this case, the problem is compounded by the nature of the technology itself.

The story of the Internet is well known. It was designed to provide survivable communications based on rapid and easy connectivity across a nation-spanning network. Its initial users were scientists and military officials, small communities that knew and could trust each other. The Internet is an open network optimized for easy connection and built on implicit trust. It has changed the world, but it is also deeply flawed. That flaw is security.

The Internet as it is currently configured and governed cannot be fully secured. Changing this to gain the further advantages offered by information technology will require a restructuring of governance, practices and standards. Right now, however, the advantage lies with the attacker. This has been apparent for years, but as a nation, we have not brought the full power of the Federal Government to bear on the problem, and what power we did bring was applied in a fragmented and incoherent manner.

This is a harsh statement, and if it is any consolation to the Committee, the United States has done a better job than any other country in cybersecurity. The last twelve months have seen more progress toward securing cyberspace than any previous year. More importantly, the Obama Administration has identified cybersecurity as one of the most important issues for national security and has begun to move forward.

However, we should bear in mind that while the United States has done more than other nations in terms of security, this is in no way adequate. One reason for this can be termed asymmetric vulnerability. We have more to lose than our opponents do. We are more reliant on information technology and networks and it is a greater source of our comparative advantage in economic competition and in national security. As a nation, we have been quicker to take advantage of the Internet and offer a "target-rich" environment to our opponents, who currently rely on it less.

Over time, this will change. No country can ignore the benefits of digital networks if it wishes its economy to be competitive, its researchers effective and its nation to be secure. In the interim, however, the United States is at greater risk than any other country. The risk is not what some cybersecurity proponents would have you believe. We are not talking about explosions, mad hackers, fatalities, or bringing the United States to its knees in a few hours. These claims are best left to Hollywood—entertaining, but a poor guide for policy. The real risk lies in the long-term informational damage to our economic competitiveness and technological leadership.

Our primary opponents in cyberspace—and we are already in a conflict even if it often takes place largely outside of public view—are nation-states and organized criminals (who sometimes work at the behest of nation state). Cyber conflict involves illicit action to penetrate computer networks. These penetrations may provide an opponent the capability to disrupt the delivery of key services, as in the case of an opponent who surreptitiously accesses the control system of a critical utility or network. This potential threat is one that we need to guard against. The real and immediate threat from conflict in cyberspace, however, is illicit action to obtain access to sensitive information—in other words, espionage and theft.

That cyber incidents are not comparable to attacks involving the use of force does not mean that they are not damaging. Clearly, there are potential military advantages that come from greater knowledge of an opponent's intentions and capabilities,

access to critical military technologies, and the ability to disrupt and slow decision-making by introducing uncertainty provides immediate advantage. Action in cyberspace has become part of modern warfare.

More importantly, cyber conflict is well suited to producing national advantage in the new kinds of competition that will shape international relations in the future. In this competition, military forces are only one source of power. Economic strength, technological leadership and the ability to innovate will be as important as military force in creating national power, particularly in competition with the rising nations who wish to reduce U.S. influence without resorting to open military conflict. The primary damage to U.S. national security and economic strength from poor cybersecurity comes from the theft of intellectual property and the loss of advanced commercial and military technology to foreign competitors. A failure to secure America's information infrastructure weakens the United States and makes our competitors stronger.

2007 was perhaps the worst year for the United States when it comes to cybersecurity—it may have been the long-awaited Electronic Pearl Harbor, despite the lack of explosions or casualties. The Secretary of Defense's unclassified e-mail was hacked. The Department of Commerce's bureau for high tech trade had to go offline after its networks were penetrated. Foreign entities penetrated the networks of the Departments of State and Energy, NASA and other Federal agencies, along with networks at Federal contractors, the defense industry and major companies. It is interesting to note that in the same period the governments of the United Kingdom, France and Germany also experienced major cyber incidents, which they attributed to China.

In response, the Bush Administration created the Comprehensive National Cybersecurity Initiative (CNCI). While the initiative made progress in securing Federal networks, the CNCI had major drawbacks. It started too late, in the last year of the Bush Administration. It was over-classified. Most importantly, despite its name, the Comprehensive National Cybersecurity initiative was not comprehensive. The CNCI focused on government networks, and while this is important, it is inadequate. Cyberspace is a global commercial network. The CNCI did not have an international component, it did not adequately address how to secure critical infrastructure, and it ignored the "dot.com" space where most commercial activity takes place. These were serious shortcomings, and they point to crucial areas for work for the new Administration.

Despite the CNCI, intense economic espionage made possible by the Internet is eroding America's technological leadership and economic strength. Repairing this situation requires two interrelated sets of actions. The first is to strengthen our national ability to innovate. Innovation is the process of coming up with news ideas, goods, and services. It has become a central element in economic competition. A more innovative nation will be stronger and more secure as it will have a stronger economy and better technology. A purely defensive strategy will not succeed. The second set of actions is to secure the networks upon which we rely for commerce, innovation and security. Two examples help demonstrate how these actions are related.

There is a strong connection between innovation and information technology. Information technology lowers the cost of acquiring information and creating new knowledge. It extends human capabilities to count and observe. Digitizing knowledge and research increased the productivity of the innovative efforts. Recognizing that research is a fundamental source of innovation, the recent stimulus bill provided a significant increase in funding for research in the hopes that this would increase innovation in the United States and with it, growth and competitiveness. This is a good idea, but there is one important caveat to bear in mind. Much of the new information created by the additional funding for research will be stored in computer databases. These databases are usually networked and connected to the Internet. That means they are vulnerable to penetration and the information stored on them accessible by others. The end result, if we do not improve cybersecurity, is that new Federal funding to increase research and innovation will be a subsidy to foreign industry as much as our own.

Another stimulus-related problem involves an infrastructure project, the Smart Grid. Smart Grid makes innovative use of advanced meters to better manage the flow of electricity. These new meters use computer technologies to make our national electrical network more efficient. Unfortunately, if the new "smart" meters are not secure, they can be "hacked," taken over by attackers, and used to disrupt the delivery of electricity. If the Smart Grid is built to existing standards, however, it will not be secure. Worse, the United States does not have a process that could deliver in a timely fashion the new standards needed to guide the construction of

secure Smart Grids. Years of under-investment in infrastructure have put us in this unfortunate situation.

These two examples show how recovery and growth, innovation and cybersecurity are intertwined. In the past, we viewed cybersecurity as a problem somehow separate from larger national issues, something that could be safely ignored or left for consideration by technical experts. This is no longer the case. Since the information infrastructure is now a central pillar of our economy and since the untrammeled use of cyberspace is crucial for economic and military security, we cannot ignore it nor can we approach it as a technical problem. An effective policy for this complicated strategic problem will engage many different elements of the American government and requires using all the tools of U.S. national power—diplomatic, military, intelligence, law enforcement and economic policy. A national strategy that does not take a comprehensive approach will fail—we have learned the hard way, this from the experience of our previous national efforts, in 1998, 2003, and 2007.

CSIS established a Commission of recognized experts in 2007 to look at what actions the Federal Government could take to improve cybersecurity. The Commission released its report in December 2008. The report laid out the elements of a comprehensive strategy. This recommended strategy called for better integration of offensive and defensive capabilities to create new modes of deterrence. It recommended expanded international engagement to establish norms and partnerships for securing cyberspace. It concluded that a voluntary, industry led approach to national security was insufficient and concluded that the Federal Government must require mandatory action to improve cybersecurity. It called for improving our ability to authenticate digital identities. Finally, the report determined that the United States needs a coherent and comprehensive organizational and policy framework to secure cyberspace.

Reorganizing government and adopting new practices to enable and secure the use of cyberspace is one of the most difficult tasks in this comprehensive approach. The United States will require a coordinated effort by many agencies. We do not currently have a mechanism to do this, although the sixty-day review of cybersecurity policy the Obama administration is undertaking may provide one. None of the problems we face in cyberspace are unsolvable, but they require a comprehensive approach that has not been used in the past. In the litany of errors and omissions that accompanies any account of previous U.S. cybersecurity policies, the failure to seek broad international engagement or to use the regulatory powers of the Federal Government head the list (along with disorganization and diffusion of effort). You have an opportunity to change this, working with the Executive Branch and the private sector.

One important contribution that Congress can make is to ensure that a national approach to securing cyberspace is forward looking. Congress can focus Federal efforts on the importance of the economic and commercial aspects of cybersecurity, and ensure that the regulatory efforts of important agencies like the Federal Communications Commission give full weight to cybersecurity—something that is not now the case. It can ensure that elements of the Department of Commerce which have crucial roles in securing cyberspace—the National Institute of Standards and Technology and the National Telecommunications and Information Administration—make security a priority. Finally, one of the most daunting tasks before Congress lies in modernizing the range of legal authorities concerning privacy, security, infrastructure protection and the management of digital identities, many of which were written decades ago for simpler technologies and times.

In considering these issues, it is worth recalling that the United States has used a market-led approach to cybersecurity for more than a decade. It has failed us. The CSIS Commission report concluded that market forces alone would not provide adequate national security. This is a major departure from previous thinking, which tended to approach the question of regulation timidly and to defer to business interests on matters of national security. Badly designed regulation is a hindrance but no regulation in situations where there is market failure is even worse. The CSIS Commission proposed a new regulatory approach based on standards and an avoidance of prescriptive rules. The Commission's recommendation is to begin with regulation for critical infrastructure—if infrastructure is truly critical, we should not be shy about mandating action to secure it.

My testimony has attempted to show that information technology has brought great benefits, but that these are accompanied by unavoidable (albeit smaller) costs that we have not done well in managing. Our goal is to take the open network we have inherited and sufficiently secure it to provide renewed economic growth, more efficient government, and stronger national security. These are attainable goals, and the Nation that finds new ways to use cyberspace securely will gain competitive ad-

vantage. With a unified and forward-looking effort, that nation can be the United States.

I thank the Committee for the opportunity to testify and will be happy to take any questions.

The CHAIRMAN. Thank you very much, Dr. Lewis.

Dr. Weiss is next.

STATEMENT OF DR. JOSEPH M. WEISS, MANAGING PARTNER, APPLIED CONTROL SOLUTIONS

Dr. WEISS. Good morning, Mr. Chairman and Members of the Committee. I would like to thank the Committee for your commitment to a comprehensive examination of the cybersecurity of control systems utilized in our Nation's industrial infrastructure, and what can be done to secure them. I also want to thank you for the opportunity to be here today to discuss this very important topic.

And I'd like to make one other point. What I think is more important is not so much cybersecurity, but critical infrastructure protection; whether the computer is working, we need to make sure the system and the processes work.

I am a nuclear engineer that has been involved in control systems for over 35 years, and control-system cybersecurity since 2000. My focus has been on developing an understanding of the complex technical and administrative issues associated with cybersecurity of control systems and how they are different than for corresponding business information-technology systems.

I've also been working with government organizations, end users, equipment suppliers, domestic and international standards organizations, national laboratories, including Sandia and Los Alamos, and others, to develop standards and solutions.

The convergence of mainstream IT and control systems requires both IT and control-system expertise, which is why I'm so glad you've invited me, so we can have a seat at the table.

One should view current control-system cybersecurity as where mainstream IT was 15 years ago. It is in the formative stage and needs support to leapfrog the previous IT learning curve.

Control systems are a system of systems. While sharing basic constructs with IT systems, control systems are technologically, administratively, and functionally different than IT, and this will have a significant effect on the Smart Grid.

Vulnerability disclosure philosophies are different, and can have devastating consequences to critical infrastructure. A major concern is that there are very few control-system cyberexperts. I believe, less than 100—with no formal university curriculum——

The CHAIRMAN. Could you repeat that, the first——

Dr. WEISS. Yes.

The CHAIRMAN.—part of the sentence?

Dr. WEISS. I believe there are less than 100 people worldwide who truly know and understand control-system cybersecurity. And I can elaborate more, if you like.

The CHAIRMAN. No.

Dr. WEISS. And one of the things we do not have is any formal university curricula. We also have no certifications. I happen to have a professional engineering license. There are no questions

whatsoever on security. The CISSP has no questions dealing with control systems. We're in the cracks.

And what's more, the lack of control-system security expertise extends into the government arena, which is focused on repackaging IT solutions that don't address the actual control-system cyberevents that have occurred to date.

The issue at hand is the protection of the interdependent critical infrastructures of electric power, water, oil, gas, et cetera. In fact, before I came here, the Federal Aviation Administration asked me to stop by and talk to them.

Control systems form the backbone of these infrastructures, and the threat of a cyberattack is the central issue. I believe the threat is increasing, not only because of nation-state threat, which is probably what you're used to, but because the economic downturn has created many disgruntled, but knowledgeable, antagonists. Examples of this are the wireless hack in Australia in 2000, where a sewage discharge valve was opened. A disgruntled employee for a federally owned canal system in California installed software that damaged a computer used to divert water out of a local river. And literally in yesterday's newspaper, in L.A. they indicted a disgruntled engineering technician who disabled the leak-detection system for three oil derricks off the coast of Southern California. This was yesterday.

There are only a handful of control-system suppliers, and they supply applications worldwide. The control systems architectures and default passwords are common to each vendor. Consequently, if one industry is vulnerable, they all could be.

The result of a coordinated cyberattack on any or some combination of the critical infrastructures could be devastating to the U.S. economy and security. We're talking months to recover. We're not talking days.

It's an international problem, as North American control-system suppliers provide systems globally, and non-North American suppliers provide systems to North America. A number of suppliers have source code development activities in countries with dubious credentials.

The concern is real. There have been more than 125 control-system cyberincidents I've been able to document, and they've occurred in electric power, in transmission distribution, power generation, including fossil, hydro, gas turbine, and nuclear plants. They've also occurred in water, oil, gas, chemicals, paper, and agribusiness. The impacts have ranged from trivial to significant environmental damage to significant equipment damage to deaths. We've already had a cyberincident in the United States that has killed people.

The following recommendations provide steps to improve the security and reliability of these critical systems:

First, understand the unique control-system cybersecurity issues against all threats, intentional and unintentional. And part of that also includes, not just the threats you'd think of, we're also talking about things like EMP, electromagnetic pulse, and other types of events. These have actually affected control systems already.

Another one that may sound trivial but is terribly important, and that's, How much is—how much security is enough security? We

don't know. We need to develop control-system unique solutions, policies, and training based on actually control-system cyberincidents. We have not yet connected the dots, and we're starting to see similar events in similar locations.

And for control systems, the U.S. CERT and the ISACs, you know, the Information Sharing and Analysis Centers, do not work for information sharing on control systems. We need an information-sharing mechanism staffed by vetted control-system experts. And I use the word "vetted" because, in the commercial world, having a clearance doesn't help, and often can hurt. It's very different. And we do need regulation. And I can tell you what I believe the regulation should be, and especially since you're Commerce.

The CHAIRMAN. You mean "vetted" is dangerous because that——

Dr. WEISS. No, clearances are dangerous.

The CHAIRMAN. OK.

Dr. WEISS. For the—not for Department of Defense applications, but for commercial industry.

But, what we need going on is regulation, and the regulation is to mandate the NIST standards, and that's why, to me, this is so important. You're Commerce. You have NIST. I was part of the team that extended NIST SP 800–53 to address control systems, and we actually used that to look backward in time at actual control-system cyberevents to make sure it worked.

And one other thing I should mention, one of the things control systems do not have to date: forensics. We don't really have a way of going back and analyzing control-system cyberincidents. We have to read between the lines.

And finally, we need education and certifications that are unique to the control-system world, so we have some confidence that what is being done is being done by people who know and understand the situation. And, as I mentioned before, we've fallen between the cracks, and we really are looking for your help. We feel this is important, and we need your help.

Thank you, and I look forward to taking questions.

[The prepared statement of Dr. Weiss follows:]

PREPARED STATEMENT OF DR. JOSEPH M. WEISS, MANAGING PARTNER, APPLIED CONTROL SOLUTIONS

Good afternoon, Mr. Chairman and Members of the Committee. I would like to thank the Committee for your invitation to discuss the current status of cyber security of the control systems utilized in our Nation's critical infrastructure.

I am a nuclear engineer who has spent more than thirty years working in the commercial power industry designing, developing, implementing, and analyzing industrial instrumentation and control systems. I have performed cybersecurity vulnerability assessments of power plants, substations, electric utility control centers, and water systems. I am a member of many groups working to improve the reliability and availability of critical infrastructures and their control systems, including the North American Electric Reliability Council's (NERC) Control Systems Security Working Group (CSSWG), the Instrumentation Systems and Automation Society (ISA) S99 Manufacturing and Control Systems Security Committee, the National Institute of Standards and Technology (NIST) Industry-Grid Working Group, Institute for Electrical and Electronic Engineers (IEEE) Power Engineering Society Substations Committee, International ElectroTechnical Commission (IEC) Technical Committee 57 Working Group 15, and Council on Large Electric Systems (CIGRE) Working Group D2.22-Treatment of Information Security for Electric Power Utilities (EPUs). I would like to state for the record that the views expressed in this testimony are mine.

Until 2000, my focus strictly was to design and develop control systems that were efficient, flexible, cost-effective, and remotely accessible, without concern for cyber security. At about that time, the idea of interconnecting control systems with other networked computing systems started to gain a foothold as a means to help lower costs and improve efficiency, by making available operations-related data for management "decision support." Systems of all kinds that were not interconnected with others and thereby could not share information ("islands of automation") became viewed as an outmoded philosophy. But at the same time, there was no corresponding appreciation for the cyber security risks created. To a considerable extent, a lack of appreciation for the potential security pitfalls of highly interconnected systems is still prevalent today, as can be witnessed in many articles on new control systems and control system conferences. As such, the need for organizations to obtain information from operational control system networks to enable ancillary business objectives has often unknowingly led to increased cyber vulnerability of control system assets themselves.

The timing of this hearing is fortuitous as the Stimulus Bill has recently been approved which is stimulating work on the Smart Grid, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cyber security standards are being updated, the Chemical Facility Anti-Terrorism Standards (CFATS) is being reviewed, and the water industry R&D Roadmap has been issued. In each case, I believe there are shortcomings that can have significant impacts on the security of our critical infrastructures if they are not adequately addressed.

Introduction [1]

Industrial Control Systems (ICS)[2] are an integral part of the industrial infrastructure providing for the national good. While sharing basic constructs with Information Technology (IT) business systems, ICSs are technically, administratively, and functionally more complex and unique than business IT systems. Critical infrastructure protection focuses on protecting and maintaining a *safe and reliable* supply of electric power, oil, water, gasoline, chemicals, food, etc. Computer cyber vulnerabilities are important if they can affect the safe, functional performance of these systems and processes. One should view current ICS cyber security as where mainstream IT security was fifteen years ago—it is in the formative stage and needs support to leapfrog the previous IT learning curve.

The convergence of mainstream IT and ICS systems require both mainstream and control system expertise. It is the successful convergence of these systems and organizations that will enable the promised secure productivity benefits. To ensure that ICS are adequately represented, include subject matter experts with control systems experience in all planning meetings that could affect these systems.

Generally cyber security has been the purview of the Information Technology (IT) department, while control system departments have focused on equipment efficiency and reliability—not cyber security. This has led to the current situation where some parts of the organization are now sensitized to security while others are not as yet aware of the need. Industry has made progress in identifying control system cyber security as an issue while not appreciating the full gravity of the matter. There is a significant difference between the security philosophies of enterprise IT and ICS. The purpose of enterprise security is to protect the data residing in the servers from attack. The purpose of ICS security is to protect the ability of the facility to safely and securely operate, regardless of what may befall the rest of the network.

Cyber refers to electronic communications between systems and/or individuals. This term applies to any electronic device with serial or network connections. For this White Paper, the umbrella term "cyber" addresses all electronic impacts on ICS operation including:

- intentional targeted attacks,
- unintended consequences such as from viruses and worms,
- unintentional impacts from inappropriate policies, design, technologies, and/or testing,
- Electro Magnetic Pulse (EMP),
- Electro Magnetic Interference (EMI),

---

[1] The testimony is based on the White Paper prepared for the Center for Strategic and International Studies, "Assuring Industrial Control System (ICS) Cyber Security", by Joe Weiss, dated August 25, 2008.

[2] It should be noted that many of the acronyms used in industrial controls may be similar to acronyms used in government or other applications but with different meanings. Examples are ICS, IED, and IDS. In order to avoid confusion all acronyms have been spelled out the first time they have been used.

- other electronic impacts.

The umbrella term "ICS" includes:

- automated control systems (ACS),
- distributed control systems (DCS),
- programmable logic controllers (PLC),
- supervisory control and data acquisition (SCADA) systems,
- intelligent electronically operated field devices, such as valves, controllers, instrumentation,
- intelligent meters and other aspects of the Smart Grid,
- networked-computing systems.

An ICS is actually a system of systems. A crude distinction between mainstream IT and control systems is that IT uses "physics to manipulate data" while an ICS uses "data to manipulate physics." The potential consequences from compromising an ICS can be devastating to public health and safety, national security, and the economy. Compromised ICS systems can, and have, led to extensive cascading power outages, dangerous toxic chemical releases, and explosions. It is therefore important to implement an ICS with security controls that allow for reliable, safe, and flexible performance.

The design and operation of ICS and IT systems are different. Different staffs within an organization conceive and support each system. The IT designers are generally computer scientists skilled in the IT world. They view "the enemy of the IT system" as an attacker and design in extensive security checks and controls. The ICS designers are generally engineers skilled in the field the ICS is controlling. They view "the enemy of the ICS" not as an attacker, but rather system failure. Therefore the ICS design uses the "KISS" principle (keep it simple stupid) intentionally making systems idiot-proof. This approach results in very reliable but paradoxically, cyber-vulnerable systems. Moreover, the need for reliable, safe, flexible performance precludes legacy ICS from being fully secured, in part because of limited computing resources. This results in trade-off conflicts between performance/safety and security. These differences in fundamental approaches lead to conflicting technical, cultural, and operational differences between ICS and IT that need addressing.

CIA Triad Model—Confidentiality, Availability, and Integrity

- Confidentiality describes how the system or data is accessed
- Integrity describes the accuracy or completeness of the data
- Availability describes the reliability of accessing the system or data

Traditional IT systems employ the best practices associated with "Confidentiality, Integrity, Availability" (CIA) triad model—in that order of importance. The placement of rigorous end user access controls and additional data encryption processes provide confidentiality for critical information.

Traditional ICS systems employ the best practices associated with "Confidentiality, Integrity, Availability" (CIA) triad model—in the reverse order; AIC- Availability, Integrity, Confidentiality. Extra emphasis is placed on availability and message integrity.

The converged ICS/IT model would employ the best practices associated with "Confidentiality, Integrity, Availability" (CIA) triad model—in an equally balanced way. The compromise of any of the triad will cause the system to fail and become unusable.

It is important to point out another major difference between IT and ICS systems. In an IT system, the end user generally is a person, in an ICS system the end user generally is a computer or other highly intelligent control device. This distinction lies at the heart of the issue around securing an ICS in a manner appropriate to current need.

IT systems strive to consolidate and centralize to achieve an economy of scale to lower operational costs for the IT system. ICS systems by necessity are distributed systems that insure the availability and reliability of the ICS and the systems that the ICS controls. This means that remote access is often available directly from field devices reducing the effectiveness of firewalls at the Central Demilitarized Zone (DMZ) and requiring additional protection at remote locations. The limited computer processing power in the field devices precludes use of many computer resource-intensive IT security technologies such as remote authentication servers. Newer ICS designs do, or will, employ advanced high-speed data networking technologies. Thus, what used to be a single attack vector (the host) increases by the number of smart

field devices (Intelligent Electronic Devices [IED], smart transmitters, smart drives, etc.).

The use of mainstream operating system environments such as Windows, UNIX, and Linux for running ICS applications leave them just as vulnerable as IT systems. While at the same time, the application of mainstream IT security technical solutions and/or methods will help to secure more modern ICS host computers and operator consoles (*i.e.,* PCs). In technologies such as Virtual Private Networks (VPN) used to secure communications to and from ICS networks, IT security focuses on the strength of the encryption algorithm, while ICS security focuses on what goes into the VPN. An example of this concern was demonstrated by one of the Department of Energy's National Laboratories of how a hacker can manipulate widely used "middleware" software running on current mainstream computer systems without a great deal of difficulty. In this sobering demonstration, using vulnerabilities in OPC code ("OLE for Process Control"), the system appears to be functioning properly even though it is not; while displaying incorrect information on, or withholding correct information from, system operator consoles.

Certain mainstream IT security technologies adversely affect the operation of ICS, such as having components freeze-up while using port scanning tools or block encryption slowing down control system operation—basic Denial of Service (DOS). IT systems are "best effort" in that they get the task complete when they get the task completed. ICS systems are "deterministic" in that they must do it NOW and cannot wait for later as that will be too late.

To enable proper security, these examples demonstrate the mandate to understand the ICS and control processes and to evaluate the impacts of potential security process and actions upon those systems and processes prior to implementation.

Figure 1 is used to illustrate the distinction between ICS and business IT considerations. A person is shown (see yellow arrow for location) at the bottom cylindrical torus to provide a perspective of size. In this nuclear plant case, the box shown in the figure (on the left side approximately one-quarter of the way up, see green arrow for location) is one of two main coolant pumps each consuming enough power to power approximately 30,000–50,000 homes. A power plant of this design suffered a broadcast storm resulting in a DOS. In a typical broadcast storm creating a DOS, the impact is disruption of communications across a computer network, potentially resulting in shutdown of computers as a consequence. This broadcast storm DOS shutdown the equipment controlling the pumps eventually resulting in the shutdown of the nuclear plant. The term DOS has a completely different meaning when talking about desktops being shutdown compared to major equipment in nuclear plants and other major facilities being shutdown or compromised.

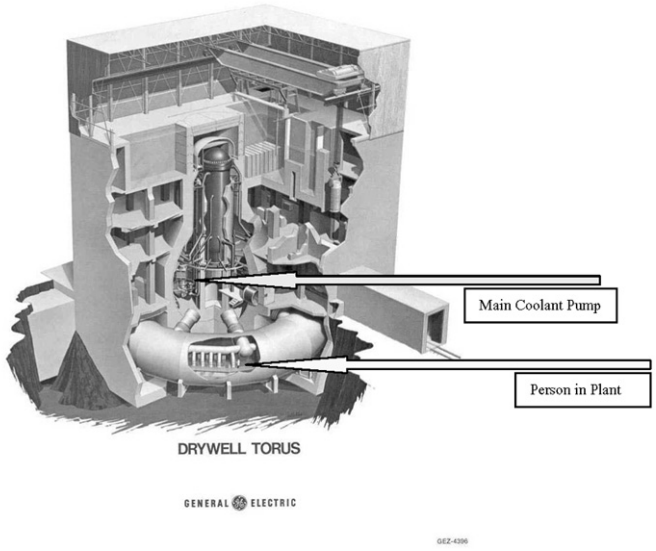

Figure 1—Nuclear Power Plant Denial of Service.

Need for Understanding

In the past, the people that implemented a system, whether Business IT or ICS, were intimately familiar with the processes and systems being automated. Today, few people possess this kind of system knowledge. Rather they design and implement systems based upon design concepts handed to them. In the case of an ICS, the designer and implementer may not even know what the end device does, how it does it, or even what it looks like. The system designer and implementer may not be in the same country as the controlled device. This disconnect allows for loss of understanding about the impacts of miss-operation of a device, device failure, or improper communication with the device.

The more complex the ICS application, the more detailed knowledge of the automated ICS processes are required: how it is designed and operated; how it communicates; how it is interconnected with other systems and ancillary computing assets. Only with this knowledge can appreciation of the cyber vulnerabilities of the system as a whole can begin. There is a current lack of ICS cyber security college curricula and ICS cyber security professional certifications.

Figure 2 characterizes the relationship of the different types of special technical skills needed for ICS cyber security expertise, and the relative quantities of each at work in the industry today. Most people now becoming involved with ICS cyber security typically come from a mainstream IT background and not an ICS background. This distinction needs to be better appreciated by government personnel (*e.g.,* DHS NCSD and S&T, DOE, EPA, etc.) responsible for ICS security. This lack of appreciation has resulted in the repackaging of IT business security techniques for control systems rather than addressing the needs of field ICS devices that often have no security or lack the capability to implement modern security mitigation technologies. This, in some cases, inadvertently results in making ICS systems less reliable without providing increased security. An example of the uninformed use of mainstream IT technologies is utilizing port scanners on PLC networks.

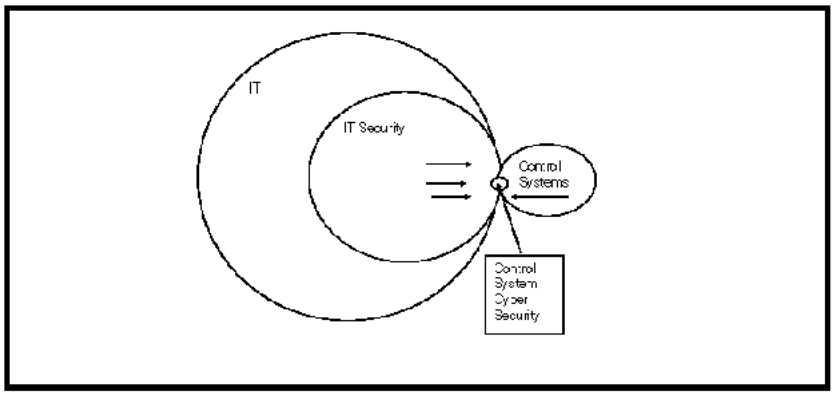

Figure 2—Relationship and Relative Availability of ICS Cyber Security Expertise.

In figure 2, we see that IT encompasses a large realm, but does not include ICS processes. It is true that IT evaluation and design models can be used to develop an ICS; the major difference is that within the Business IT model all tasks have a defined start and a defined end. In the process control model, the process is a continuous loop. Generally, the IT community avoids the continuous loop, while the ICS community embraces the continuous loop. It is the continuous loop that enables an ICS to operate efficiently and safely. As an example, automated meters "read and record the value from a meter every second". The meter will happily read and record forever, and be proud that it is doing its function.

A common misconception deals with the availability of knowledge about an ICS. There are only a limited number of DCS, SCADA, and PLC suppliers A few of the major suppliers include ABB, Areva, Alsthom, Emerson, General Electric, Honeywell, Invensys, Metso Automation, Rockwell Automation, Schneider, Siemens, Telvent, and Yokogawa. Approximately half of the suppliers are US-based while the other half are European or Asian-based. The U.S. suppliers provide systems to North America and throughout the world, except to "unfriendly" countries. The ICS systems provided internationally are the same systems provided in North America with the same architecture, same default vendor passwords, and same training.

Sales of electric industry SCADA/Energy Management Systems include the system source code, meaning that the software used in North American SCADA systems is available world-wide. Some of the largest implementations of ICS systems originating in the United States are implemented in the Middle East and China. A number of North American control system suppliers have development activities in countries with dubious credentials (*e.g.,* a major North American control system supplier has a major code writing office in China and a European RTU manufacturer has code written in Iran). There are cases where U.S. companies will remotely control assets throughout the world from North America (and vice versa). The non-North American-based ICS suppliers provide the same systems to North America as those provided to countries NOT friendly to us. There are cases where non-North American companies will remotely control assets in North America from Europe or Asia. Additionally, ICS engineers willingly share information. This truly is a global issue.

An example of information-sharing concerns is the SCADA Internet e-mail-based discussion list from Australia where people from around the world can discuss SCADA/control system issues. Unfortunately, this includes questions from individuals from suspect countries about ICS systems, processes, or devices they do not have, but that we do. This approach works in a benign world—unfortunately, we don't live in one.

There is a reticence by commercial entities to share information with the U.S. Government. Few "public" ICS cyber incidents have been documented (probably less than 10), yet there have been more than 125 actual ICS incidents. Even the "public" cases may not be easily found as they are buried in public documents such as the National Transportation Safety Board (NTSB) report on the Bellingham, WA Pipeline Disaster[3] or nuclear plant Operating Experience Reports. An interesting anecdote was a presentation made by a utility at the 2004 KEMA Control System Cyber Security Conference on an actual SCADA system external attack. This event shut down the SCADA system for 2 weeks. However, since power was not lost, the utility chose not to inform local law enforcement, the FBI, or the Electric Sector ISAC since they did not want their customers to know. This is one of the reasons it is not possible to provide a credible business case for control system cyber security.

The prevailing perception is the government will not protect confidential commercial information and organizations such as ISACs will act as regulators. That is, if two organizations have the same vulnerabilities and only one is willing to share the information, the organization sharing the information will be punished as not being cyber secure while the organization does not share will be viewed as cyber secure by default. This has Sarbanes-Oxley implications as well. It is one reason why the U.S. CERT, which is government-operated, does not work as effectively as needed. Therefore, a "Cyber Incident Response Team (CIRT) for Control Systems" by a global non-governmental organization with credible control system expertise is required. This organization would collect and disseminate information used to provide the necessary business cases for implementing a comprehensive ICS system security program. Models for this approach include CERT, InfraGard, or FAA.[4] Specific details can be provided if desired. The InfraGard model for public-private information sharing requires more sharing with the ICS community by the FBI so industry can protect themselves if a cyberattack has been detected. The FBI's "cone of silence" is not adequate. As identified by numerous government reports following the 9/11 disaster, there is a need to "connect the dots" to determine if there are patterns in events that should be followed-up. In this case, the dots that need to be connected are with ICS cyber incidents to determine if policies, technologies, and testing are adequate to address these incidents.

Operationally, there are differences between mainstream IT and ICS systems. Of primary concern is maintenance of systems. Like all systems, periodic maintenance and tuning is required to insure effective operation which must be scheduled in advance so as not to cause system impacts. Shutting down a major industrial plant may cost as much as several hundred thousand dollars per minute.

The current state of the IT world insures a high degree of intelligence and processing capability on the part of the various devices within an IT system. The standard implementation provides centralized control points for authentication and authorization of IT activities. The lifetime of the equipment in an IT network, typically, ranges from 3 to 7 years before anticipated replacement and often does not need to be in constant operation. By the very nature of the devices and their intended function, ICS devices may be 15 to 20 years old, perhaps older, before anticipated replacement. Since security was not an initial design consideration, ICS de-

[3] "Pipeline Accident Report Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10, 1999", National Transmission Safety Board Report NTSB/PAR–02/02; PB2002–916502.

[4] *http://asrs.arc.nasa.gov/overview/immunity.html.*

vices do not have excess computing capacity for what would have been considered unwanted or unneeded applications.

As can be seen, device expectations are different for ICS and IT systems, and this very difference generates two incredibly complex problems: how to authenticate access, and how to patch or upgrade software.

Of considerable importance is intra- and inter-systems communication in both the IT and ICS realms. ICS systems are intended to operate at all times, whether connected to other systems or not. This independence makes the ICS very flexible, indeed. The age of the equipment makes it difficult to authenticate communications properly. Not just between servers, but between servers and devices, devices and devices, workstations and devices, devices and people. The older technologies do not have the ability, by want of adequate operating systems, to access centralized authentication processes. By want of the ability of the ICS network to be broken into very small chunks, the use of centralized authentication is impractical, using the technologies of today. In an IT network, the authentication rules take place in the background and are hidden, for the most part, from the end user. In an ICS network, the authentication rules take place in the foreground and require interaction with the end user, causing delay and frustration.

Patching or upgrading an ICS has many pitfalls. The field device must be taken out of service which may require stopping the process being controlled. This in turn may cost many thousands of dollars and impact thousands of people. An important issue is how to protect unpatchable, unsecurable workstations such as those still running NT Service Pack 4, Windows 95, and Windows 97. Many of these older workstations were designed as part of plant equipment and control system packages and cannot be replaced without replacing the systems. Additionally, many Windows patches in the ICS world are not standard Microsoft patches but have been modified by the ICS supplier. Implementing a generic Microsoft patch can potentially do more harm than the virus or worm against which it was meant to defend. As an example, in 2003 when the Slammer worm was in the wild, one ICS supplier sent a letter to all of their customers stating that the generic Microsoft patch should not be installed as it WOULD shut down the ICS. Another example was a water utility that patched a system at a Water Treatment Plant with a patch from the operating system vendor. Following the patch, they were able to start pumps, but were unable to stop them!

The disconnection between senior management in charge of Operations from senior management in charge of security is leading to vendors being tasked to build new technology for reliability, not security purposes. The mantra of "from the plant floor to the Boardroom" is being followed without seriously asking the question of why an executive in the Boardroom would want to control a valve in a plant or open a breaker in a substation. Several years ago, a heat wave caused failures of a large number of electric transformers. In order to address this, the vendor installed temperature sensing and decided that getting information out to the largest possible audience was the best way to proceed. Consequently, the new transformer was built with a Microsoft IIS webserver integrally built into the transformer (Figure 3). Cyber vulnerable technologies such as Bluetooth and wireless modems are being built-in to ICS field devices. As one vendor claims: "They now have a Bluetooth connection for their new distribution recloser. If your line folks and/or engineers would like to sit in the truck on those rainy days checking on the recloser . . ." This means it is possible to get onto the SCADA network far downstream of the corporate firewall. In many cases, it is not possible to bypass the vulnerable remote access without disabling the ICS devices.

UNIT SUBSTATIONS NOW WEB-ENABLED TO SIMPLIFY ACCESS TO POWER TRANSFORMER DATA

Aug. 29, 2005 – Equipped with an Ethernet interface and Web server, Vendor A Unit Substations now provide simple, affordable access to power system information including transformer coil temperatures using a standard Web browser. The pre-engineered equipment ships in standard lead-times and connects to a customer's existing Ethernet Local Area Network much like adding a PC or printer.

Unit substations include a Temperature Controller, which provides remote access to transformer data, in addition to its primary role in controlling cooling fans. With a simple click of a mouse, it is easy to monitor transformer coil temperatures per phase, and verify cooling fan status at a glance. Among the many potential benefits, these new capabilities make it possible to correlate circuit loading with transformer temperatures to extend equipment life.

The typical unit substation incorporates Medium Voltage Metal-Enclosed Switchgear on the primary side and Low Voltage Switchgear or Low Voltage Switchboard on the secondary.

Vendor A was the first manufacturer in the world to embed an Ethernet interface and Web server into its power distribution equipment, allowing customers easier access to power system information. The family of power distribution equipment includes medium and low voltage switchgear, unit substations, motor control centers, switchboards and panelboards.

Figure 3—Distribution Transformer with Built-in Webserver.

A great concern is the integration of ICS systems with other systems such as Geographical Information Systems (GIS) or customer information systems. The unintended consequences of incompatible software or inappropriate communications have caused significant cyber incidents. This is an insidious problem because the individual systems work as designed, while the vulnerability is the interconnection of individually secure systems. In one case, the rebooting of a control system workstation that was not even on the control system network directly led to the automatic shutdown of a nuclear power plant. In this case, both the workstation and the PLC worked exactly as designed—two rights made a wrong. In another instance, incompatible software turned a fossil power plant into a "yo-yo" causing it to swing from maximum load to minimum load and back, within configured parameters, for 3 hours causing extreme stress to the turbine rotor.

There are currently very few forensics to detect or prevent these types of events, thus pointing to the need for additional or improved monitoring and logging. This lack of ICS cyber forensics has two aspects. The first is for performing forensics on COTS operating systems (*e.g.,* Windows). The second and more challenging issue is how to perform cyber forensics on an antique 1200 baud modem to determine if a cyber event has occurred. Technologies exist, but will removing a hard drive actually impact the restart and operation of an ICS?

One final concern almost seems trivial but isn't. In most tabletop exercises, the ultimate fix is to "pull the plug" (isolate the ICS from all others). Unfortunately, in complex ICS implementations, it may not be possible to know if the ICS really has been isolated. Consequently, a very important issue is to determine how an or-

ganization can tell if the ICS has been isolated and also if any Trojans have been left that can affect restart.

Why Do We Care

It is often, but mistakenly, assumed that a cyber security incident is always a premeditated targeted attack. However, NIST defines a Cyber Incident [5] as: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional." Unintentional compromises of CIA are significantly more prevalent and can have severe consequences, but this does not seem to be part of many current discussions of ICS cyber security. The direct cause of many ICS cyber incidents are unintentional human error. This phenomenon must be addressed by cyber security standards if they are to be effective. It is important to note that protecting ICS from these unintentional compromises also protects them from intentional compromise and outside threat.

Contacts throughout industry have shared details and adverse affects of more than 125 confirmed ICS cyber security incidents to date. The incidents are international in scope (North America, South America, Europe, and Asia) and span multiple industrial infrastructures including electric power, water, oil/gas, chemical, manufacturing, and transportation. With respect to the electric power industry, cyber incidents have occurred in transmission, distribution, and generation including fossil, hydro, combustion turbine, and nuclear power plants. Many of the ICS cyber incidents have resulted from the interconnectivity of systems, not from lack of traditional IT security approaches such as complex passwords or effective firewalls. Impacts, whether intentional or unintentional, range from trivial to significant environmental discharges, serious equipment damage, and even deaths.

Figure 4 shows the result of a Bellingham, WA, pipe rupture which an investigation concluded was not caused by an intentional act. Because of the detailed evaluation by NTSB, this is arguably the most documented ICS cyber incident. According to the NTSB Final Report, the SCADA system was the proximate cause of the event. Because of the availability of that information, a detailed post-event analysis was performed which provided a detailed time line, examination of the event, actions taken and actions that SHOULD HAVE been taken.[6]

---

[5] National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006. *http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf*

[6] "Bellingham, Washington Control System Cyber Security Case Study", Marshall Abrams, MITRE, Joe Weiss, Applied Control Solutions, August 2007, *http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham__Case__Study__report%2020sep071.pdf*

Figure 4—Bellingham, WA Gasoline Pipeline Rupture.

Figure 5 is a picture of the Idaho National Laboratory (INL) demonstration of the capability to intentionally destroy an electric generator from a cyberattack.[7]

Figure 5—INL Demonstration of Destroying Large Equipment via a cyberattack.

An attempt was made to categorize the severity of these events. The prevailing view has been there have been no significant ICS cyber incidents, but that industry will respond when a significant event occurs. Consequently, a database of ICS cyber incidents was examined to determine the level of severity of these incidents. Arbitrarily, three levels of severity were developed based on impacts:

[7] *http://news.yahoo.com/s/ap/20070927/ap__on__go__ca__st__pe/hacking__the__grid__13.*

Severe

This represents failures, omissions, or errors in design, configuration, or implementation of required programs and policies which have the potential for major equipment and/or environmental damage (more than millions of dollars); and/or extreme physical harm to facilities' personnel or the public; and/or extreme economic impact (bankruptcy).

Example: The Bellingham, WA gasoline pipeline rupture's impact was 3 killed, $45M damage, and bankruptcy of the Olympic Pipeline Company. Forensics were not available to determine the actual root cause. This incident would not have been prevented by mainstream IT security policies or technologies.

Moderate

This represents failures, omissions, or errors in design, configuration, or implementation of required programs and policies which have the potential for moderate equipment and/or environmental damage (up to hundreds of thousands of dollars) with at most some physical harm to facility personnel or the public (no deaths).

Examples: (1) Maroochy (Australia) wireless hack caused an environmental spill of moderate economic consequence. This incident would not have been prevented by mainstream IT security policies or technologies. (2) Browns Ferry 3 Nuclear Plant Broadcast Storm could have been caused by a bad Programmable Logic Controller (PLC) card, insufficient bandwidth, or caused by mainstream IT security testing. Forensics were not available to determine the actual root cause. This incident would not have been prevented by mainstream IT security policies or technologies.

Minor

This represents failures, omissions, or errors in design, configuration, or implementation of required programs and policies which have the potential for minimal damage or economic impact (less than $50,000) with no physical harm to facility personnel or the public.

Example: Davis Besse Nuclear Plant cyber incident caused by a contractor with a laptop contaminated by the Slammer worm plugging into the plant Safety Parameter Display System. This incident could have been prevented by mainstream IT security policies.

From the incident data base, many of the incidents would have been judged to be Moderate or Severe. Most would not have been detected nor prevented by traditional IT security approaches because they were caused by the system interconnections or inappropriate policies or testing—not by mainstream IT cyber vulnerabilities. In order to improve security and avoid vast expenditures on systems and equipment without real improvements in automation network security, there is a critical need to examine previous ICS cyber incidents to determine if there are patterns in these incidents, what technologies would detect such events, and what policies should be followed. For mainstream IT security approaches to be effective, they need to be combined with ICS expertise that appreciates potential impact on facilities. Examination of ISA SP99 requirements and risk definitions and tools such as the Cyber Security Self-Assessment Tool (CS2SAT)[8] make it clear that consequences must be understood in terms of the effects on facilities, major impact on equipment, environmental concerns, and public safety.

One way to move toward cross-sector convergence in cyber security ways and means is for all stakeholders to use the same terminology and to eliminate duplicative or overlapping sets of security standards' requirements. NIST offers a set of high-quality publications addressing most of the relevant managerial, administrative, operational, procedural, and technical considerations. Each of these publications, such as SP 800–53, have been put through a significant international public vetting process, including, to the extent possible, by authorities in the national security domain. NIST offers its documents to all organizations interested in using them as a basis for developing in-common standards within the ICS community. The recent Nuclear Regulatory Commission Draft Regulatory Guide 5022 specifically references NIST SP 800–53 and other appropriate NIST documents.

Incentives versus Regulation

Because I am very familiar with the electric power industry, I will focus on that segment. However, the information and experience from this segment generalizes across the entire critical infrastructure.

When the EPRI Enterprise Infrastructure (cyber security) Program was initiated in 2000, control system cyber security was essentially a non-factor—it was a prob-

[8] U.S. CERT Control Systems Security Program, *http://csrp.inl.gov/Self-Assessment_Tool.html.*

lem of omission. Immediately following 9/11, the Federal Energy Regulatory Commission (FERC) attempted to provide incentives for security improvements by issuing a letter that would allow security upgrades to be included in the rate base. For various reasons, very few utilities took advantage of the offer and little was done. Consequently, in 2003 FERC approached the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Working Group with an ultimatum—do something or FERC would do it to you. In order to preclude regulations, industry promised they would produce cyber security requirements that would comprehensively secure the electric enterprise. The electric industry eventually developed the NERC CIP series of standards and the nuclear industry developed the Nuclear Energy Institute (NEI) guidance documents (NEI–0404). Instead of providing a comprehensive set of standards to protect the electric infrastructure, the NERC CIPs and NEI–0404 were ambiguous and with multiple exclusions. The industry went from being vulnerable because of lack of knowledge to now being vulnerable because of excluding systems and technologies and then claiming compliance. The electric industry has demonstrated they cannot secure the electric infrastructure without regulation. Other industrial verticals have similarly defaulted. Therefore, regulation is needed.

Recommendations

- Develop a clear understanding of ICS cyber security.
- Develop a clear understanding of the associated impacts on system reliability and safety on the part of industry, government and private citizens.
- Define "cyber" threats in the broadest possible terms including intentional, unintentional, natural and other electronic threats such as EMP.
- Develop security technologies and best practices for the field devices based upon actual and expected ICS cyber incidents.
- Develop academic curricula in ICS cyber security.
- Leverage appropriate IT technologies and best practices for securing workstations using commercial off-the-shelf (COTS) operating systems.
- Establish standard certification metrics for ICS processes, systems, personnel, and cyber security.
- Promote/mandate adoption of the NIST Risk Management Framework for all infrastructures or at least the industrial infrastructure subset.
- Establish a global, non-governmental Computer Emergency Response Team (CERT) for Control Systems staffed with control system expertise for information sharing.
- Establish a means for vetting experts rather than using traditional security clearances.
- Establish, promote, and support an open demonstration facility dedicated to best practices for ICS systems.
- Provide regulation and incentives for cyber security of critical infrastructure industries.
- Include Subject Matter Experts with control system experience at high level cyber security planning sessions.
- Change the culture of manufacturing in critical industries so that security is considered as important as performance and safety.

Summary

Recognize that first and foremost, ICS systems need to operate safely, efficiently, and securely which will require regulation. ICS cyber vulnerabilities are substantial and have already caused significant impacts including deaths. Security needs to be incorporated in a way that does not jeopardize the safety and performance of these systems. One should view ICS cyber security as where mainstream IT security was fifteen years ago—it is in the formative stage and needs support to leapfrog the previous IT learning curve. There is a convergence of mainstream IT and control systems that will require both areas of expertise. To ensure that ICS are adequately represented, include subject matter experts with control systems experience in all planning meetings that could affect these systems. The prevailing perception is the government will not protect confidential commercial information and organizations such as ISACs will act as regulators. This has Sarbanes-Oxley implications as well. It is one reason why the U.S. CERT, which is government-operated, does not work as effectively as needed and a "CIRT for Control Systems" by a global non-governmental organization with credible control system expertise is required.

The CHAIRMAN. Thank you very much, Dr. Weiss.
Dr. Amoroso?

STATEMENT OF DR. EDWARD G. AMOROSO, SENIOR VICE PRESIDENT AND CHIEF SECURITY OFFICER, AT&T INC.

Dr. AMOROSO. OK. So, first of all, thanks very much for the invite. I do appreciate it.

Mr. Chairman, I'm an example of a person who's very much in the trenches, day to day, working cybersecurity issues. My job at AT&T is the realtime protection of our vast infrastructure, so you can almost think of AT&T as a microcosm of the critical infrastructure that we have in our country. I mean, we have, you know, these wireless assets and Internet assets and business and commercial-service assets, and certainly do have our share of control systems, as well. So, day in, day out, we're working very hard to protect our systems from hackers and terrorists and criminals and all the things that really present quite a challenge for our Nation.

Now, for me, personally, I was first introduced to the topic when I joined Bell Laboratories in the early 1980s, and AT&T was working cybersecurity issues in those days, mostly with the Federal Government. You might remember that, in the 1980s, when you talked about cybersecurity—we didn't even have that term then—you got a lot of blank stares, right? You might get somebody in Washington interested, you might get a bank interested, but certainly no businesses. We don't have a legacy in this area. And I thought Dr. Weiss's comments were a good example of, maybe, where we were in computers and networks about 20 years ago, probably a good two-decade lag, perhaps, in our control systems.

So, for me, personally, to get to the point where I have the competence and capability to protect AT&T's infrastructure, AT&T put me through 24 years of doing almost nothing but cybersecurity. They paid for me to go get a Ph.D. in computer science, they sent me to Columbia Business School to learn the business issues, they put up with me writing four books on the topic, so I've been through, you know, kind of a quarter of a century of boot camp in cybersecurity, and I'm here to, maybe, just provide a little bit of perspective and a couple of suggestions on some things that I think are going to be important for our country.

And I want to use an example. There's a particular type of threat that you may be reading about. If you picked up the *New York Times* today, then you saw there was an article on "botnets," which has become a buzzword. These are pretty nasty attack approaches. A "botnet" is something that harnesses the power of all of our PCs in our homes. I think just about everyone in this room would probably admit, perhaps privately, that they don't administer their PC too well at home. I know that I don't; and I do this for a living. When you don't, it's very easy for attackers or terrorists or folks from who the heck knows where can drop—to drop software onto your PC that would, very unsuspectingly, be off doing things over your broadband connection.

When you do this, when you do this on a large scale and set up controllers to aim all of this energy, this cybersecurity, cyberattack energy at an unsuspecting victim—could be a civilian agency of the United States—the results can be pretty lethal. It's like aiming a

laser-guided weapon at a—at, as I said, an unsuspecting victim; could shut down government. And you reference earlier, Mr. Chairman, the experience that Estonia had when that was done to them.

A couple of things by way recommendations. Number one, I think it becomes imperative that, in our government procurement process, that we start paying more attention to threats that are valid today. I look, almost daily, at requests for proposal and requests for information that come from Washington to the private sector for products and services that we would be selling them, and they generally don't have sufficient security embedded in the set of requirements that come to us. I can't tell you how many times we'll respond to a bid, and append it with what we believe would be sufficient security to protect the government. I think this is something we need to very quickly address.

Second, I think it's imperative that we start building a greater international cooperation. When we're off chasing one of these things in realtime, chasing a botnet or trying very hard to protect one of our customers, it's generally the case that the attack is coming, as you referenced earlier, Mr. Chairman, from around the world, and there really is no place for us to turn. Certainly as a major carrier, one would think, my goodness, it would probably be the case that AT&T could very easily reach out to any number of international carriers or countries or contacts, but that is not the case. There is no easy way for us to go work with—you referenced China and Russia, the two examples of countries where, if there's an attack emanating from there, we have to work around it—not so much with it, but around it. And that's something that I think needs to be address very quickly.

Third recommendation is that it's pretty obvious that the world is moving more and more toward a mobility base. I'll bet everybody in this room has a mobile phone, you know, tucked in their pocket, hopefully on vibrate. That's going to change the game pretty significantly. When we think about the types of attacks and problems that we see in the computer and network area, they become all the more intense as mobility becomes a fundamental piece of our society, if it hasn't already. I think it's already a basic part of our critical infrastructure.

So, I think government and the private sector is going to have to work more closely with the carriers, because we are the—we are the—if you think about it, there's an attacker, there's a victim, and what sits in between? The thing that sits in between is the network.

So, we appreciate the invite to address the Committee, look forward to working with you. We've prepared some remarks that I hope you'll take a chance—take a moment to read. And look forward to answering any questions you might have.

[The prepared statement of Dr. Amoroso follows:]

PREPARED STATEMENT OF DR. EDWARD G. AMOROSO, SENIOR VICE PRESIDENT AND CHIEF SECURITY OFFICER, AT&T INC.

Good morning, my name is Edward Amoroso. I currently serve as Senior Vice President and Chief Security Officer of AT&T. I have worked in the area of cybersecurity for the past 24 years, starting at Bell Labs. My current responsibilities include design and operation of the security systems and processes that protect AT&T's vast domestic and international wired and wireless infrastructure. This in-

frastructure supports AT&T's voice and data networks, and permits AT&T to provide the Internet access, telephony, video entertainment, data transmission and managed services that AT&T offers to its many millions of customers around the globe.

My educational background includes a Bachelor's degree in physics from Dickinson College, as well as Masters and PhD degrees in computer science, both from the Stevens Institute of Technology, where I have also served as an adjunct professor of computer science for the past twenty years. I am a graduate of the Columbia Business School, and have written four books and many articles on the topic of cyber-security.

On behalf of AT&T, I would like to thank the Committee for this invitation to comment on the cyber-security challenges facing my company, this Nation and the rest of the world. My comments include a professional perspective on how and why cyber-security threats have increased significantly over the past 5 years, as well as suggestions on how these threats should be addressed.

I believe most citizens equate the issue of cyber-security with viruses that find their way onto computers, or with the stories they hear about so-called "security breaches" resulting from laptops being lost or stolen. These are certainly problems, but from the perspective of protecting the Nation's critical infrastructure, these issues are not severe. Cyber-security is more about protecting the infrastructure from intrusion by individuals or forces determined to disrupt the flow of data and the storage of information. Motives might be mere mischief, making a political statement, gaining business advantage, making pecuniary gain, exposing a vulnerability or something more sinister.

In the mid-1990s, attacks on the infrastructure sometimes were clumsy, or so sophisticated as to be admired, but they did not cause lasting damage. But just as computing has advanced and evolved, so too has the frequency and form of attacks. For a time, those determined to intrude (call them hackers for simplicity-sake) were able to take advantage of the fact that most consumers, businesses and government agencies had not done a good job maintaining the security of their operating systems and common applications (such as browsers and e-mail applications) by applying security patches and running system security programs. "Patching" has improved dramatically across the global infrastructure, and anti-malware applications have become common place. Thus, attackers now use "phishing" or "pharming" approaches, whereby an unsuspecting victim is tricked into giving away passwords or personal information, or allowing malware to be dropped onto machines—even those that are properly patched. Last year the FBI announced that revenues from cybercrime, for the first time ever, exceeded drug trafficking as the most lucrative illegal global business, estimated at reaping more than $1 trillion annually in illicit profits.

Evolving and more lethal type of cyber-attacks can devastate infrastructure. One form of attack uses "botnets," which work by harnessing the power of unprotected PCs from homes and businesses. Malicious intruders, hackers and even terrorists are getting very good at harnessing the power of PCs and aiming them at unsuspecting victims. It has become so easy and rampant that the risk has grown exponentially. The result is a laser-like cyber-attack on an unsuspecting business or government system. Estonia, for example, was the subject of a botnet attack 2 years ago, and the results were catastrophic: The entire country was disconnected from the Internet, and the event has come to be known as "WWI" for "Web War I."

For AT&T, cyber-security is the collective set of capabilities, procedures and practices that protect our customers and the services we offer them from the full spectrum of cyber-threats, including botnets. This assures that the information, applications, and services our customers want are secure, accurate, reliable and available wherever and whenever they are desired. Cyber-security is a leading corporate priority, and we are investing significant resources in making our network and our customers more secure. To this end, strong cyber-security is essential to maintaining the integrity and reliability of the network, and well as protecting privacy of personal customer information.

The technology within our network is rapidly evolving to support new applications and services. This year alone, AT&T is investing more than $18 billion in expanding the capabilities of our network and infrastructure to meet the rapid global expansion of advanced information technology and services, and to enhance reliability and security. The size and scope of AT&T's global network, coupled with our industry-leading cyber-security capabilities, gives us a unique perspective into malicious cyber-activity. Our advanced network technology currently transports more than 17 Petabytes a day of IP data traffic, and we expect that to double every 18 months for the foreseeable future. Our network technologies give us the capability to analyze traffic flows to detect malicious cyber-activities, and, in many cases, get very

early indicators of attacks before they have the opportunity to become major events. For example, we have implemented the capability within our network to automatically detect and mitigate most Distributed Denial of Service Attacks within our network infrastructure before they affect service to our customers. Indeed, part of the investment I described above is targeted to advancing our attack mitigation capabilities. We doubled, and are now redoubling, our ability to provide global coverage to scrub for denial-of-service attacks. We went from one domestic scrubbing complex to multiple locations across the United States, as well as nodes in Europe and Asia. This gives us the ability to filter out attack traffic as close to the source of the threat as possible.

To address the growing cyber threat to our nation, and in particular the threat of botnets, three actions are recommended. First, our Federal procurement process needs to be upgraded to implement sufficient security protections to deal with large-scale cyber-attack. The denial-ofservice threat, for example, is largely overlooked in most civilian agency networks. On the other hand, private sector companies like AT&T offer advanced services that can mitigate the threat of a denial-of-service attacks before they arrive on an agency's doorstep. Without a strategic emphasis to build strong cyber-security protections into the Federal requirements development process, however, those protections are unlikely to find their way into systems procurement requirements.

A second recommended action involves international partnership during a cyber-attack. When a botnet is aimed at some critical asset, the servers controlling the attack might be scattered to the farthest reaches of the globe. The local service provider is thus in the best position to take suitable security action. But this requires international cooperation that has been so far inadequate. Such a course would be consistent with the recent recommendations by the National Security Telecommunications Advisory Committee (NSTAC) that international coordination receive prioritized attention. Specifically, NSTAC recommended that the Federal Government pursue development of international cyber-incident warning and responsible capabilities since network attacks or incidents originating outside of the United States raise increasing concerns about the security and availability of domestic national security and emergency preparedness communications. In many ways, the international paradigm reflects the flaws in the current, domestic security paradigm—international coordination on incident response remains largely ad hoc. The continuing absence of a coordinated, scalable, international structure for response that includes all relevant stakeholders undercuts efforts to develop systemic solutions and responses.

Finally, our government should rethink its own relationship with its network service providers. As attacks become more mobile and network-based, the service provider has the best vantage point to mitigate the threat. Too often, in our work at AT&T, we see government and business systems designed with the service provider at arms-length. This practice must be discouraged. In fact, agencies that run their own cyber-security operation should be ready to justify such decision. They cannot stop network threats such as botnets on their own.

To this end, we endorse the several NSTAC recommendations that encourage such relationship rethinking. We believe that the public and private sectors can and should create structures for timely and secure sharing of cyber-security threat and response information between government and industry, and between and among critical infrastructures in a trusted, collaborative environment. In partnership with the private sector, the government can and should create a secure and responsive identity management framework to support cyber-based identity processes and applications, thereby ensuring emergency response access to critical infrastructure in support of disaster recovery. In collaboration with industry, the government can and should create a comprehensive incident-response architecture embracing critical infrastructure facilities and core infrastructure services. Perhaps most importantly, the government should collaborate with industry on research and development efforts in pursuit of critical cyber-security capabilities, and in furtherance of interoperable identity management processes between government and the private sector.

To conclude, I am pleased that this Committee is focusing on cyber-security, and looking forward to working with you to develop practical steps to ensure that cyber security does not threaten our Nation's present and future well-being.

The CHAIRMAN. Thank you very much.
Dr. AMOROSO. You bet.
The CHAIRMAN. You've written four books?
Dr. AMOROSO. Yes.

The CHAIRMAN. Are they——

Dr. AMOROSO. But, Dr. Spafford's books are actually better than mine.

[Laughter.]

The CHAIRMAN. Are they? Well, then—I'm going to forget all about yours, then.

[Laughter.]

The CHAIRMAN. Dr. Spafford?

STATEMENT OF DR. EUGENE H. SPAFFORD, PROFESSOR AND EXECUTIVE DIRECTOR, PURDUE UNIVERSITY CENTER FOR EDUCATION AND RESEARCH IN INFORMATION ASSURANCE AND SECURITY (CERIAS) AND CHAIR OF THE U.S. PUBLIC POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING MACHINERY (USACM)

Dr. SPAFFORD. Thank you, Mr. Chairman and Members of the Committee.

To put some of my comments in a little bit of context, I've been working in computing and computing security for about 30 years, and I have done that in a number of different kinds of roles; certainly, as a researcher at a university; and some of the things that we have invented, that I've invented with my students, are in use worldwide right now, protecting systems. They're common security tools and methods. The students themselves have gone off to important roles. In fact, one of our most recent Ph.D. graduates serves the Sergeant at Arms of the Senate. And we have graduates who are working in a number of different Federal agencies.

I have worked as a consultant and founder of commercial firms. And I have worked as a consultant for Federal agencies, including the U.S. Government Accountability Office, Air Force, the National Security Agency, the FBI, the National Science Foundation, and national labs. So, I have seen across a very broad spectrum of the places where cyber is used, and some of the problems involved.

And the simplest way to state this is, the Nation is under attack, and it is a hostile attack, it is a continuing attack. It has been going on for years, and we have largely been ignoring it. The commercial losses, by best estimates, are in the tens of billions of dollars per year. To put that in context, imagine a Hurricane Katrina-style event occurring every year and being ignored.

The classified largest—classified losses may be as large or even larger, because some of the things that are at risk can't really be easily valued in dollars. It's very difficult to value our national security and protection.

There are a number of reasons why this has been ignored and why the problem continues. I would invite you to look in my written testimony; I have more material there.

But, one of the issues that we have to face is, this is not primarily a network problem, it is a computing problem, it is the endpoints, it is the computer systems people use, it is the cell phones, the control nodes, and the other items, that people are breaking into. The network is a conduit and has some of its own problems, but computing is a much bigger problem than simply the Internet.

Second, there are no single easy solutions. It is not simply a technology problem, where we can come up with a fix and apply it. Too many people think that's the case.

Security is a process. It's an ongoing process akin to having policemen on the beat or having patrols off the coast. We have to continue to fund and be vigilant and improve what we do in defense.

Cybersecurity is a combination of technology, of policy, and of knowledge and people. And we have problems in all three areas. Again, I address some of this in my written testimony.

Part of the problem in policy is the fact that we haven't done much at all to put up a deterrent. We do not strike back at those who attack our systems. If they are criminal elements, our law enforcement doesn't have the tools, the manpower, or, very often, the authority to go after those individuals. And so, they continue to make millions of dollars per week—some of the credit card fraud—and they reinvest that in new tools, far more than we are investing in development of defensive tools here in this country.

For nation-state type of attacks, we don't apply any of the kinds of diplomatic or economic pressures that we might be able to do to try to discourage that behavior.

So, we're going to have to have some improvements in technology. We're going to have to have improvements in the knowledge and people involved. And this is an area I addressed extensively in my written testimony.

But, let me say something about the technology, because that's an area that I've worked in so much. The current view, that security can be had by adding something on afterwards or by applying patches to problems, simply won't work. It has not worked. It will not work. If we continue our current approach to producing and buying technology, we are going to continue to be vulnerable.

We need to apply more funding and support to research. And the research can't be near-term, let's-come-up-with-a-patch-for-the-latest-botnet-or-the-latest-firewall-problem, but long-term research as to how to fundamentally redesign some of the systems we're using and the security involved. That funding has to be continuing, and it should go toward some risky ideas, because if we aren't approaching risky ideas, we're not likely to come up with the breakthrough ideas that are necessary.

Such kinds of research are done at, largely, universities, but also at the national labs, as has been noted, and many independent firms that do have research arms. These not only produce results and experience, but they produce people, people who can go on and be faculty members, can be researchers to found companies, serve in the government and other places.

So, our investment in research, even if the research results don't always produce something that we can use, do have a benefit in the long term for the country and the economy and the knowledge base, but it must be significant and sustained

When I was a member of the PITAC, the report we issued in 2005 indicated that we believed at least a tripling of the research budget at that time was necessary. There was actually a slight decrease. Current funding could probably stand a many-times-over increase.

Let me point out that this is not simply a Federal problem, but a national problem. We're going to have to have other parties step up. It's not something that the Federal Government can solve all by itself. And it's actually an international problem, as has been noted. We have friends around the world whose banking systems, telecommunications systems, supply systems, healthcare, and other public infrastructure, are threatened. If the oil wells offshore from some of the countries we're friends with are compromised because their control systems are corrupted, it could have a devastating impact on our economy. We cannot afford to be insular in our thinking.

In closing, I included a well-known aphorism in my testimony that I've seen attributed to a number of different authors, John Dryden, the English playwright, being one of them, that insanity is doing the same thing over and over again and expecting different results. Our cybersecurity application, particularly in the government, has been insane for years. You have a chance to change that.

Thank you for your attention. I look forward to your questions.

[The prepared statement of Dr. Spafford follows:]

PREPARED STATEMENT OF DR. EUGENE H. SPAFFORD, PROFESSOR AND EXECUTIVE DIRECTOR, PURDUE UNIVERSITY CENTER FOR EDUCATION AND RESEARCH IN INFORMATION ASSURANCE AND SECURITY (CERIAS) AND CHAIR OF THE U.S. PUBLIC POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING MACHINERY (USACM)

Introduction

Thank you Chairman Rockefeller and Ranking Member Hutchison for the opportunity to testify at this hearing.

By way of self-introduction, I am a Professor at Purdue University. I also have courtesy appointments in the departments of Electrical and Computer Engineering, Philosophy, and Communication at Purdue, and I am an adjunct professor at the University Texas at San Antonio. At Purdue, I am also the Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS). CERIAS is a campus-wide multidisciplinary institute, with a mission to explore important issues related to protecting computing and information resources. We conduct advanced research in several major thrust areas, we educate students at every level, and we have an active community outreach program. CERIAS is the largest such center in the United States, and we were recently ranked as the #1 such program in the country. CERIAS also has a close working relationship with dozens of other universities, major commercial firms and government laboratories.

Along with my role as an academic faculty member, I also serve on several boards of technical advisors, and I have served as an advisor to Federal law enforcement and defense agencies, including the FBI, the Air Force and the NSA. I was also a member of the most recent incarnation of the President's Information Technology Advisory Committee (PITAC) from 2003 to 2005. I have been working in information security for over 25 years.

I am also the Chair of USACM, the U.S. public policy committee of the ACM. With over 90,000 members, ACM is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. USACM acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. It seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community.

USACM is a standing committee of the ACM. It tracks U.S. public policy initiatives that may affect the membership of ACM and the public at large, and provides expert input to policy-makers. This advice is in the form of non-partisan scientific data, educational materials, and technical analyses that enable policy-makers to reach better decisions. Members of USACM come from a wide-variety of backgrounds including industry, academia, government, and end users.

My testimony is as an expert in the field. My testimony does not reflect official positions of either Purdue University or the ACM, although I believe that my comments are consistent with values and positions held by those organizations.

General Comments

Our country is currently under unrelenting attack. It has been under attack for years, and too few people have heeded the warnings posed by those of us near the front lines. Criminals and agents of foreign powers have been probing our computing systems, defrauding our citizens, stealing cutting-edge research and design materials, corrupting critical systems, and snooping on government information. Our systems have been compromised at banks, utilities, hospitals, law enforcement agencies, every branch of the armed forces, and even the offices of the Congress and White House. Although exact numbers are impossible to obtain, some estimates currently run in the tens to hundreds of billions of dollars per year lost in fraud, IP theft, data loss, and reconstitution costs. Attacks and losses in much of the government and defense sector are classified, but losses there are also substantial.

Over the last few decades, there have been numerous reports and warnings of the problems issued. When I was a member of the PITAC in 2003–2005, we found over a score carefully-researched and well-written reports from research organizations that highlighted the dangers and losses, and pointed out that the problem was only going to get worse unless drastic action is taken. Our own report from the PITAC, *Cyber Security: A Crisis of Prioritization,* published in 2005, echoed these concerns but was given scant attention. Other reports, such as *Toward a Safer and More Secure Cyberspace* by the National Academies have similarly been paid little attention by leaders in government and industry. Meanwhile, with each passing week, the threats grow in sophistication and number, and the losses accumulate.

I do not mean to sound alarmist, but the lack of attention being paid to these problems is threatening our future. Every element of our industry and government depends on computing. Every field of science and education in our country depends, in some way, on computing. Every one of our critical infrastructures depends on computing. Every government agency, including the armed forces and law enforcement, depend on computing. As our IT infrastructure becomes less trustworthy, the potential for failures in the institutions that depend on them increases.

There are a number of reasons as to why our current systems are so endangered. Most of the reasons have been detailed in the various reports I mentioned above and their lists of references, and I suggest those as background. I will outline some of the most significant factors here, in no particular order:

- Society has placed too much reliance on marketplace forces to develop solutions. This strategy has failed, in large part, because the traditional incentive structures have not been present: there is no liability for poor quality, and there is no overt penalty for continuing to use faulty products. In particular, there is a continuing pressure to maintain legacy systems and compatibility rather than replace components with deficient security. The result is a lack of reward in the marketplace for vendors with new, more trustworthy, but more expensive products.
- Our computer managers have become accustomed to deploying systems with inherent weaknesses, buying add-on security solutions, and then entering a cycle of penetrate-and-patch. As new flaws are discovered, we deploy patches or else add on yet new security applications. There is little effort devoted to really designing in security and robustness. This also has contributed to unprotected supply chains, where software and hardware developed and sold by untrusted entities is then placed in trusted operational environments: the (incorrect) expectation is that the add-on security will address any problems that may be present.
- There is a misperception that security is a set of problems that can be "solved" in a static sense. That is not correct, because the systems are continuing to change, and we are always facing new adversaries who are learning from their experiences. Security is dynamic and changing, and we will continue to face new challenges. Thus, protection is something that we will need to continue to evolve and pursue.
- Too few of our systems are designed around known, basic security principles. Instead, the components we do have are optimized for cost and speed rather than resilience and security and those components are often needlessly complex. Better security is often obtained by deploying systems that do less than current systems—extra features not necessary for the task at hand too often provide additional avenues of attack, error, and failure. However, too few people understand cyber security, so the very concept of designing, building, or obtaining less capable systems, even if they are more protected, is viewed as unthinkable.
- We have invested far too little on the resources that would enable law enforcement to successfully investigate computer crimes and perform timely forensic

activities. Neither have we pursued enough political avenues necessary to secure international cooperation in investigation and prosecution of criminals operating outside our borders. As a result, we have no effective deterrent to computer crime.

- The problems with deployed systems are so numerous that we would need more money than is reasonably available simply to patch existing systems to a reasonable level. Unfortunately, this leads to a lack of funding for long term research into more secure systems to replace what we currently have. The result is that we are stuck in a cycle of trying to patch existing systems and not making significant progress toward deploying more secure systems.
- Over-classification hurts many efforts in research and public awareness. Classification and restrictions on data and incidents means that it is not possible to gain an accurate view of scope or nature of some problems. It also means that some research efforts are inherently naive in focus because the researchers do not understand the true level of sophistication of adversaries they are seeking to counter.
- Too little has been invested in research in this field, and especially too little in long-term, risky research that might result in major breakthroughs. We must understand that real research does not always succeed as we hope, and if we are to make major advances it requires taking risks. Risky research led to computing and the Internet, among other things, so it is clear that some risky investments can succeed in a major way.
- We have too many people who think that security is a network property, rather than understanding that security must be built into the endpoints. The problem is not primarily one of "Internet security" but rather of "computer and device" security.
- There is a common misconception that the primary goal of intruders is to exfiltrate information or crash our systems. In reality, clever adversaries may simply seek to modify critical applications or data so that our systems do not appear to be corrupted but fail when relied upon for critical functions—or worse, operate against our interests. We seldom build and deploy systems with sufficient self-checking functions and redundant features to operate correctly even in the presence of such subversion.
- Government agencies are too disorganized and conflicted to fully address the problems. Authorities are fragmented, laws exist that prevent cooperation and information sharing, and political "turf" battles all combine to prevent a strong, coordinated plan from moving forward. It is debatable whether there should be a single overarching authority, and where it should be if so. However, the current disconnects among operational groups including DHS, law enforcement, the armed forces and the intelligence community is a key part of the problem that must be addressed.
- We have too few people in government, industry and the general public who understand what good security is about. This has a negative effect on how computing is taught, designed, marketed, and operated. I discuss this in more depth later in this testimony.

I would be remiss not to note that most systems handling personal information have also been poorly designed to protect privacy. Good security is necessary for privacy protection. Contrary to conventional wisdom, it is not necessary to sacrifice privacy considerations to enhance security. However, it takes additional effort and expense to design to both protect privacy *and* improve security, and not everyone is willing to make the effort despite the rewards.

This battle is global. Our colleagues in other countries are also under siege from criminals, from anarchists, from ideologues, and from agents of hostile countries. Any effective strategy we craft for better cyber security will need to take into account that computing is in use globally, and there are no obvious national borders in cyberspace.

Additionally, it is important to stress that much of the problem is not purely technical in nature. There are issues of sociology, psychology, economics and politics involved (at the least). We already have technical solutions to some of the problems we face, but the parties involved are unable to understand or agree to fielding those solutions. We must address all these other issues along with the technical issues if we are to be successful in securing cyberspace.

Rethinking Computing [1]

Fifty years ago, IBM introduced the first commercial all-transistor computer (the 7000 series). A working IBM 7090 system with a full 32K of memory (the capacity of the machine) cost about $3,000,000 to purchase—over $21,000,000 in current dollars. Software, peripherals, and maintenance all cost more. Rental of a system (maintenance included) could be well over $500,000 per month. The costs of having such a system sit idle between jobs (and during I/O) led the community to develop operating systems that supported sharing of hardware to maximize utilization. It also led to the development of user accounts for cost accounting and development of security features to ensure that the sharing didn't go too far. As the hardware evolved and became more capable, the software also evolved and took on new features.

Costs and capabilities of computing hardware have changed by a factor of tens of millions in five decades. It is now possible to buy a greeting card at the corner store with a small computer that can record a message and play it back to music: that card has more memory and computing power than the multimillion dollar machine of 1958. Yet, despite these incredible transformations, the operating systems, data bases, languages, and more that we use are still basically the designs we came up with in the 1960s to make the best use of limited equipment. We're still suffering from problems known for decades, and systems are still being built with intrinsic weaknesses.

We failed to make appreciable progress with the software because, in part, we've been busy trying to advance on every front. It is simpler to replace the underlying hardware with something faster, thus getting a visible performance gain. This helps mask the ongoing lack of quality and progression to really new ideas. As well, the speed with which the field of computing (development and application) moves is incredible, and few have the time or inclination to step back and re-examine first principles. This includes old habits such as the sense of importance in making code "small" even to the point of leaving out internal consistency checks and error handling. (Y2K was not a one-time fluke—it was instance of an institutionalized bad habit.)

Another such habit is that of trying to build every system to have the capability to perform every task. There is a general lack of awareness that security needs are different for different applications and environments; instead, people seek uniformity of OS, hardware architecture, programming languages and beyond, all with maximal flexibility and capacity. Ostensibly, this uniformity is to reduce purchase, training, and maintenance costs, but fails to take into account risks and operational needs. Such attitudes are clearly nonsensical when applied to almost any other area of technology, so it is perplexing they are still rampant in IT.

For instance, imagine the government buying a single model of commercial speedboat and assuming it will be adequate for bass fishing, auto ferries, arctic icebreakers, Coast Guard rescues, oil tankers, and deep water naval interdiction—so long as we add on a few after-market items and enable a few options. Fundamentally, we understand that this is untenable and that we need to architect a vessel from the keel upwards to tailor it for specific needs, and to harden it against specific dangers. Why cannot we see the same is true for computing? Why do we not understand that the commercial platform used at home to store Aunt Bea's pie recipes is *not* equally suitable for weapons control, health care records management, real-time utility management, storage of financial transactions, and more? Trying to support everything in one system results in huge, unwieldy software on incredibly complex hardware chips, all requiring dozens of external packages to attempt to shore up the inherent problems introduced by the complexity. Meanwhile, we require more complex hardware to support all the software, and this drives complexity, cost and power issues.

The situation is unlikely to improve until we, as a society, start valuing good security and quality over the lifetime of our IT products. We need to design systems to enforce behavior within each specific configuration, not continually tinker with general systems to stop each new threat. Firewalls, intrusion detection, antivirus, data loss prevention, and even virtual machine "must-have" products are used because the underlying systems aren't trustworthy—as we keep discovering with increasing pain. A better approach would be to determine exactly what we want supported in each environment, build systems to those more minimal specifications only, and then ensure they are not used for anything beyond those limitations. By having a

[1] Adapted from *Rethinking computing insanity, practice and research,* CERIAS Weblog, December 15, 2008, <*http://www.cerias.purdue.edu/site/blog/post/rethinking_computing_insanity_practice_and_research/*>. In turn, this post was derived from my essay in the October 2008 issue of *Information Security* magazine.

defined, crafted set of applications we want to run, it will be easier to deny execution to anything we don't want; To use some current terminology, that's "whitelisting" as opposed to "blacklisting." This approach to design is also craftsmanship-using the right tools for each task at hand, as opposed to treating all problems the same because all we have is a single tool, no matter how good that tool may be. After all, you may have the finest quality *multitool* money can buy, with dozens of blades and screwdrivers and pliers. You would never dream of building a house (or a government agency) using that multitool. Sure, it does many things passably, but it is far from ideal for expertly doing most complex tasks.

Managers will make the argument that using a single, standard component means it can be produced, acquired and operated more cheaply than if there are many different versions. That is often correct insofar as direct costs are concerned. However, it fails to include secondary costs such as reducing the costs of total failure and exposure, and reducing the cost of "bridge" and "add-on" components to make items suitable. There is less need to upgrade and patch smaller and more directed systems far less often than large, all-inclusive systems because they have less to go wrong and don't change as often. There is also a defensive benefit to the resulting diversity: attackers need to work harder to penetrate a given system, because they don't know what is running. Taken to an extreme, having a single solution also reduces or eliminates real innovation as there is no incentive for radical new approaches; with a single platform, the only viable approach is to make small, incremental changes built to the common format. This introduces a hidden burden on progress that is well understood in historical terms—radical new improvements seldom result from staying with the masses in the mainstream.

Therein lies the challenge, for researchers and policy-makers. The *current cybersecurity landscape* is a major battlefield. We are under constant attack from criminals, vandals, and professional agents of governments. There is such an urgent, large-scale need to simply bring current systems up to some minimum level of security that it could soak up way more resources than we have to throw at the problems. The result is that there is a huge sense of urgency to find ways to "fix" the current infrastructure. Not only is this where the bulk of the resources is going, but this flow of resources and attention also fixes the focus of our research establishment on these issues, When this happens, there is great pressure to direct research toward the current environment, and toward projects with tangible results. Program managers are encouraged to go this way because they want to show they are good stewards of the public trust by helping solve major problems. CIOs and CTOs are less willing to try outlandish ideas, and cringe at even the notion of replacing their current infrastructure, broken as it may be. So, researchers go where the money is—incremental, "safe" research.

We have crippled our research community as a result. There are too few resources devoted to far-ranging ideas that may not have immediate results. Even if the program managers encourage vision, review panels are quick to quash it. The recent history of DARPA is one that has shifted toward immediate results from industry and away from vision, at least in computing. NSF, DOE, NIST and other agencies have also shortened their horizons, despite claims to the contrary. Recommendations for action (including the recent *CSIS Commission report to the President*) continue this by posing the problem as how to secure the current infrastructure rather than asking how we can build and maintain a trustable infrastructure to replace what is currently there.

Some of us see how knowledge of the past combined with future research can help us have more secure systems. The challenge continues to be convincing enough people that "cheap" is not the same as "best," and that we can afford to do better. Let's see some real innovation in building and deploying new systems, languages, and even networks. After all, we no longer need to fit in 32K of memory on a $21 million computer. Let's stop optimizing the wrong things, and start focusing on discovering and building the right solutions to problems rather than continuing to try to answer the same tired (and wrong) questions. We need a major sustained effort in research into new operating systems and architectures, new software engineering methods, new programming languages and systems, and more, some with a (nearly) clean-slate starting point. Failures should be encouraged, because they indicate people are trying risky ideas. Then we need a sustained effort to transition good ideas into practice.

I'll conclude with a quote that many people attribute to Albert Einstein, but I have seen multiple citations to its use by John Dryden in the 1600s in his play *The Spanish Friar*: "Insanity: doing the same thing over and over again expecting different results."

What we have been doing in cyber security has been insane. It is past time to do something different.

Education

One of the most effective tools we have in the battle in cyber security is knowledge. If we can marshal some of our existing knowledge and convey it to the appropriate parties, we can make meaningful progress. New knowledge is also necessary, and there too there are urgent needs for support.

History

In February 1997, I testified before the House Science Committee. At that time, I observed that nationally, the U.S. was producing approximately three new Ph.Ds. in cybersecurity[2] per year. I also noted that there were only four organized centers of cyber security education and research in the country, that none of them were very large, and that all were judged to be somewhat at risk. Indeed, shortly after that testimony, one of the centers dissolved as institutional support faded and faculty went elsewhere.

Although the number of university programs and active faculty in this area have increased in the last dozen years, the number involved and the support provided for their efforts still falls far short of the need. As an estimate, there have been less than 400 new Ph.Ds. produced in cyber security in the U.S. over the last decade with some nontrivial percentage leaving the U.S. to work in their countries of origin. (Approximately 25 percent of those graduates have come from CERIAS at Purdue.) Of those that remained, less than half have gone back into academia to be involved in research and education of new students.

In my testimony[3] in 1997 and in subsequent testimony in 2000, I provided suggestions for how to increase the supply of both students and faculty in the field to meet the anticipated demand. Three of my suggestions were later developed by others into Federal programs: the Centers of Academic Excellence (CAE), the Scholarship for Service program, and the Cyber Trust program.

Today, we have about a dozen major research centers around the country at universities, and perhaps another two dozen secondary research groups. Many, but not all, of these institutions are certified as CAEs, as are about 60 other institutions providing only specialized cyber security education. The CAE program has effectively become a certification effort for smaller schools offering educational programs in security-related fields instead of any true recognition of excellence; there are some highly regarded programs that do not belong to the CAE program for this reason (Purdue and MIT among them). One problem with the way the CAE program has evolved is that it does not provide any resources that designated schools may use to improve their offerings or facilities.

The Scholarship for Service program, offered through NSF, has been successful, but in a limited manner. This program provides tuition, expenses and a stipend to students completing a degree in cyber security at an approved university. In return, those students must take a position with the Federal Government for at least 2 years or pay back the support received. Over the last 7 years, over 1000 students have been supported under this program at 30 different campuses. The majority of students in these programs have, indeed, gone on to Federal service, and many have remained there. That is an encouraging result. However, the numbers work out to an average of about four students per campus per year entering Federal service, and anecdotal evidence indicates that demand is currently five times current production and growing faster than students are being produced. This program address needs in other segments of U.S. society.

NSF has been the principal supporter of open university research in cyber security and privacy through its Cyber Trust program (now called Trustworthy Computing). That effort has produced a number of good results and supported many students to completion of degrees, but has been able to support only a small fraction (perhaps less than 15 percent) of the proposals submitted for consideration. Equally unfortunate, there has been almost no support available from NSF or elsewhere in government for the development and sustainment of novel programs that are not specifically designated as research; as an example, CERIAS as an important center of education, research and outreach has never received direct Federal funding to support core activities, staff, and educational development. If it were not for periodic gifts from generous and civic-minded industrial partners, the center would have dis-

---

[2] This and related numbers in my report exclude individuals working primarily in cryptology. Although cryptography is necessary for good security, there is a difference between those who study the mathematics of codes and ciphers, and those who study systems and network security; the two general areas are related much in the way mathematicians and mechanical engineers are.

[3] Available online <*http://spaf.cerias.purdue.edu/usgov/index.html*>

appeared years ago—and may yet, given the state the economy. Other defined centers are similarly precariously funded.

Future

We need significant, sustained efforts in education at every level to hope to meet the challenges posed by cyber security and privacy challenges. In the following, I will outline some of the general issues and needs, with some suggestions where Federal funding might be helpful. A study by an appropriate organization would be necessary to determine more precisely what program parameters and funding levels would be useful. Given the complexity of the issues involved, I can only outline some general approaches here.

Let me note that many of these activities require both a ramp-up and sustainment phase. This is especially true for postgraduate programs. We do not currently have the infrastructure to switch into "high gear" right away, nor do we have the students available. However, once students are engaged, it is disruptive and discouraging to them and to faculty if resources and support are not provided in a steady, consistent fashion.

I will start by reiterating my support for the existing Scholarship for Service program. It needs to include additional funding for more students, and to allow recipient institutions to pursue curricular development and enhancement, but is otherwise functioning well.

K–12

Our children are the future. We should ensure that as they are being taught how to use the technology of tomorrow that they also are getting a sound background in what to do to be safe when using computers and networks. We teach children to cover their mouths when they sneeze, to wash their hands, and to look both ways when they cross the street—we should also ensure that they know something about avoiding phishing, computer viruses, and sharing their passwords. Older students should be made familiar with some of the more complex threats and issues governing computing especially privacy and legal implications.

Avenues for teaching this material certainly include the schools. However, too many of our Nation's schools do not currently offer any computing curriculum at all. In many schools, all that is taught on computers is typing, or how to use the WWW to research a paper. Many states have curricula that treat computing as a vocational skill rather than as a basic science skill. Without having a deeper knowledge of the fundamentals of computing it is more difficult to understand the issues associated with privacy and security in information technology. Thus, teaching of computing fundamentals at the K–12 level needs to be more widespread than is currently occurring, and the addition of cyber security and privacy material nationally should be considered as part of a more fundamental improvement to K–12 education. Recently the leaders of the computing community released recommendations on how the Federal Government's Networking and Information Technology Research and Development (NITRD) Program could be strengthened to address shortfalls in computer science education at the K–12 level.[4]

Consideration should be given to encouraging various adjunct educational opportunities. Children's TV is one obvious venue for conveying useful information, as is WWW-based delivery.

Computing has a significant diversity problem. Cyber security and privacy studies appear, anecdotally, to be very attractive to students from underrepresented groups, including females. Presenting meaningful exposure to these topics at the K–12 level might help encourage more eager, able young people to pursue careers in those or related STEM fields.

Undergraduate Degrees

Of the thousands of degree-granting institutions throughout the U.S., perhaps only a few hundred have courses in computer security basics. These courses are usually offered as an elective rather than as a part of the core curriculum. As such, basic skill such as how to write secure, resilient programs and how to protect information privacy are not included in standard courses but relegated to the elective course. This needs to change or we will continue to graduate students who do not understand the basics of the area but who will nonetheless be producing and operating consumer computing artifacts.

More seriously, we have a significant shortfall of students entering computing as a major area. Last year was the first year in six where the enrollment of undergraduates in CS did not decline. The significance of this concern is not only impor-

[4] *http://www.acm.org/public-policy/NITRD__Comment__final.pdf*

tant from a national competitiveness stand-point, but it implies that we will have a significant shortfall of trained U.S. citizens in the coming years to operate in positions of national responsibility. We are already off-shoring many critical functions, and without an increase in the U.S. production of computing majors, this will pose a significant national security threat.

Graduate Degrees

There is disagreement within the field about the level of education needed for some positions in the work force. Clearly, there is a range of positions, some of which may only require an under-graduate degree, but many that require at least a Master's degree. Some educators (myself included) believe that a strong undergraduate degree in computing or software engineering, or in some other field related to cyber security (*e.g.,* criminal justice), should be obtained followed by a graduate degree to ensure appropriate depth of knowledge.

There continues to be a need for Ph.D. graduates in cyber security. Individuals at this level are needed for advanced concept development in academia, industry and government. Generally, a Ph.D. is also required for faculty positions and some senior technical supervisory positions. Given the strong demand in this field and the number of institutions with need of faculty with experience in security or privacy topics, there will undoubtedly be a continuing and increasing demand for graduates at this level.

One of the issues facing researchers in academia is the lack of access to current commercial equipment. Most funding available to researchers today does not cover obtaining new equipment. Universities also do not have sufficient resources to equip laboratories with a variety of current products and then keep them maintained and current. As a result, unless faculty are adept at striking deals with vendors (and few vendors are so inclined) they are unable to work with current commercial security products. As a result, their research may not integrate well with fielded equipment, and may even be duplicative of existing solutions. The situation is in some senses similar to that of the 1980s when major research institutions were able to seek grants to get connections to research networking, but has evolved to a point where almost every college and university has network access. We now need a program to fund the instantiation of experimental laboratories for cyber security with a cross-section of commercial products, with an eventual goal of having these be commonplace for teaching as well as research.

Some faculty and their students are willing and able to work on classified problems so long as that work is near enough to their home institution to make travel reasonable. The best solution is to have a facility on campus capable of supporting classified research. This is not common on today's campuses.[5] It is not inexpensive to build or retrofit a facility for classified processing, and it is costly to staff and maintain it. Research grants almost never cover these costs. A Federal program to identify institutions where such facilities would be useful, and then build and support them might be helpful.

To produce graduate students requires resources for stipends, laboratory equipment, and general research support, as well as support for the faculty advisors. Given university overhead costs, it will often cost more than $250,000 over a period of years for a graduate student to complete a Ph.D. That support must be consistent, however, because interruptions in funding may result in students leaving the university to enter the work force. Additionally, there needs to be support for their advisors, usually as summer salary, travel, and other expenses. Here again, consistency (and availability) are important. If faculty are constantly worried about where the money will come from for the coming year, some will choose to leave the field of study or academia itself.

Other Disciplines

Computing is not the only area where advanced research can and should occur. As noted earlier, the cyber security "ecology" includes issues in economics, law, ethics, psychology, sociology, policy, and more. To ensure that we have an appropriate mix of trained individuals, we should explore including training and support for advanced education and research in these areas related to cyber security and privacy. Encouraging scholars in these areas to work more closely with computing researchers would provide greater synergy.

On possibility that should be explored is to expand the current Scholarship for Service program in a manner that includes students taking advanced degrees with a mix of cyber studies and these other areas; as an example, the program might

[5] As an example, I need to travel over 70 miles from Purdue to be able to find a cleared facility.

fund students who have completed an undergrad in cyber security to obtain a J.D., or a student with a degree in public policy obtaining an M.S. in cyber privacy. Upon graduation those individuals would be highly qualified to enter government service as policy experts, prosecutors, investigators, and other roles where there is currently an urgent and growing need for multidisciplinary expertise.

Training

There are many people working in the IT field today who have security and privacy as one of their job functions. Given the pace of new tool development, best practices, new threats, and other changes, it is necessary that these individuals receive periodic training to stay current with their positions. Many 3rd-party organizations are currently providing such training (although the expense per student is significant), but as demand grows it seems unlikely that these efforts will scale appropriately. It is also the case that not all individuals who currently need such training either know they need it, or can afford it.

There should be an effort made, perhaps through DHS and/or the Department of Education, to provide ongoing training opportunities to the workforce in a cost-effective and timely manner. This might be by way of some mechanism that is delivered over the Internet and/or through community colleges. "Train the trainer" opportunities should be considered as well.

Note that this is not the same as continuing education as it assumes that the students involved already know how to perform their jobs. Rather, this is training in new tools and techniques to enable individuals to stay current in their positions.

Adult Education

The majority of citizens today using personal computers do not know anything about computer security, yet they are common targets for fraud and abuse. Phishing, Spam, and botnets are all generally targeted at home computers. Most people do not know that they need additional knowledge about security, and those that do are often unsure where to go to obtain that knowledge.

This is an area where many different techniques could be employed. Having educational modules and resources available online for citizens to review at their leisure would seem to be an obvious approach. Providing incentives and materials for ISPs, community groups, public libraries, and perhaps state and local governments to offer courses and information would be another possibility. Public television is yet another avenue for education of the general population about how to defend their computing resources.

Coupled with this effort at citizen education might be some program to provide access and ratings of products that could be obtained and deployed effectively. Unfortunately, there are many ineffectual products on the market, and some that are actually malicious in the guise of being helpful. Providing resources for citizens to get product details and up-to-date information on what they should be doing could make a large difference in our national cyber security posture.

Professional Education

We have many people in professional roles who use computers in their work, but who were not exposed to computing education during their formal studies. These positions include law enforcement personnel, judges, doctors, lawyers, managers, C-level executives, bankers, and more. In these various professions the individuals need education and training in cyber security and privacy basics as they relate to their jobs. They also need to be made aware that lack of security has real consequences, if not for their organizations, then for the country, and that it should be taken seriously.

Many professional organizations already provide organized training along these lines; for example, the National White Collar Crime Center (NW3C) offers courses for law enforcement personnel. Mechanisms need to be developed to help scale these offerings and motivate more professionals to take them. Where no such courses are available they need to be developed in conjunction with experienced and competent advisors who understand both the material involved and the issues specific to the professions.

Concluding Remarks

The cyber security problem is real. Informed warnings have been large ignored for years, and the problems have only gotten worse. There is no "silver bullet" that will solve all our problems, nor are solutions going to appear quickly.

Any program to address our problems will need to focus on deficiencies in our regulatory system, in the economic incentives, and in user psychology issues as well as the technical issues. We need a sustained, significant research program to address questions of structure, deployment, and response. We need a significant boost

to law enforcement to act as an effective deterrent. Most of all, we need a comprehensive and wide-reaching program of education and training to bring more of the population in line to address the problem than the small number of experts currently involved.

Thus, there needs to be a significant investment made in both students and research in cyber security and privacy. The PITAC report made a conservative recommendation of tripling available research funding per year in 2005, although the committee privately discussed that 4–5 times the base could be productively spent. We noted that much of the money designated as R&D funding is really spent on the "D" portion and not on research. In the years since that report, it is unlikely that the amount has more than doubled, and that is due, in part, to standard inflationary issues and across-the-board increases rather than any targeted spending.

A conservative estimate for FY 2010 would similarly be to at least triple the current allocation for basic research and for university fellowships, with some nontrivial fractions of that amount dedicated to each of privacy research, cyber forensics tools and methods for law enforcement, to cyber security infrastructure, and to multidisciplinary research. Equal or increasing amounts should be allocated in following years. An additional annual allocation should be made for community and professional education. This is almost certainly less than 1 percent of the amount lost each year in cyber crime and fraud in the U.S. alone, and would be an investment in our country's future well-being. Again, it is important to separate out the "R" from the "R&D" and ensure that increases are made to the actual long-term research rather than to short term development.

There must be a diverse ecology of research funding opportunities supported, with no single agency providing the vast majority of these funds. Opportunities should exist for a variety of styles of research to be supported, such as research that is more closely aligned with specific problems, research that is better coordinated amongst larger numbers of investigators, research that involves significant numbers of supporting staff beyond the PI's, and so on. The NITRD Coordination Office is well-suited to assist with coordination of this effort to help avoid duplication of effort.

There are many good topics for research expenditures of this order of magnitude and beyond. As already mentioned, there are numerous problems with the existing infrastructure that we do not know how to solve including attribution of attacks, fast forensics, stopping botnets, preventing spam, and providing supply chain assurance. More speculative tasks include protecting future architectures including highly portable computing, developing security and privacy metrics, creating self-defending data, semi-autonomous system protection, building high-security embedded computing for real-time controls, and beyond. The PITAC report listed 10 priority areas, and the National Academies report lists more. The community has never had a shortage of good topics for research: it has always been a lack of resources and personnel that has kept us from pursuing them.

Above all, we must keep in mind two important facts: First, protection in any realm, including cyber, is a process and not a goal. It is an effort we must staff and support in a sustainable, ongoing manner. And second, as with infections or growth of criminal enterprises, a failure to appropriately capitalize the response now will simply mean, as it has meant for over two decades, that in the future the cost will be greater and the solutions will take longer to make a difference.

References

1. *Cyber Security: A Crisis of Prioritization;* Report from the President's Information Technology Advisory Committee; National Coordination Office, NITRD; 2005.

2. *Toward a Safer and More Secure Cyberspace;* Seymour E. Goodman and Herbert S. Lin, Editors; National Academy Press; 2007.

3. *Unsecured Economies: Protecting Vital Information;* McAfee Corporation; 2008.

4. *Security Cyberspace for the 44th Presidency;* Center for Strategic & International Studies; 2008.

Acknowledgements

I wish to acknowledge comments and assistance provided to me in preparing this testimony from Becky Bace, Steve Cooper, Dan Geer, Harry Hochheiser, Lance Hoffman, Carl Landwehr, Ed Lazowska, Victor Piotrowski, Bobby Schnable, Carlos Solari and Cameron Wilson. Despite listing their names here, none of those individuals necessarily agrees with, nor endorses any of my comments or opinions.

The CHAIRMAN. Thank you.

Senator Nelson, will you change that? Good. OK.

Extremely good presentations. I apologize, again, for the lack of attendance. I just use all the other meetings going on, but I don't know how somebody would manage to not be here.

You've talked, the four of you, about saying that you produce teachers, and government labs produce people who go into universities, and the rest of it. On the other hand, I think you, Dr. Lewis, said that we don't have anybody learning anything about this. Senator Snowe and I are putting together a bill which would emphasize, and we would welcome anybody's cosponsorship, and she's from the Intelligence Committee, and Senator Nelson is from the Intelligence Committee. You said people pass through engineering and they just simply never come across the word "cyber" problems. And I'm wondering how you think this can be changed.

I mean, one, we've got to change the way the private sector looks at it. That would be my second question. I just put out the first, but, second, how do we begin to train a body of people? This ought to be the most fascinating, cerebral, national-security, I'm-a-good-American problem that exists. But, it's not attracting people. Why?

Dr. LEWIS. A couple of reasons. First, you know, we've had a larger decline across the board—and I know this Committee is well aware of it—in science, technical education, engineering, mathematics. We've underfunded it for years, and now we're reaping the benefit. I was at a classified briefing, a couple of months ago, where we were comparing how foreign countries were doing to the United States. And it used to be we were ahead. And in the briefing we had a couple of months ago, the foreign countries had caught up, and somebody said, "How did that happen?" And the answer is, "Well, if you don't spend the money for 15 years, they're going to catch up."

So, what I would say—and I think this fits in with Dr. Spafford's remarks—the way to get more students is to pay people, to give them incentives to go into this. It is fascinating, but we know that students sit down and say, "How am I going to make a living?" And right now we don't have the demand for it. So, fund people to go in; that would be a great idea. Think about things like competitions; that would help. And get industry to pay attention to this so there will be demand at the receiving end.

The CHAIRMAN. Well, then why doesn't that work? It's manifestly self-evident for big and small companies. I think AT&T and Verizon and others are pretty familiar with it. It just cries out for the smartest, most creative people, who can make a huge difference in the future of their country.

Dr. LEWIS. We've been having—I'll just say, quickly—we've been having a discussion with some of the people working in the government on this about what we call the "conversion experience." And it's like that Saul-on-the-road-to-Tarsus moment, where the light bulb goes over your head. And we're trying to figure out how many people have realized this is a major national security problem. And I don't think enough have, is the short answer.

Dr. SPAFFORD. Sir, I'll add to this. This year, nationwide, we probably have about 50 or 60 new Ph.D.s in the field, total. And of those, perhaps 10 to 15 are going to return to their home countries to start businesses to compete against the U.S., because our visa policies won't let them stay. Of the remaining 45, about half

will go into industry, possibly to startups, and the remaining will go into university environments, where they will be teaching classes and perhaps creating a new generation of students. But, that means that we have perhaps an annual increment of 15 to 20 new faculty a year for thousands of educational institutions across the country, and tens of thousands of commercial organizations. The numbers are way too small. And in part it is—as Dr. Lewis noted, we are not portraying an image that this is an exciting career path, or one that is—they can make a living at. Instead, we hear about how jobs are going offshore to other companies—other countries, how we don't have enough people in the stem disciplines. For many years, some of our best students went off to become bankers and lawyers. Maybe not our best students, considering what happened, but——

[Laughter.]

Dr. SPAFFORD.—nonetheless, those career paths seem to be much more attractive.

So, there's a—it's a total issue.

The CHAIRMAN. Yes.

Dr. AMOROSO. Mr. Chairman, I would offer just an—a personal note. When I was a high school student, it was right around the time that Arno Penzias and Bob Wilson won the Nobel Prize for the Big Bang Theory, and Bob Wilson came and gave a talk to my science club or high school—something like that. And it was about the most inspiring thing I ever saw, and I decided I wanted to go to Bell Laboratories. And there were a group of people in my generation that really wanted to do that.

I think we've skipped a generation since then. I've noted, in my prepared remarks, that I've been an adjunct professor at Stevens Institute of Technology for 20 years. My graduate class right now is about 98 percent foreign national, and we're teaching cybersecurity to non-Americans.

I think we have a unique opportunity, though. Everyone in this room, when we were young, you amused yourself, probably, outside, running around. What do kids amuse themselves with now? Xbox and computer games and so on. We've got a generation of youngsters who, I think, are ripe and ready for careers in this area, and I think legislation should take full advantage of that and try and attract these youngsters into careers in the areas that were noted.

The CHAIRMAN. Our legislation will.

Senator Udall?

Senator UDALL. Thank you, Mr. Chairman.

I think some of you have touched on this a little bit, but I'd like you to go into more depth for me. Are we confident, in the United States, that the U.S. infrastructure, whether it's a power grid or the telephone networks, as you've described, Dr. Amoroso, with AT&T, our oil and gas infrastructure, our infrastructure on our airlines, controlling airlines in the air—are we confident that we can withstand a major cyberattack to these kinds of networks? And what are the scenarios you see if we had an attack? What scenarios would follow from there?

Dr. WEISS. Let me answer that question. In fact, if you'd bear with me, can I just go back to what you were asking before, and then I'll directly answer?

Senator UDALL. [Inaudible.]

Dr. WEISS. I'm kind of, in a sense, a fish out of water, not being a traditional IT person. I'm a control-system engineer. One of our big problems is, when you look at the cybersecurity centers of excellence, they're in the computer science departments, they are not in the electrical engineering department, they are not in the chemical engineering department, they are not in the mechanical engineering department, they are not in the nuclear engineering department. So, part of what we have is this very much of a dichotomy between what people normally associate with a computer and what we, in industry, use as computers. And I go back to the fact that they are very different.

I ended up getting a master's, through University of Washington, on strategic planning for critical infrastructures. Our textbook on cybersecurity was written by Matt Bishop, from U.C. Davis, and it was dated 2003. It was a 1,000-page college textbook. The words "SCADA" or "control system" were not mentioned once. We are—it's a different area. It is a very, very interdependent, functional type of discipline that needs to be there, and it isn't. So, I just wanted to bring that into play.

And the other thing, too, is, one of the differences in industry, if you will, is, this is a huge business issue, as well as security issue. And part of our problems can be unintentional cyberincidents. They can have almost the same impact—shutting down nuclear plants, you know, having pipeline ruptures. These have already happened. They weren't intentional, but it still shut down plants, killed people, et cetera. Part of it is because we don't have adequate training, we don't have adequate standards. So, I just wanted to go back.

Now, if you'll—if you will, I'll address what you were asking.

Our systems were initially designed—were originally, and still, to this day, designed—for performance. Security is an add-on. Are our systems vulnerable? They're very vulnerable. The issue, to me, is—and this is another aspect, too—some of our biggest control-system cyberincidents did not come from the Internet and did not come from Windows. They were control-system issues. These control-system issues destroyed equipment, shut down plants. The Northeast outage lasted 3 days—actually, 1 to 2 days, but I'm saying 3. And the reason is, there was no damage to equipment. When you damage equipment—I assume you've seen the tape of Aurora. This is where, by cyber alone, they destroyed a large diesel generator. Physically destroyed it. This is what we're talking about. It's destruction of equipment that takes months—many, many months to procure. And we don't even make that equipment in the U.S. anymore.

So, when you're asking about international issues, think about, Where do we get those, and how do we know even what's going to be replaced, is going to do what we want, and maybe not have a Trojan embedded? This is a very, very difficult, complicated issue that I want to get across. It is very real. And it's not those laptops

that you see that we're concerned about, it's equipment—very expensive, very long-term design-and-procure equipment.

Dr. LEWIS. I take a little different view—I'll just jump in real quick—because I think—you know, the—one of the things you've heard is that there's a real risk here, and there's a real potential for damage. We want to make sure that doesn't happen. But, we're under attack right now. We're suffering losses. Sometimes people say we have to worry about an electronic Pearl Harbor. We probably had our electronic Pearl Harbor in 2007. And we might have had one in 1998 or 1999. And, as you've heard from all of us, you know, we just kind of say, "Oh, well, gee, that's too bad." You know? So, we are, every day, suffering big losses, and I don't know which—which loss do you want to talk about? Do you want to talk about breaking into NASA and stealing launcher designs? Do you want talk about stealth? Do you want to talk—what do you want to talk about?

So, I worry more about the loss of information, and I think that's the attack—the beauty of this is, if you fix one, you sort of address the other. We do have to worry about the attacks on critical infrastructure, but right now we are being—I don't know what the right word is—"robbed," I guess; "robbed" would be the right word—by foreign entities, of our most valuable technology, and we have to stop that.

So, I'm not worried about some crisis in the future. I'm worried about the crisis we're in now.

The CHAIRMAN. Senator Nelson?

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. By the way, Dr. Lewis, we could not even get the NASA IG to investigate the stealing of those rocket designs through the Internet at NASA.

Dr. Weiss, you're right, they did that demonstration project, known as Aurora through digital means to hack into the power plant's generator and cause it to shut down.

We've got a serious problem in national security. I have the privilege of serving with the immediate past chairman of the Intelligence Committee, and we see it there. For example, *Defense Daily* has just written that hackers are managing to invade our military computer systems, though the defenses are competent to stymie most of the attempts. This is what General Chilton, the Strategic Command commander, says, "Every day, there are attempts to penetrate our network, some of which are successful, but many, many more are defeated."

This Senator's office computers have been invaded three times in the last month, and one of them looks pretty serious, as if it's talking to a computer in some international arena.

Dr. Amoroso, you mentioned in your statement, about the *Times* report today on Conficker. It infected a large number of computers and turned that into one of the largest botnets.

How should the private sector best deal with this type of problem, when it's so fast-moving that you get a result and you get a defense in a matter of days or even hours? Should we go to the National Institute of Standards and Technology, to set some sort of

baseline cybersecurity standards or set up some kind of best practices? What should we do?

Dr. AMOROSO. I have some thoughts on that. I think there are two things you need to do.

First off, you need a stopgap, because we can't do research to solve a problem that could happen in the next hour. Need something that will deal with the problem immediately. And I believe the network is the place to do that. So, most of the international and domestic carriers have these big—you can think of them as, like, a big sponge that can absorb energy, or like a big old shock absorber in the network, so when the Conficker botnet is being aimed at the Department-of-This, or this or that agency, or some company, we can soak up all that energy. Now, again, that is a stopgap. That works today. That's how we stop attacks now. You know, plumbers sitting in the bowels of our network, basically, with these, you know, big shock absorbers.

The long-term solution is, we've got to fix computing. I think Dr. Spafford is right. I mean, we've got a lot of broken software out there, including the software that's probably running on your computers. You click an "I Accept" button when you install it, and if you read that language, it basically says, "This computer is—you know, this software doesn't work, you know, and you're accepting all the risk." So, I think a lot of our research activity needs to be directed to fixing the endpoints.

So, stopgap, near term, primarily focused on network; research, long term, primarily focused on computing. And I think that's the right approach for our Nation.

Senator NELSON. Well, Mr. Chairman, I'll conclude and just say that I think, in our subcommittee, as I serve you and the full Committee, that we want to look at NIST and the NSF, at new opportunities for them to examine these questions that have been raised this morning.

Thank you.

The CHAIRMAN. Thank you, Senator Nelson.

And, in fact, in Olympia Snowe's and my bill, which I hope that you'll all cosponsor, we go very aggressively after this question, and through the National Science Foundation, of awarding scholarships, just anything we can, to attempt to get people into the field and get them stimulated. NIST is this national treasure which nobody here ever goes to visit. You can't—you can't sort of do NIST from a distance, you've got to be there, you've got to talk. I remember going, 20 years ago, and they said they hadn't seen a Senator in 5 years. It was a bit depressing.

So, my question to you, you've got this question of penetration testing. I like that phrase. It's the proactive probing and testing of cyberdefense. The idea behind conducting penetration testing is to better now where our vulnerabilities are. There are a lot of companies that probably know this, but I don't know what kinds of companies are aware of their vulnerabilities. It's a very basic, naive question. I'm pretty sure that the majority have absolutely no idea of what they are. So, question number one, How do you reach out, the government can't do this advertising like DOD can, saying they're being hacked into 3 million times a day, and people just pass over that, how do you reach out to the private sector, which

is going through tough times, but will be going through far tougher times if they're not alert to this, and get them aware of it? How do you do it? One, you've got to get students interested. It's just shocking to hear you say that they're not. How do you get business to inventory itself? Or, if you don't, does NIST do it?

Dr. WEISS. Can I respond to a couple of your questions?

One is, there is——

The CHAIRMAN. You'll have time, Doctor.

Dr. WEISS. OK. In the electric industry, there are currently some requirements—they're not near as comprehensive as they should be, but they do attempt to drive that.

But, I wanted to mention one other thing, because I keep going back to this. An industrial control system is very different than an IT system. You had mentioned penetration testing. Penetration testing is fine for a traditional business-type IT system or network. If you penetration test a legacy control system, you will shut it down or kill it. You will be your own hacker. We've had this happen often, not just throughout the U.S., but all over the world.

Part of what we need to do is develop—and again, think about this for the Smart Grid, too—when you start talking about these legacy devices, these are not your Microsoft operating systems, these are your legacy devices—this is, again, what would be designed by a chemical engineer or an electrical engineer, a mechanical engineer, a nuclear engineer. We need to have a set of, essentially, testing criteria and assessment criteria specific to that. And training needs to be there for that. And I go back to—curricula needs to be there for that. And I just want to mention this, because too often we're lumped with everybody else, "Go do what everybody else is doing." It will shut us down.

The CHAIRMAN. Well, the reason I'm asking it is because sometimes you don't have the time to start a generation of people on their way. You have to do it. And it's an absolute priority. A number of years ago when some of this began to be talked about, I got all of our chemical companies on the Ohio River to come together, and I said, "How are you protecting yourselves? You're on the water. By definition, your penetration is easy." And then I met with them again, a year or so later, and they had put sidearms on the hip of the people who were on the other side of the chemical plant who were letting the workers in.

Now, that was shocking to me. That was shocking to me. These are very sophisticated chemical companies, and I don't understand why they're not onto this.

VOICE: Mr. Chairman?

The CHAIRMAN. Oh, no. Maria, I've got to shut up, because three votes just started, and Maria's got a much better question than I did.

Senator CANTWELL. I don't know about that, Mr. Chairman, but I have enjoyed—well, I actually haven't enjoyed the discussion; I think it's been a very enlightening panel, but it is pretty disgusting that we've had more people trying to cook up exotic toxic assets than willing to spend their time killing bugs on the Internet. So, it is a poor statement about where people have been lured.

But, Dr. Weiss, back to your point about control systems and the curriculum. And we're proud that you're a U Dub alum. What kind

of curriculum are you talking about, from the sense of power system engineering or——

Dr. WEISS. Well——

Senator CANTWELL.—control systems? Obviously you know, in the Northwest, with so many hydroelectric dams, we get the fact that hacking that system is a——

Dr. WEISS. Yes.

Senator CANTWELL.—big problem.

Dr. WEISS. Yes. And it's—by the way, it's all over. I mean, because everybody has industrial systems. But, I've given lectures at the University of Illinois. I gave one at Mississippi State. I've given one—or at the Naval Post-Grad at National Defense University. The issue that we need——

Senator CANTWELL. Are we talking about a 4-year degree in control systems, or are you talking about a basic computer science——

Dr. WEISS. No, what I'm really looking at is two things. One is just, maybe, a semester or a quarter dealing with this, because, within the chemical engineering department or within nuclear, you're going to have courses on control-system theory. You don't have that, if you will, in computer science. Computer science will have everything pointed toward traditional IT.

Senator CANTWELL. So, are you saying that this is an add-on program to either computer science or——

Dr. WEISS. I see it as a joint——

Senator CANTWELL.—power-system engineering or——

Dr. WEISS. I see it as a joint effort, because you can't divorce the computer science part. This is computers. But, for our world, you can't—you can't divorce the science from it, either.

Senator CANTWELL. Can we go to NIST and what——

Dr. WEISS. Sure.

Senator CANTWELL.—exactly do you think needs to—needs to happen, as far as security standards at NIST, and how we get there, given that there's obviously a lot of organizations, like the IEEE and others, that are involved in standard-setting, and they can help in creating a framework for government to get at this sooner.

Dr. WEISS. Let me, if you'll bear with me, explain where this came from. It was the law of unintended consequences. And that was FISMA—you know, the Federal Information Security Management Act—is a Federal law for all Federal agencies, and NIST developed, you know, the framework, NIST SP 800–53, et cetera. The law of unintended consequences was, people didn't realize one of the Federal agencies happened to have been the Tennessee Valley Authority, with coal-fired power plants and hydro plants and nuclear plants and dams. The other thing they didn't realize is that the Bonneville Power Administration is a Federal agency. And what was happening is, when those agencies tried to use the existing IT standards, which was what NIST SP 800–53 was, they failed their IT security audits, because they weren't appropriate. So, what we ended up doing—I was actually under contract to MITRE, supporting NIST on this—is, we went back and we looked at—because I am a member of IEEE and ISA and all of the other organizations—and what we did was to look at what was missing

in those standards that needed to be included for industrial control systems, and then we extended NIST SP 800–53 to address that.

And then what we did is something beyond that. We went back and looked at things like the Bellingham, Washington, gasoline pipeline rupture, the Browns Ferry Nuclear Plant broadcast storm, et cetera. And we asked, "Now that we've done this, would—if you would have followed the NIST standards, would you have been able to prevent that?" So, we looked at this to basically say, "Is this going to be usable?"

Senator CANTWELL. So, we don't have standards for control systems in place, or—and we don't have a mechanism for updating them, either, as new facilities come online or as new technology is introduced.

Dr. WEISS. Well, these are systems—and, again, I keep—I hate to keep coming back to the point, they're different—these systems have lifetimes of 10 to 20 years. These are not 3 to 5 years, like with your traditional IT. So, once you put these in, you are not going to replace them, no matter what you find, in terms of vulnerabilities. We have to work around that.

Dr. LEWIS. Just quickly, NIST has two big problems. OK? Problem one, we're still in sort of a compliance culture, you know, "Here's your paper plan. Did you live up to your paper plan? Hey, that's great." And we all know, from FISMA, that you can get a good FISMA grade and still be totally insecure. So, we have to move out of the compliance mode to something else, and sometimes people talk about attack-based metrics or metrics that are based on what's actually happening, and not on some piece of paper.

The second big problem NIST has is that the offense does not inform the defense. Now, it does a little, but it doesn't adequately. So, we know what's going on in the offensive world. We even have offensive people, ourselves. But, they don't hook up with NIST and they don't help NIST write their standards.

And so, if you could fix those two things——

Senator CANTWELL. And is fixing that having people feel comfortable in having that dialogue, that issue about——

Dr. LEWIS. Yes, they're——

Senator CANTWELL.—legal vulnerability? Is that——

Dr. LEWIS. Exactly right.

Senator CANTWELL.—right.

Dr. LEWIS. There are some legal impediments that I think we'll have to look at, laws that might have made sense in the 1980s, but may not work in the more interconnected world we're in today.

Senator CANTWELL. You know, I think this is a very important issue, Mr. Chairman, in the sense that, you know, you get an operating system, people beat on it for months and months and months and months, and try to break the system before it's really introduced. But, you're saying, on a system that meets the basic compliance, doesn't have that kind of stress test to it, and then doesn't have the advancements and technology checked up, as well. It sounds like we need a much more robust system at NIST.

Dr. LEWIS. Robust and nimble. And I think Dr. Spafford's remarks pointed out that the people who are our opponents, they pay a lot of attention to this, they spend a lot of money, and they come up with new attack vectors every week, if not every month.

Senator CANTWELL. But, what is that, what's the "nimble" part? What would the "nimble" part be in a structure like that?

Dr. LEWIS. "Nimble" would be paying attention to what's actually happening now on the networks, paying attention to, "What are the attacks that are succeeding?" and adjusting the standards to make sure that that's what you're protecting against. This is going to be hard, because, in some ways, the NIST process is—I love NIST, but it's a—can be a little stately, at time. And the criminals, the nation-states we're going against, they evolve very quickly. So, "nimble" means finding a way to make the NIST standards a bit more responsive to external events.

Dr. SPAFFORD. I would just like to add——

The CHAIRMAN. And quickly, because——

Dr. SPAFFORD. Yes, sir—that one of the things——

The CHAIRMAN. Like, 1 minute.

Dr. SPAFFORD.—that I really should stress, if we want to respond is, we need to look to our law enforcement community, not so much—standards are certainly going to help, but standards are a minimum, always. What we really need to do is, we also have to have a deterrent capability for our commercial marketplace. Many of the things that are going on are basically criminal, and if we could deter that, increase the risk for those criminals, it would go a long way toward helping fix the situation.

Senator CANTWELL. And international cooperation on catching them.

Dr. SPAFFORD. That would definitely be part of it.

Senator CANTWELL. Thank you, Mr. Chairman. Thank you for this important hearing.

The CHAIRMAN. Thank you, Senator Cantwell.

And I'll just close it by thanking all of you. Again, I'm mortified by the lack of attendance, but, you know, such is life. That's why I had to scream and yell to try to get Maria back, because she's a real IT expert, Senator Cantwell.

This is going to be the first of a number of hearings on this subject. We're going to drive it home. We've got to raise the profile of cybersecurity, we've got to get the President, after the 60-day review, is it Melissa who's doing that?, to get the person; and then, behind that there's probably got to be an advisory board so that it's just pounding in on the President, who happens to love this kind of subject. You know, thank heavens for that. I mean, he knows about it, but he needs to know a lot more about it, and I think he'll be very proactive. And then, the creativity for the long-term solutions, and promote public awareness, and protect civil liberties, which always have to be a part of it, as I remember from the FISA debate.

But, what you've given us is a very, very excellent first-hearing set of analysis, and we are the better for it, and we thank you.

Hearing is adjourned.

[Whereupon, at 11:17 a.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. OLYMPIA J. SNOWE TO DR. JAMES A. LEWIS

Question 1. The Internet has revolutionized some many different areas of society and the economy. The innovation, adoption, and sheer size of the Internet are simply unparalleled. The Internet currently comprises of more than 1.5 billion users, 570 million computers, and 174 million websites. However, we will eventually enter a new iteration of the Internet with the migration from IPv4, a 32-bit addressing space, to IPV6, a 128-bit addressing, which provides 5 x 10^{28} IP addresses for every individual on earth (or 6.5 x 10^{23} addresses for every square meter of the earth's surface). In addition, Internet Corporation for Assigned Names and Numbers (ICANN) plans to allow the expansion of generic top level domains from the current 21 domains to eventually hundreds if not thousands. Both of these efforts as well as others present amazing opportunity and potential for the evolution of the Internet but also present significant challenges with cybersecurity.

What will this eventual expansion of IP addresses and domains mean with respect to cybersecurity and threats? With domain name system techniques such as fast fluxing, pharming, DNS cache poisoning, being used by botnets, it could present an even greater challenge because there is even a greater pool of resources available, right?

Answer. We've built an insecure global network. Now we are expanding to include more people, more devices and more services. We don't have adequate mechanisms to manage risk, and "Internet governance" is weak. If we continue on the same path, risk will only increase. ICAO (the International Civil Aviation Organization) which sets minimum standards for civil aviation, may be a good precedent for thinking about national will have to cooperate.

Question 2. The first sentence of Cisco's 2008 Annual Security Report states "Compared to previous years, online criminals are becoming even more sophisticated and effective, employing a greater number of relatively smaller, more targeted campaigns to gain access to sensitive data." Another report by IBM's Internet Security Systems X-Force Team highlighted that the number of new malicious Websites in the fourth quarter of 2008 alone surpassed the number seen in the entirety of 2007 by 50 percent and that new categories of threats affecting clients are on the rise, specifically in the areas of malicious documents, multimedia applications, and potentially Java applications which are easy to host on the Web.

It seems that tackling the issue of cyber threats is a little bit like "whack-a-mole," in that you discover and fix one vulnerability but then due to the sophistication and resourcefulness of the criminals, ten more cyberattacks pop-up. So how can we realistically deal with this, which seems to be a perpetually increasing problem?

Answer. The best approach is to stop playing whack-a-mole, a reactive game where you let the enemy set the agenda, to a proactive approach that starts to reshape the cyber environment. We need a national policy that blends improved technology, international engagement, regulation and standards and consumer training. A holistic approach or a comprehensive approach is the only way to get out of the "whack-a-mole" cycle.

Question 3. The IBM report stated that of "all the [cyber] vulnerabilities disclosed in 2008, only 47 percent can be corrected through vendor patches." Last April, the New York Times reported thousands of corporate executives were targets of a phishing attack that attempted to install malware on the recipients' computers. Security experts found that less than 40 percent of antivirus programs were able to identify and stop the attack. Cisco's report mentioned that criminals are getting access to computers and networks by exploiting weaknesses in technologies, software, and systems.

Is the software industry really performing the necessary due diligence to make sure their products are up to par with respect to security or do security concerns/ vulnerabilities take a back seat to getting the product or next version out in the

market? It seems as if, with all the patches, that the industry does not have the foresight to proactively fill the holes, correct?

Answer. Some IT companies perform due diligence and some don't. A coordinated approach that held companies to common standards or to shared best practices would help reduce many easy avenues for attack. The Government can help companies cooperate, use its purchasing power to drive improvement, and consider regulation where necessary. One way to think about this is the automobile industry—we give Americans some minimal training, but the real reason the rate of fatal accidents has decreased is because cars are built more safely. At first, car companies resisted safety improvements, but after the government mandated some basic requirements, they now compete to provide safer cars. We need to start the same dynamic for the Internet.

Question 4. With the countless web applications, add-ons, software, shareware, how can we imbed a "best practices" or set of cybersecurity standards that better protect users and their computers from vulnerabilities or cyberattacks? A criminal can target a seemingly innocuous web browser add-on application to gain access to one's computer or a network, right?

Answer. The only way to make the cyber environment more secure is to use a combination of tactics and approaches—better law enforcement, international cooperation, improved products, and increased consumer awareness. This is like any other crime—we can never eliminate crime but we can significantly decrease the rate of crime and the rewards to criminals.

Question 5. While a notable percent of threats and attacks originate here domestically, the vast majority come from overseas. The 2007 cyberattacks on DOD, DHS, and Commerce were all initiated by unknown foreign entities. China is most prolific host of malicious Websites. Russia, with the Russian Business Network (RBN), is a hot-bed of activity.

We can certainly do a lot to address the domestic threats as well as to protect our borders, but what can we specifically do across our borders to address the source of the attacks?

Answer. We need a comprehensive approach that takes action in the intelligence, diplomatic and law enforcement spheres. We can shape the international environment to be more secure if we engage—this will happen automatically and the ad hoc and erratic approach the U.S. has taken in the past only guarantees failure. Stronger law enforcement cooperation, a visible deterrent policy and a diplomatic strategy that creates norms for international behavior and, perhaps, sanctions for noncompliance can reduce cross-border threats. The U.S. needs to integrate cybersecurity into all of its foreign policy engagement and not treat it as an afterthought.

Question 6. As you may know, Chairman Rockefeller and I created the E-rate program, which provides discounted telecommunications services to schools and libraries, as an amendment to the Telecommunications Act of 1996. The E-rate program has been instrumental in making Internet access available to schools and libraries—before the program, only 14 percent of schools had Internet access. Today, nearly 100 percent of America's schools, 94 percent of individual classrooms, and 98 percent of public libraries are now wired. Internet access and information technology have truly enhanced the learning environment and process as well as better prepared our students for entering the digital global economy. With E-rate, students are learning how to use the Internet as a research tool, for collaborating on assignments and projects with individuals in other geographical locations, and downloading homework—the list goes on.

However, various studies and surveys indicate that students have a false sense of security when using the Internet—they're often too lax in their security with usernames/passwords and they more readily provide personal information online. Are we doing enough for K–12 students in teaching them about cybersecurity? It seems we could do a lot more to infuse cybersecurity education into school's curriculum, do you agree?

Answer. To continue the information highway analogy, just as we make students take driver's ed before they can venture out onto the roads, we need to think of some kind of reasonable cyber training. Cyber training should avoid hysteria and I am not recommending that we "license" users, but since we as a nation are increasingly dependent on the use of the Internet, it is time to provide formal training on safe Internet use for students.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. OLYMPIA J. SNOWE TO DR. JOSEPH M. WEISS

April 17, 2009

Senator Snowe:

Thank you for the opportunity to respond to your very pertinent questions. Because of the subject matter's importance, I enlisted a distinguished group of information technology (IT) security, telecommunications, and control systems security experts to assist me in responding to your questions. This group includes Dr. Marshall Abrams, Mr. Walt Boyes, Mr. Jacob Brodsky, Mr. Eric Cosman, Mr. Philip Craig Jr., Mr. Lou Hatton, Mr. Marcus Sachs, Dr. Phyllis Schneck, Mr. Jonathan Stanford, and Mr. Robert Webb. It is our consensus view that a more effective oversight climate, which includes better standards and possibly new legislation and regulation, is needed.

The responses are both general in nature and specific to my personal expertise in the area of cybersecurity for industrial automation and control systems (IACS). IACS are an integral component of our critical infrastructure. They are not as well understood and sometimes not as well-protected as the majority of our cyber assets and are among our most important assets. IACS are very different from office or enterprise IT systems, too. The security philosophy that works for office and enterprise IT systems is to save the servers, because that's where the data is. On the plant floor, the requirement is to preserve the real time operating systems and maintain IACS availability. That is, the fundamental difference between IT and IACS in addressing security is the best way to protect a security breach in IT is to STOP the flow of data and protect the servers whereas in IACS stopping the flow of data could be disastrous to the process and to safety. You can see how different the response of each sector to a cyber incident must therefore be.

Security is hard work, often with no obvious short-term reward (*e.g.,* an immediate impact on the bottom line). Therefore, people in every sector—public, private, traditional IT, and IACS—often avoid doing security. Those entrusted to improving security of cyber systems are often frustrated by their peers and management who do not believe cybersecurity is necessary or even important. Moreover, they feel frustration due to the amount of effort required to overcome organizational politics or other roadblocks so resources for improvements in technology, processes, and procedures can be brought to bear.

According to the April 5, 2009 issue of *The Washington Post,* years after the Department of Interior had been warned its computer network was dangerously exposed to hackers—and ordered by a Federal judge to fix the problems—the vulnerabilities remained. New threats and threat agents arise continually, such as a recently indicted ex-employee of Pacific Energy Resources.[1] After being informed he would not become a permanent employee, this individual compromised the leak detection systems of several off-shore oil platforms while being logged in from his home. With the emphasis on Smart Grid currently, it is important to note that on April 7, 2009, Michael Assante, Vice President and Chief Security Officer of the North American Electric Reliability Corporation (NERC), issued a letter concerning the inadequacy of the electric industry's approach to identifying critical assets under NERC cybersecurity standards.

We believe there should be an integrated team of IT and IACS professionals from the public and private sectors working on cybersecurity, with a dedicated leader who understands the issues and who preferably will not leave in a year.

In conclusion, there is a need for a more effective oversight climate, which includes better standards and possibly new legislation and regulation, is needed.

Please let me know if we can answer any questions or provide further input to support the proposed legislation.

Respectfully,

JOE WEISS, PE, CISM,
Applied Control Solutions, LLC, Cupertino, CA.

Question 1. The Internet has revolutionized many different areas of society and the economy. The innovation, adoption, and sheer size of the Internet are simply unparalleled. The Internet currently comprises of more than 1.5 billion users, 570 million computers, and 174 million websites. However, we will eventually enter a new iteration of the Internet with the migration from IPv4, a 32-bit addressing

[1] "Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System", By David Kravets, March 18, 2009, *wired.com, http://blog.wired.com/27bstroke6/2009/03/feds-hacker-dis.html.*

space, to IPv6, a 128-bit addressing, which provides 5 x 10^{28} IP addresses for every individual on earth (or 6.5 x 10^{23} addresses for every square meter of the earth's surface). In addition, Internet Corporation for Assigned Names and Numbers (ICANN) plans to allow the expansion of generic top level domains from the current 21 domains to eventually hundreds if not thousands. Both of these efforts as well as others present amazing opportunity and potential for the evolution of the Internet but also present significant challenges with cybersecurity.

What will this eventual expansion of IP addresses and domains mean with respect to cybersecurity and threats? With domain name system techniques such as fast fluxing, pharming, DNS cache poisoning, being used by botnets, it could present an even greater challenge because there is even a greater pool of resources available, right?

Answer. By itself, the expansion of the IP addresses and domains does not increase or reduce the cyber vulnerabilities. However, an article titled "IPv6 Security Challenges" in the February 2009 issue of Computer, published by the IEEE Computer Society, raises multiple security issues associated with IPv6. While current attack methodologies might not work as well in a new world of virtually unlimited IP addresses and domain names, new technical problems will emerge that can be leveraged by criminals, terrorists, and state-sponsored groups. The real issue is not the size of the address space, but whether there is a minimum security threshold that must be met. This is almost impossible to do retroactively, which is why standards are so important. Rather than taking the approach of connecting first and then trying to apply security, we have to start thinking in terms of systems and endpoint capability. This can allow applying traditional IT security principles like defense-in-depth to systems having little or no defense at the present time. If a device or system cannot demonstrate a minimum level of security, it should never be connected to the network. Most importantly, we must realize that the principles of good security are only partially dependent on good technology. Users must adopt and use good technology, but equally important, they must adopt and use good security practices. Any security hardware or software can be rendered inadequate if users paste their passwords on post-it notes. Like today's world, it will continue to be an arms race to find and either exploit or mitigate problems.

There is a quiet but significant risk with all IP addresses—they need to be treated with augmented privacy—analogous to the social security number, which until relatively recently wasn't considered as needing protection. The association of IP addresses to machine name or function provides a virtual roadmap to the underlying IP communications systems and connectivity. The case of the Associated Press (AP) v the State of Arkansas (Dec. 18 2008) marked the beginning of the press and public both wanting to use the Freedom of Information Act (FOIA) to obtain association of machine name and function with IP addresses. The court ruled against the AP in this case, but the AP filed an appeal. Going forward, this case could pose a threat if reversed. New addressing gives us a fresh chance to handle IP addresses more carefully.

The corollary to this question is: "Will a significant increase in the number of intelligent devices increase the cyber threat to the Smart Grid and other industrial applications?" The answer is that this will significantly increase the "threat space." Furthermore, many of these new devices are not designed to be cyber secure. Many legacy devices in industrial networks that will continue to be deployed for years were not designed with cybersecurity features. In fact, some of these devices, new and old, have been exploited already. It should also be noted that electric transmission, distribution, and power plants currently use mostly serial communications and will continue to use some amount of serial communications even with the Smart Grid. The greater the dependence on network connectivity, the greater the consequences will be when a network fails, or is deliberately used as an attack vector that targets specific communications or inter-connected devices. Consider the August 2003 Northeast blackout, which was not a cyber initiated event. However, the consequences were enormous—estimated at over $7 billion. Imagine the consequences of such a blackout over most of the United States, with major power shortages lasting many months instead of a few days. You can begin to appreciate the potential increase in risk of a "Smart Grid," dependent on thousands or millions of intelligent devices, all carefully managing power generation and usage. To be sure, much of our infrastructure has been very resilient and fault tolerant because it was diverse, independent, and not interconnected. The pervasive network connectivity envisioned in the expansion of the IP address space provides tremendous opportunities. But it also increases the possibly and consequences of such failures. Only by assuring significantly improved security, and an adequate level of independence and diversity in our critical infrastructure's cyber resources, can we

minimize the possibility of such horrific events, and realize the advantages we anticipate gaining.

Our experience in the last 5 years has shown that many organizations will not adopt adequate measures to assure security. Measurable security outcomes should be mandated by law in any cases where the infrastructure is critical to the well-being of our citizens. To be sure, the industry should be allowed to participate in determining how best to meet those requirements.

The first sentence of Cisco's 2008 Annual Security Report states "Compared to previous years, online criminals are becoming even more sophisticated and effective, employing a greater number of relatively smaller, more targeted campaigns to gain access to sensitive data." Another report by IBM's Internet Security Systems X-Force Team highlighted that the number of new malicious Websites in the fourth quarter of 2008 alone surpassed the number seen in the entirety of 2007 by 50 percent and that new categories of threats affecting clients are on the rise, specifically in the areas of malicious documents, multimedia applications, and potentially Java applications which are easy to host on the Web.

Question 2. It seems that tackling the issue of cyber threats is a little bit like "whack-amole," in that you discover and fix a single vulnerability but then due to the sophistication and resourcefulness of the criminals, ten more cyberattacks pop-up. So how can we realistically deal with this, which seems to be a perpetually increasing problem?

Answer. One has to assume that most, if not all, networks and/or systems will be attacked and that we must provide a resilient capability. Resilience comes from the concept of defense-in-depth. It means that there should be layers of defense such as perimeter defense, network segmentation, and system isolation to the degree possible so that if one layer is penetrated others may provide protection. Technology and procedures must be developed to permit continued operations even while under attack. In fact, "attack resiliency" might become a new theme, replacing "attack prevention" as the focus of security operations.

One of the key challenges with the Internet is that anyone, anywhere, can send any amount of traffic content to any destination—and by virtue of the design of the Internet, the payload arrives, even if it causes a cyber train-wreck in its wake.

Researchers, companies and governments worldwide have produced incredible science in identification of malicious Internet use (*e.g.,* botnets) that disrupts the communications fabric that may be needed for critical operations. Public-private partnerships transcend national boundaries to identify and prosecute criminals behind Internet abuse. However, these efforts cannot respond in real-time, and do not solve the existing challenge of disabling malicious Internet traffic.

The Internet communications fabric must be made more intelligent to not route and deliver malicious network traffic. In addition to saving bandwidth for both emergency and commercial use, this would kill the profit model for the botnet culture and severely lessen the effectiveness of distributed denial-of-service (DDoS) attacks.

For IACS, that could even mean developing a dedicated network independent of the Internet—an "Industry Net" designed for the performance and security needs of industry. Again, one must remember that even with the move to IP communications, there will continue to be serial communications that also need to be addressed. Another reason resilience is important for industrial control systems is that their operating lifetimes are so long, typically 10 to 20 years or longer. These are not changed out because of cyber threats and consequently, restoration is of great concern.

There are many similar challenges in the world today—defense against physical weapons and against evolving diseases are good examples. An excuse like "but it is hard" is not a reason to give up or ignore applicable threats. We can and must fight these threats with a combination of the best intelligence, the best technology, defense-in-depth, and resilient and reconfigurable systems that can function without connectivity when isolation may be necessary. All of this must be integrated and flexible (so that new technologies are not precluded). Economic incentives or binding legal measures are needed so that critical components of the infrastructure's connectivity—be they hardware, software, or people—don't compromise the whole. The weakest link in the chain is currently an issue for the electric industry, where the Federal power entities are being held to higher standards (*e.g.,* the Federal Information Security Management Act and related NIST standards such as Special Publication 800–53) than the non-Federal power entities (*i.e.,* the North American Electric Reliability Corporation [NERC] Critical Infrastructure Protection [CIP] cybersecurity standards). That is, the non-Federal power entities are weak links that could cause failure of the Federal power entities, and that is plain wrong.

The IBM report stated that of "all the [cyber] vulnerabilities disclosed in 2008, only 47 percent can be corrected through vendor patches." Last April, the New York Times reported thousands of corporate executives were targets of a phishing attack that attempted to install malware on the recipients' computers. Security experts found that less than 40 percent of antivirus programs were able to identify and stop the attack. Cisco's report mentioned that criminals are getting access to computers and networks by exploiting weaknesses in technologies, software, and systems.

Question 3. Is the software industry really performing the necessary due diligence to make sure their products are up to par with respect to security or do security concerns/vulnerabilities take a back seat to getting the product or next version out in the market? It seems as if, with all the patches, that the industry does not have the foresight to proactively fill the holes, correct?

Answer. In short, no, the industry does have the foresight to proactively fill the holes. However, a combination of factors precludes it from effectively doing so.

Good Security is a TEAM effort, and the software industry is only a part of the team. Good security is combination of good software design, good system hardware and software architecture, the successful application of good policies and procedures to protect systems, and many other factors. Much of the software industry is very serious about proactively improving software security; it has spent millions to do so. But unless the user demands and adopts the upgrades, it can have little effect. In the case of IACS, the user is often precluded from adopting such upgrades, because they will destroy the basic functionality of the system we are trying to protect. In those cases, the user must find alternative means to protect that system and its vulnerable software. Regulation that requires the user to take measures to protect vulnerable software will help to drive toward better results.

Competition and the marketplace is currently a significant factor; you are correct—the drive to get products out limits the amount of improvement (if any) that occurs with each new version. Requirements to protect key systems and to develop more secure software can both help the vendors overcome some of the impediments to better software and systems.

The lack of comprehensive standards—vendors are reluctant to invest sufficient funds on security, because their work may be eclipsed by regulation or standards or another vendor's defacto standard—so they wait. Users are reluctant to improve security because they don't believe they will be able to recover their investment, especially if a different (than their approach) standard or law is adopted after they spend significant funding—so they wait. All of this is exacerbated by a lack of well-accepted evidence that we are facing a real problem. So while there have been significant improvements, they have not been fast enough or far reaching enough to preclude a major event within our critical infrastructure. Carefully developed requirements that demand action can help to break the waiting game, and get the involved stakeholders working together to achieve more meaningful results sooner.

There is no "simple" silver bullet solution that can be "plugged into" each important system to protect it. Each system or application typically requires an engineered solution. Each system is different, and because of the limitations on the ability of legacy equipment to use new or upgraded software, alternative solutions must often be developed. Solutions can be developed, and there is specialty software and equipment designed to protect inherently weak or vulnerable systems. But it must be evaluated and configured for the system in which it is applied.

Unfortunately, patching security holes will be with us for the foreseeable future, particularly for commercial-off-the-shelf (COTS) software, including operating system software. Software that incorporates cybersecurity best practices will certainly help. However, there is a large body of older legacy software in production use that is vulnerable to malicious code. A recent report regarding several hundred security breaches spanning several years found that the vast majority of successful data breaches were attributed to systems not being managed in accordance with best security practices. A lack of patching does not cause breaches; the core issue is a lack of management engagement and an ignorance of well-known security practices.

In general purpose IT systems, automated patching can be a solution to address "buggy" software. IACS incorporating general purpose operating systems are often modified by the IACS supplier. Consequently, automated patching can cause problems not typically encountered in general purpose systems. IACS typically have minimal computing resources. Applying traditional security approaches, such as Anti-virus software, can be too resource-intensive. This might result in unintended IACS shutdowns. Consequently, more work is needed to identify appropriate security practices for IACS. Until IACS security matures, vulnerable components must be isolated from attack vectors that would not usually apply in a general computing system environment.

Many IACS cyber vulnerabilities stem from issues besides "buggy" software. The infamous "Aurora" demonstration by the Idaho National Laboratory used dial-up modems to physically destroy hardware, in this case, a diesel generator. Inadequate security testing can miss cyber vulnerabilities and inadequate security planning can be the cause of cyber incidents. The interactions of various types of software can cause unanticipated cyber problems. As examples, interactions between normally-functioning software caused a fossil Tower plant to overstress a turbine,[2] and a nuclear power plant to automatically shutdown.[3] In both instances, no IT security policies were violated, but it is clear that such policies should have addressed the scenarios leading to the events. There is a critical need for effective IACS security policies and robust security testing procedures that address the unique characteristics of these types of systems and their operating environments.

Question 4. With the countless web applications, add-ons, software, shareware, how can we imbed a "best practices" or set of cybersecurity standards that better protect users and their computers from vulnerabilities or cyberattacks? A criminal can target a seemingly innocuous web browser add-on application to gain access to one's computer or a network, right?

Answer. You are correct in that a criminal can target a seemingly innocuous web browser add-on application to gain access to one's computer or a network. Consequently, multiple organizations are attempting to establish cybersecurity standards and guidelines. Good standards that are kept up to date are very important. However standards are only one component in achieving adequate cybersecurity. The complete picture includes robust and meaningful standards; effective implementation of the standards; improvements in software and equipment security; developing new types of secure equipment; and an effective information sharing process for addressing new attack vectors and threats commensurate with the risks they present.

Harmonization to a single set of standards and guidelines would help. However, user awareness is often lacking, and existing standards and guidelines aren't always followed. As an example, a security consultant left compromised thumb drives in a parking lot to demonstrate via social engineering that people would pick up the drives and insert them into their corporate workstations even though such actions were against their company's IT policies. Sadly, they did as expected! Senior management must create a culture of security among employees, while addressing cultural barriers between IT and other organizations. To secure a modern IACS, there must be a coordinated effort between IT security, networking and telecom organizations, and the control systems personnel. Management must provide an adequate governance structure that includes appropriate oversight and adequate resources for ensuring security. Unfortunately, such a coordinated approach to security is not the norm.

IACS security must be approached from an engineering perspective, founded on the goal of improving system safety, performance, reliability, and availability in the face of cyber-related threats. The fundamental objective is to protect the integrity of the process, and security is an element of that. The IACS community should develop an adequate risk assessment methodology, an acceptable vulnerability assessment methodology, and measures of acceptable levels of security that are based on the goals of system safety, performance reliability, and availability.

To be sure, there currently is a lack of information sharing regarding IACS cybersecurity events. For IACS, the U.S. Computer Emergency Response Team (CERT) and industry Information Sharing and Analysis Centers (ISACs) do not work well. It is unlikely that the proposed DHS ICS–CERT will either. Government should fund, collaborate with, but NOT manage, a Cyber Incident Response Team (CIRT) for Control Systems. This can overcome private industry's concerns about confidential information being made public. It could ensure that vetted experts will be available as a resource for incident handling and mitigation, and that private industry will not be punished for disclosing cyber incidents. An example is MITRE's *A*viation *S*afety *I*nformation *A*nalysis and *S*haring (*ASIAS*) System used by the Federal Aviation Administration (FAA) to promote open exchange of safety information. I have information related to more than 125 IACS cyber incidents. One of the major conclusions of the 9/11 Commission was the lack of "connecting the dots" regarding terrorism threats. Similarly, there has been no attempt to "connect the dots" with

[2] "Runkle and Labbe—"Optimizing Turbine Life Cycle Usage and Maximizing Ramp Rate," 16th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference, 49th Annual ISA Power Industry (POWID) Conference, Volume 49/ISA Volume 466, 4–9 June 2006, San Jose, California.

[3] Operating Experience Report OE26424—Isolation of Condensate Demineralizer System and Subsequent Plant Trip While Testing Software Change (Hatch), 3–11–08.

IACS cyber incidents. Such an effort could pay multiple dividends in helping to develop more appropriate policies and architectures, better procurement guidelines, and more buy-in of the real problems that exist.

While a notable percent of threats and attacks originate here domestically, the vast majority come from overseas. The 2007 cyberattacks on DOD, DHS, and Commerce were all initiated by unknown foreign entities. China is most prolific host of malicious websites. Russia, with the Russian Business Network (RBN), is a hot-bed of activity.

Question 5. We can certainly do a lot to address the domestic threats as well as to protect our borders, but what can we specifically do across our borders to address the source of the attacks?

Answer. It is doubtful we can separate the domestic and international threats. Just as the Internet is global, computer suppliers are also global. For example, Dell and Hewlett Packard are domestic brands, but are manufactured all over the world. Toshiba is a Japanese company that supplies North America, while the former IBM laptop product line was purchased by a Chinese company—Lenovo. Domestic suppliers obtain components and software from international sub-suppliers. Supply chains provide another opportunity for malicious activity. The same applies to IACS environments, where there is a mix of domestic suppliers like General Electric, Emerson, and Honeywell, and international suppliers like Siemens from Germany, Areva from France, and ABB from Switzerland. At least one major American IACS supplier has a SCADA software development center in China.

There are a number of steps we can take to improve security, especially where critical infrastructure is involved. We can filter and limit communications, and provide network segmentation and isolation of our more important systems. We can monitor communications to identify traffic patterns and share information on unexpected and problematic network activities.

Properly identifying the sources of attacks or exploits assumes that adequate forensic capabilities exist. In several recent cyber incidents, even the newest control systems did not have logging capability adequate to identify the causal factors of the incidents. Current IT forensic approaches may actually harm IACS or inhibit critical restart capabilities. Consequently, there is a critical need to develop an appropriate IACS forensics methodology and related set of protocols.

As you may know, Chairman Rockefeller and I created the E-rate program, which provides discounted telecommunications services to schools and libraries, as an amendment to the Telecommunications Act of 1996. The E-rate program has been instrumental in making Internet access available to schools and libraries—before the program, only 14 percent of schools had Internet access. Today, nearly 100 percent of America's schools, 94 percent of individual classrooms, and 98 percent of public libraries are now wired. Internet access and information technology have truly enhanced the learning environment and process as well as better prepared our students for entering the digital global economy. With E-rate, students are learning how to use the Internet as a research tool, for collaborating on assignments and projects with individuals in other geographical locations, and downloading homework—the list goes on.

Question 6. However, various studies and surveys indicate that students have a false sense of security when using the Internet—they're often too lax in their security with usernames/passwords and they more readily provide personal information online. Are we doing enough for K–12 students in teaching them about cybersecurity? It seems we could do a lot more to infuse cybersecurity education into school's curriculum, do you agree?

Answer. Yes, I agree we need to infuse more cybersecurity into the K–12 education process. Computer access is becoming ubiquitous and social networking sites are breaking down previous privacy barriers. There should be a better awareness among K–12 students regarding security and the need to take security seriously. This is especially important given the high level of social activity prevalent amongst youth, who are early adopters of potentially risky online technology. Our young should be educated that security risks exist when visiting websites, downloading files from untrusted sites, chat and instant messaging, and file sharing. They also need to understand cyber threats are more than just a threat to computers, but can also lead to personal threats like cyber bullying and cyber stalkers. Cybersecurity awareness education should be integrated into curricula in the same way that "looking both ways before crossing the street" has been.

There is also a need to reach out to young people attending college and within the work force. Almost all new technologies have digital communication capability, which means there are often cyber vulnerabilities. Cybersecurity is interdisciplinary in nature, and should be taught as such. Currently, IT security certifications and

audit metrics exist for the information security community. However, there are no certifications for IACS security or audit metrics unique adapted for IACS. We need to "train the trainers" regarding IACS security and develop the appropriate curricula. This is a pressing need when it is seen that there are at best a few hundred people in the entire world who are security subject matter experts specifically relating to IACS.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. OLYMPIA J. SNOWE TO DR. EDWARD G. AMOROSO

Question 1. The Internet has revolutionized some many different areas of society and the economy. The innovation, adoption, and sheer size of the Internet are simply unparalleled. The Internet currently comprises of more than 1.5 billion users, 570 million computers, and 174 million websites. However, we will eventually enter a new iteration of the Internet with the migration from IPv4, a 32-bit addressing space, to IPv6, a 128-bit addressing, which provides 5 x 10^{28} IP addresses for every individual on earth (or 6.5 x 10^{23} addresses for every square meter of the earth's surface). In addition, Internet Corporation for Assigned Names and Numbers (ICANN) plans to allow the expansion of generic top level domains from the current 21 domains to eventually hundreds if not thousands. Both of these efforts as well as others present amazing opportunity and potential for the evolution of the Internet but also present significant challenges with cyber security.

What will this eventual expansion of IP addresses and domains mean with respect to cyber security and threats? With domain name system techniques such as fast fluxing, pharming, DNS cache poisoning, being used by botnets, it could present an even greater challenge because there is even a greater pool of resources available, right?

Answer. You highlight two important changes in the Internet ecosystem. From a security perspective, the key issue is that "change" always creates opportunities for vulnerabilities to be exploited. The industry's transformation to IPv6 is an example of a particularly significant change, and, consequently, a significant opportunity for exploitation, particularly in light of the proliferation of new and increasingly sophisticated threats. AT&T and other network service providers continuously evaluate IPv6 deployment, and all service providers have the potential to play a greater role in addressing such vulnerabilities by building robust, smart-network system capabilities. Government policy should support such private sector efforts.

With respect to domain name expansion, AT&T has filed comments with ICANN demonstrating that new generic top level domain names should not be introduced until a whole range of Internet ecosystem issues, including Internet security and stability, are adequately studied and understood.

Question 2. The first sentence of Cisco's 2008 Annual Security Report states "Compared to previous years, online criminals are becoming even more sophisticated and effective, employing a greater number of relatively smaller, more targeted campaigns to gain access to sensitive data." Another report by IBM's Internet Security Systems X-Force Team highlighted that the number of new malicious Websites in the fourth quarter of 2008 alone surpassed the number seen in the entirety of 2007 by 50 percent and that new categories of threats affecting clients are on the rise, specifically in the areas of malicious documents, multimedia applications, and potentially Java applications which are easy to host on the Web.

It seems that tackling the issue of cyber threats is a little bit like "whack-a-mole," in that you discover and fix one vulnerability but then due to the sophistication and resourcefulness of the criminals, ten more cyberattacks pop-up. So how can we realistically deal with this, which seems to be a perpetually increasing problem?

Answer. Your analogy is apt, and we must not allow the game to get out of control. The most realistic way to deal with threats of this nature is to take a holistic approach, assuring that throughout the ecosystem, we have developed sophisticated and flexible cyber security capabilities. To this end, government policies should encourage private sector investments in innovative security capabilities. As a network provider, cyber security is an AT&T priority; we seek to assure that the information, applications, and services our customers want are secure, accurate, reliable, and available wherever and whenever they are desired through the provisioning of a highly-intelligent network capable of identifying and mitigating cyberattacks. Our intelligent network capabilities are an important component of a proactive approach to cybersecurity which includes prevention and rapid mitigation of threats as they emerge.

Question 3. The IBM report stated that of "all the [cyber] vulnerabilities disclosed in 2008, only 47 percent can be corrected through vendor patches." Last April, the

New York Times reported thousands of corporate executives were targets of a phishing attack that attempted to install malware on the recipients' computers. Security experts found that less than 40 percent of antivirus programs were able to identify and stop the attack. Cisco's report mentioned that criminals are getting access to computers and networks by exploiting weaknesses in technologies, software, and systems.

Is the software industry really performing the necessary due diligence to make sure their products are up to par with respect to security or do security concerns/vulnerabilities take a back seat to getting the product or next version out in the market? It seems as if, with all the patches, that the industry does not have the foresight to proactively fill the holes, correct?

Answer. Cyber security should be viewed as an ecosystem and not be viewed as the exclusive domain of either software application providers or network providers. Effective cyber security solutions will rely upon smart networks working hand in hand with software based solutions. As noted above, the government should seek to encourage private sector investment in both innovative network security and edge application security technologies. From my perspective, both application and network providers are committed to addressing these challenges, but vulnerabilities remain and need to be addressed, particularly through the increasing availability of application software that allows end-users within an enterprise to "turn off" unneeded features.

Question 4. With the countless web applications, add-ons, software, shareware, how can we imbed a "best practices" or set of cyber security standards that better protect users and their computers from vulnerabilities or cyberattacks? A criminal can target a seemingly innocuous web browser add-on application to gain access to one's computer or a network, right?

Answer. You have identified a significant and difficult challenge because, as you note, criminal can target an add-on application to gain control. I believe that the key to embedding best practices is in virtualization and greater centralization of cyber security capabilities. This represents the best opportunity to respond to real-time attacks and remove bad decisionmaking from end-users. In this respect, network service providers can help address these issues by offering comprehensive network based managed security services across their customer base. AT&T is investing heavily in making our core network the first line of defense in cyber security for our entire customer base. We see it as our responsibility to educate our customers about the need for professionally-managed cyber security in order to protect them from exploitation.

From a software perspective, dealing with complexity is a significant challenge, so complexity must be reduced so that secure software can be more easily written to include operating system design techniques, such as the inclusion of a policy enforcement kernel, to guard against a range of attacks.

Question 5. While a notable percent of threats and attacks originate here domestically, the vast majority come from overseas. The 2007 cyberattacks on DoD, DHS, and Commerce were all initiated by unknown foreign entities. We can certainly do a lot to address the domestic threats as well as to protect our borders, but what can we specifically do across our borders to address the source of the attacks?

Answer. A cooperative and coordinated response by governments and the private sector is necessary in order to contain cyber threats. These threats are possible only because of the inherently anonymous nature of the global digital infrastructure as it has evolved, and because illicit behaviors may find a safe haven, for a variety of reasons, in places throughout the world. For this reason, a constructive trans-national public and private sector dialogue on cyber security must ensue, so that globally coordinated, cooperative solutions can emerge. This dialogue can build on the cooperation and discussions that are already taking place with strong private sector involvement in order to respond to global cyber threats.

Question 6. As you may know, Chairman Rockefeller and I created the E-rate program, which provides discounted telecommunications services to schools and libraries, as an amendment to the Telecommunications Act of 1996. The E-rate program has been instrumental in making Internet access available to schools and libraries—before the program, only 14 percent of schools had Internet access. Today, nearly 100 percent of America's schools, 94 percent of individual classrooms, and 98 percent of public libraries are now wired. Internet access and information technology have truly enhanced the learning environment and process as well as better prepared our students for entering the digital global economy. With E-rate, students are learning how to use the Internet as a research tool, for collaborating on assignments and projects with individuals in other geographical locations, and downloading homework—the list goes on.

However, various studies and surveys indicate that students have a false sense of security when using the Internet—they're often too lax in their security with usernames/passwords and they more readily provide personal information online. Are we doing enough for K–12 students in teaching them about cyber security? It seems we could do a lot more to infuse cyber security education into school's curriculum, do you agree?

Answer. Yes. With the widespread use of computers at the earliest ages today, it makes sense to start educating our children about digital literacy—both "online safety" as well as "cybersecurity awareness." Online safety means focusing on children's use of the Internet in a way that protects their privacy, security and wellbeing, and respect for others. Cybersecurity education is also essential and involves teaching kids about the basics of cybersecurity and importance of understanding the harm that viruses and other threats post to them personally and to society at large.

AT&T, we are teaching children to be alert and aware online and providing services that help them create a safer online experience. For example, AT&T's parental controls allow parents, at no cost, to control the content to which their children may obtain access to the Internet. In the context of the AT&T Hometown Tours program, we have visited more than 100 communities nationwide and taught children key Internet safety skills, such as protecting computers against viruses, hackers and spam, as well as reviewing age-appropriate content, and the potential dangers associated with social networking. We also have implemented an online safety program with our partner iKeepSafe, and the DARE officers, reaching children in grades K–5 in thousands of communities across the country.

These online safety initiatives help keep families aware of the threats around them, but they supplement, and are not a substitute for, holistic network-based and software-based cyber security practices.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. OLYMPIA J. SNOWE TO DR. EUGENE H. SPAFFORD

Question 1. What will this eventual expansion of IP addresses and domains mean with respect to cyber security and threats? With domain name system techniques such as fast fluxing, pharming, DNS cache poisoning, being used by botnets, it could present an even greater challenge because there is even a greater pool of resources available, right?

Answer. I have spoken with several of my colleagues about this question, and the best answer we can provide is "We do not know for certain." The vast majority of our problems are traceable to two major shortcomings: poor security of host endpoints, and a significant problem in traceback and attribution of misbehavior. Neither of these problems is likely to see any change resulting from more domains or a switch to IPv6.

If we have more addresses with a switch to IPv6 (the only likely way to expand addresses) we will have a situation where it is more difficult—and highly impractical—for attackers to scan networks to find unadvertised but vulnerable hosts. However, it will also be more difficult for defenders to scan networks to look for unauthorized connections.

The biggest issue with IPv6 is that very little of the current security infrastructure (firewalls, intrusion detection, etc) is designed to work with IPv6. Thus, a switch won't result in any significant benefits directly, but could introduce new problems if the infrastructure isn't upgraded simultaneously.

Having new domains and a larger IP space will both make it more difficult to "blacklist" addresses in a reliable manner. The expanded IP and namespace could make it easier for bad actors to hide or relocate their operations, but current resources seem sufficient to hide most of their activities, so it is difficult to say if a switch would result in any significant change.

Question 2. It seems that tackling the issue of cyber threats is a little bit like "whack-a-mole," in that you discover and fix one vulnerability but then due to the sophistication and resourcefulness of the criminals, ten more cyberattacks pop-up. So how can we realistically deal with this, which seems to be a perpetually increasing problem?

Answer. I addressed this, in part, in my written testimony. The solution is to pay more attention to the development of the systems that are deployed. In large part, this means that we need to spend more on development of hardened, minimal, systems. We must recognize that we need to invest in development of systems that are better suited to use in high-risk environments, rather than general-purpose systems designed without strong practices.

We also need to invest in law enforcement and follow-up, to increase the risk for people who abuse systems. This works in other arenas, but is largely missing in cyber.

A key issue is one of economics and false value. Right now, most users of computing technology (the Federal Government included), buy and deploy systems without really valuing the potential losses if the systems are compromised. As a result, the systems are purchased, configured, and operated as cheaply as possible, without due consideration given to the risk potential. (Analogy: constructing military facilities out of cardboard because it is cheap, without thinking about the potential risks and needs over the longer term.)

We can do better, but it requires both discipline and funding.

Question 3. Is the software industry really performing the necessary due diligence to make sure their products are up to par with respect to security or do security concerns/vulnerabilities take a back seat to getting the product or next version out in the market? It seems as if, with all the patches, that the industry does not have the foresight to proactively fill the holes, correct?

Answer. Industry could do better, but the incentives aren't there. To perform more tests or develop better tools would not only take time, but cost money. Right now, there is no real business reason for companies to expend extra resources to harden systems because there is little evidence that customers are willing to pay the extra cost. Customers large and small continue to buy systems that have been shown to have a poor record of safety, and make choices based on purchase price rather than on added security features.

This is related to my answer to Question 2—we need to create an environment where it is possible to have multiple systems tailored for specific applications rather than trying to adapt the same general-purpose systems that are used in people's homes for use in business and government. With a variety of systems, those that require more testing and security features could have the extra cost included—although other factors would need to be brought to bear to ensure that the more secure systems were purchased and deployed in environments where needed rather than the less-expensive (and less well-designed) systems. This goes to creating an environment where management is held responsible for failures, and there are recognized standards and metrics for good security.

Question 4. With the countless web applications, add-ons, software, shareware, how can we imbed a "best practices" or set of cyber security standards that better protect users and their computers from vulnerabilities or cyberattacks? A criminal can target a seemingly innocuous web browser add-on application to gain access to one's computer or a network, right?

There are some technical approaches currently under development that could help with these issues. However, as noted above, unless the extra cost is minimal or otherwise amortized, they may not widely adopted.

As suggested by your answer, some better standards would definitely help. So would better enforcement of existing laws and rules. However, I am skeptical that any new regulations would be especially helpful until current laws and regulations are enforced on a more regular and consistent basis.

Question 5. We can certainly do a lot to address the domestic threats as well as to protect our borders, but what can we specifically do across our borders to address the source of the attacks?

Answer. The answer to this comes in parts.

First, there are criminal activities originating in friendly or neutral countries. We can do more by ensuring that we have reciprocal cyber crime treaties in place. The law enforcement officials in those countries must have the training and resources to assist in investigation of offenses.

Second, there are criminal activities originating in unfriendly countries. In these cases, we have not obtained significant assistance in law enforcement investigations. In some cases, the activities are sanctioned or even supported by those governments. Where there is little cooperation, other leverage is necessary such as financial or political sanctions. Techniques currently used to address international criminal activities involving drugs, counterfeiting, and other criminal activity with these countries could also be employed in cyber, although I am uncertain if enabling legislation would be required.

In both cases we need to raise the priority of enforcement and provide the necessary resources to match that prioritization.

Question 6. However, various studies and surveys indicate that students have a false sense of security when using the Internet—they're often too lax in their security with usernames/passwords and they more readily provide personal information online. Are we doing enough for K–12 students in teaching them about cyber secu-

rity? It seems we could do a lot more to infuse cyber security education into school's curriculum, do you agree?

Answer. Yes, I agree. I will note that we also don't do a very good job of teaching basic computer science in K–12.

We used to have an effective and far-reaching program through my center (CERIAS) for K–12 education but were forced to discontinue it because there were no sources of support. We also had to discontinue our community education programs for the same reason.

○