# ENHANCING AND IMPLEMENTING THE CYBERSECURITY ELEMENTS OF THE SECTOR-SPECIFIC PLANS

## JOINT HEARING

BEFORE THE

## SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY AND SCIENCE AND TECHNOLOGY

JOINT WITH THE

## SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

## COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 31, 2007

**Serial No. 110–82**

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

48–977 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

## COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRARA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

---

## SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

JAMES R. LANGEVIN, Rhode Island, *Chairman*

ZOE LOFGREN, California
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
AL GREEN, Texas
VACANCY
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

MICHAEL T. MCCAUL, Texas
DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
PETER T. KING, New York *(Ex Officio)*

JACOB OLCOTT, *Director & Counsel*
DR. CHRIS BECK, *Senior Advisor for Science & Technology*
CARLA ZAMUDIO-DOLAN, *Clerk*
DR. DIANE BERRY, *Minority Senior Professional Staff Member*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

SHEILA JACKSON LEE, Texas, *Chairwoman*

EDWARD J. MARKEY, Massachusetts
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
YVETTE D. CLARKE, New York
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*
DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
PETER T. KING, New York *(Ex Officio)*

MATHEW WASHINGTON, *Director*
ERIN DASTE, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
COLEY O'BRIEN, *Minority Senior Counsel*

# CONTENTS

# ENHANCING AND IMPLEMENTING THE CYBERSECURITY ELEMENTS OF THE SECTOR-SPECIFIC PLANS

---

**Wednesday, October 31, 2007**

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY,
JOINT WITH THE
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION,
*Washington, DC.*

The subcommittee met, pursuant to call, at 3:45 p.m., in Room 311, Cannon House Office Building, Hon. James R. Langevin [chairman of the Emerging Threats, Cybersecurity, and Science and Technology Subcommittee], presiding.

Present: Representatives Langevin, Etheridge, Pascrell, Jackson Lee, Clarke, McCaul, and Lungren.

Mr. LANGEVIN. The Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, and the Subcommittee on Transportation Security and Infrastructure Protection will now come to order.

The subcommittees today are meeting to receive testimony on enhancing and implementing the cybersecurity elements of the sector-specific plans. I will begin by recognizing myself for the purpose of an opening statement.

Good afternoon. Over the past few months, the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology has held numerous hearings to assess how far-reaching our cybersecurity vulnerabilities are and how best to address them. Today, we will be focusing on the extent to which cybersecurity has been implemented as part of our 17 different sector-specific plans.

We are joined today by the Transportation Security and Infrastructure Protection Subcommittee led by Chairwoman Sheila Jackson Lee of Texas and Ranking Member Lungren. Though this is our first joint hearing on the subject, I very much look forward to working with the chairwoman and ranking member, along with my ranking member on the subcommittee on these issues of the 110th Congress as it continues.

Although critical infrastructure protection is usually associated with physical protection of facilities, there is a growing realization that cybersecurity must receive equal attention. This holds true es-

pecially since the Nation's critical infrastructure relies extensively on computerized information systems and electronic data.

As we learned 2 weeks ago in a hearing on control systems and the electricity grid, many elements of our Nation's critical infrastructure are vulnerable to cyber attack in part because the computers are connected to the Internet. A cyber attack against a portion of our critical infrastructure could have devastating consequences that could cascade across the country.

Similarly, an attack on our control systems could cause serious physical harm, for example, through the introduction of raw sewage into drinking water systems or through the catastrophic failure of critical electrical generators.

One of the most important ways we can secure our infrastructure is through the implementation of the sector-specific plans. These 17 plans, one for each critical infrastructure sector in the U.S., are supposed to describe how each sector will identify, prioritize, and protect their physical and cyber assets. These plans are based on the high level of Federal guidance in the National Infrastructure Protection Plan, or NIPP, released by DHS in 2006. The NIPP is the roadmap for the sectors to follow when developing their sector-specific plans.

The completion of the sector-specific plans will allow DHS to write a national annual report on critical infrastructure protection which is designed to give us a general assessment of the security of our infrastructure. This firsthand report is scheduled to be released next week. Today, we will focus specifically on the cyber aspects of these plans.

I have two significant concerns about the efforts of the Department of Homeland Security in this area. First, according to the Government Accountability Office report, released today, many of the 17 plans are incomplete when it comes to cybersecurity. The GAO rated these 17 sector-specific plans according to three categories—either fully addressed, partially addressed, or not addressed at all—and found that none of the plans fully addressed all 30 cybersecurity criteria. GAO reports many plans have no way of identifying the consequences of a cyber attack or reporting metrics of progress in implementing the plans to DHS. GAO concluded that without comprehensive plans, certain sectors could be ill prepared to respond to a cyber attack.

Now, the plans are supposed to be the easier part of this process, but if we are struggling just to get the plans right, we are going to have an even tougher time achieving true security. Our main goal, of course, is actually protecting our critical infrastructure or at least making it resilient to attack; that should be the primary focus of our efforts. But as the first step, DHS must improve the current state of the cyber elements of the sector-specific plans. What we have now is simply unacceptable.

My second concern is with the implementation of the plan. Today's sector witnesses will describe the varying degrees to which they have begun translating their plans into actual improvements. It should be noted, of course, that the sector-specific plans were officially released in May 2007, so there has not been a great deal of time for action. While sectors have started implementing their plans, much work clearly remains to be done.

Under the Department's current public-private partnership approach, I don't believe the Federal Government can adequately ensure the security of our critical infrastructure. Thus far, DHS has adopted a laissez-faire approach, it seems, towards critical infrastructure owners and operators. The sector-specific plan process is entirely voluntary and there are no regulatory requirements attached to it.

Many would argue, however, that protecting critical infrastructure is an issue of national security, a core constitutional responsibility of the Federal Government. Under this viewpoint, laissez-faire is arguably not the appropriate model.

This observation is not intended to be an argument for more regulation or a criticism of our private sector partners. In a perfect world, we either wouldn't have to worry about security or would have an unlimited amount of money to spend on it, but this is clearly not a perfect world.

The Federal Government and the American people want to ensure that there is a high level of cybersecurity protections on our critical infrastructure. But, as Dr. Gordon notes in his testimony, private sector owners and operators have a hard time making the business case for increased cybersecurity investments.

Recognizing there may, in fact, be a market failure when it comes to private sector cybersecurity, I have asked the second panel of witnesses to discuss ways to incentivize owners and operators of critical infrastructure to better protect their systems. Some believe that with the proper incentives, the private sector can respond faster and more efficiently to future threats. Clearly, without appropriate consideration of all available public policy tools, the private sector's participation in critical infrastructure efforts may not reach its full potential, but I do think we need to look at a broad range of options in this area.

I have great apprehension, though, about the current framework DHS is creating with the sector-specific plans as they relate to cybersecurity. But I am hopeful that today's discussion will be a valuable tool in trying to strike the right balance that will ensure a high level of security with a low level of government involvement.

Mr. LANGEVIN. That concludes my opening statement, and the Chair now recognizes the ranking member of the subcommittee, the gentleman from Texas, Mr. McCaul, for an opening statement.

PREPARED STATEMENT OF THE HONORABLE JAMES R. LANGEVIN, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE

Good afternoon. Over the past few months, the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology has held numerous hearings to assess how far reaching our cybersecurity vulnerabilities are and how best to address them. Today we will be focusing on the extent to which cybersecurity has been implemented as part of our 17 different Sector Specific Plans. We are joined today by the Transportation Security and Infrastructure Protection Subcommittee, led by Chairwoman Jackson-Lee and Ranking Member Lungren. Though this is our first joint hearing on the subject, I very much look forward to working with the Chairwoman and Ranking Member on these issues as the 110th Congress continues.

Although critical infrastructure protection is usually associated with physical protection of facilities, there is a growing realization that cybersecurity must receive equal attention. This holds true especially since the nation's critical infrastructure relies extensively on computerized information systems and electronic data. As we learned two weeks ago in a hearing on control systems and the electricity grid, many elements of our nation's critical infrastructure are vulnerable to cyber attack

VerDate Nov 24 2008 08:44 Dec 16, 2009 Jkt 000000 PO 00000 Frm 00009 Fmt 6633 Sfmt 6621 H:\DOCS\110-HRGS\110-82\48977.TXT HSEC PsN: DIANE

in part because their computers are connected to the Internet. A cyber attack against a portion of our critical infrastructure could have devastating consequences that cascade across the country. Similarly, an attack on our control systems could cause serious physical harm, for example through the introduction of raw sewage into drinking water systems or through the catastrophic failure of critical electrical generators.

One of the most important ways we can secure our infrastructure is through the implementation of the Sector Specific Plans. These 17 plans——one for each critical infrastructure sector in the U.S.—are supposed to describe how each sector will identify, prioritize, and protect their physical and cyber assets. These Plans are based on the high level Federal guidance in the National Infrastructure Protection Plan—or NIPP—released by DHS in 2006. The NIPP is the road map for the sectors to follow when developing their Sector Specific Plans. The completion of the Sector Specific Plans will allow DHS to write a National Annual Report on Critical Infrastructure Protection, which is designed to give us a general assessment of the security of our infrastructure. The first annual report is scheduled to be released next week.

Today we will focus specifically on the cyber aspects of these plans. I have two significant concerns about the efforts of the Department of Homeland Security. First, according to the Government Accountability Office report released today, many of the 17 plans are *incomplete* when it comes to cybersecurity. The GAO rated the 17 Sector Specific Plans according to three categories: fully addressed, partially addressed, or not addressed, and found that none of the plans fully addressed all 30 cybersecurity criteria GAO reports that many plans have no way of identifying the consequences of a cyber attack or reporting metrics of progress in implementing the plans to DHS. GAO concluded that without comprehensive plans, certain sectors could be ill prepared to properly respond to a cyber attack.

Now, the plans are supposed to be the easier part of this process. But if we're struggling just to get the plans right, we're going to have an even tougher time achieving true security. Our main goal, of course, it actually protecting our critical infrastructure, or at least making it resilient to attack. That should be the primary focus of our efforts, but, as a first step, DHS must improve the current state of the cyber elements of the sector specific plans. what we have now is simply unacceptable. My second concern is with the implementation of the plans. Today's sector witnesses will describe the varying degrees to which they have begun translating their plans into actual improvements. It should be noted that the sector plans were officially released in May 2007, so there has not been great deal of time for action. While many sectors have started implementing their plans, much work remains to be done. Under the Department's current public/private partnership approach, I do not believe the Federal government can adequately ensure the security of our critical infrastructure.

Thus far, DHS has adopted a laissez-faire approach toward critical infrastructure owners and operators. The Sector specific Plan process is entirely voluntary, and there are no regulatory requirements attached to it. Many would argue, however, that protecting critical infrastructure is an issue of national security, a core constitutional responsibility of the Federal government. Under this viewpoint, laissez-faire is arguably not the appropriate model. This observation is not intended to be an argument for more regulation or a criticism of our private sector partners. In a perfect world, we either wouldn't have to worry about security or would have an unlimited amount of money to spend on it. But this is clearly not a perfect world.

The Federal government and the American people want to ensure there is a high level of cybersecurity protections on our critical infrastructure, but, as Dr. Gordon notes in this testimony, private sector owners and operators have a hard time "making the business case" for increased cybersecurity investments. Recognizing that there may in fact be a market failure when it comes to private sector cybersecurity, I've asked the second panel witnesses to discuss ways to incentivize owners and operators of critical infrastructure to better protect their systems. Some believe that with the proper incentives, the private sector can respond faster and more efficiently to future threats. Clearly, without appropriate consideration of all available public policy tools, the private sector's participation in critical infrastructure protection efforts may not reach its full potential.

I have great apprehension about the current framework DHS is creating with the sector specific plans as they relate to cybersecurity. But I am hopeful that today's discussion will be a valuable tool in trying to strike the right balance that will ensure a high level of security with a low level of government involvement.

Mr. MCCAUL. I thank the chairman, and Chairwoman Jackson Lee and Ranking Member Lungren.

Let me first say how honored I was yesterday to announce with you the creation of a commission to study this issue of cybersecurity, which has the top and brightest minds in the country on cybersecurity participating. It will be chaired by Admiral Inman, who is a former Director of NSA, Deputy Director of CIA, a good friend of mine, one of the brightest individuals I think I have ever met; and Scott Charney, who I had the opportunity to work with at the Department of Justice, who headed up the Computer Crime and Intellectual Property section.

I look forward to working with you in a bipartisan way. It is actually a nonpartisan commission that will provide recommendations for the next administration and the Congress on this very important issue.

This hearing today will bring attention to the importance of protecting the Nation's critical information technology infrastructure. In response to the President's seventh Homeland Security Directive, the Department of Homeland Security has developed the National Infrastructure Protection Plan. It is designed to provide a coordinated approach to establish national priorities, goals, and requirements for all 17 sectors of our economy that own and operate critical infrastructures across the country.

Since every sector depends to a certain extent on IT systems and networks, it is very important that each sector's plan includes its approach to securing its information infrastructure. The sector-specific plans have undergone what some might call a tortuous evolution. Even so, it is important to realize that these plans are one piece of developing a common framework across the 17 diverse sectors.

What this subcommittee has discovered in its hearings is that each of the 17 sectors is dependent upon information infrastructure in one way or another. Some are more dependent upon it than others, but each sector could be vulnerable to cyber threats and cyber attacks if appropriate steps are ignored. For example, a hacker could infiltrate the billing system of a hospital or retail store or affect credit numbers or health information for a vast number of individuals. This would inject the financial and/or health care system with uncertainty.

Similarly, we learned earlier this month that industrial control systems could cause very real physical damage if not properly secured.

We need to make sure that all the sectors are aware of their inherent interdependencies, and also that all sectors have critical information infrastructure, even if they don't think they do, that needs to be evaluated and appropriately secured. The sector-specific plans are the first step in securing this country's critical infrastructure.

Again, Chairman Langevin and I—I was pleased to announce yesterday that we are participating in a commission to develop recommendations on cyber and information security policy for the next President. It is important to evaluate the actions of the current administration, build upon its successes, and incorporate its lessons

learned as we move forward to improve our Nation's overall cybersecurity.

With that, Mr. Chairman, I yield back.

Mr. LANGEVIN. I thank the gentleman.

And the Chair now recognizes the chairwoman of the Subcommittee on Transportation Security and Infrastructure Protection, the gentlelady from Texas, Ms. Sheila Jackson Lee, for an opening statement. And let me just again, as I mentioned in private to the chairwoman, say how grateful I am that we are doing this joint hearing and how much I certainly look forward to working with you, Madam Chair, as we go forward.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. And let me offer my equal appreciation of the opportunity to continue a topic that my committee, Transportation Security and Infrastructure Protection, along with the ranking member of that subcommittee, has continued to have a keen eye.

And as I do so, might I just acknowledge the existence of the National Infrastructure Protection Plan. In meeting with a number of those from the private sector, we know that the work that we are doing today, the work that you have done, is extremely important and is an urgent topic of the private sector's participation in protecting our country's critical infrastructure.

So, again, I am grateful to Chairman Langevin for inviting the Subcommittee on Transportation Security and Infrastructure Protection to participate in this hearing; and I look forward to our future collaboration where our issues of concern interact.

Today's hearing regards the implementation or existence of the cybersecurity elements of the 17 sector-specific plans, SSPs, under the National Infrastructure Protection Plan. Ranking Member Lungren and myself take particular interest in this topic as DHS protection falls under our subcommittee's jurisdiction. We have been and continue to be very vigilant about the Department's protection of our Nation's critical infrastructure, beyond cybersecurity to also address physical and human considerations. Thanks again to Chairman Langevin, however, we will learn today about how the Department is protecting critical infrastructure from a cybersecurity perspective, and I look forward to seeing how the lessons learned today apply to other critical infrastructure protection programs. Thus far, I have been disappointed with DHS SSP efforts, but I look forward to learning more today and continuing the journey so that we can work together public and private sector.

SSP is a massive and unprecedented undertaking. According to the Homeland Security Act of 2002, critical infrastructure includes systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. Based upon this definition, critical infrastructure is not just bridges and water utilities, but also financial centers and transactions. It is therefore clear that when such a vast and important mission is combined with a young agency, it is incumbent upon it and its oversight committee to have frank and honest discussions about the efficacy of our SSP efforts.

Protecting our systems and assets from natural and human-made disasters is exclamated by the fact that approximately 85 percent of the country's critical infrastructure is owned and operated by the private sector. Furthermore, this administration did not encourage the government to regulate the private sector owners and operators, and for them, instead—to protect their critical infrastructure, but instead it encouraged voluntary partnerships.

I raised the question earlier this morning about whether or not there needs to be regulation or should we continue in the voluntary effort. How well the Department manages this voluntary relationship with the private sector to protect our critical infrastructure is and will continue to be a major priority for our committee and my subcommittee specifically.

Recently, Chairman Thompson and I directed committee staff to investigate the implementation of the NIPP and SSPs to learn whether they are motivating private industry to protect our critical infrastructure. Because such a large task is based upon a voluntary partnership, we need to give great attention to whether actions are indeed being taken. That will be the focus of my attention at today's hearings.

And might I also say that I believe there is a great interest in the private sector to be engaged. They know that they have a large share of the private infrastructure or the infrastructure of this Nation. Then, what is the vehicle, what is the formula, what is the structure that should be utilized to engage the private sector and to make this work?

After all, we are responsible for securing America collectively, and this committee, the full committee, knows full well the question will be asked, maybe only of this committee, if the possibility occurs of a terrorist act in this Nation.

The release of the NIPP and SSPs was delayed significantly. Unfortunately, the threat to our critical infrastructure was not simultaneously delayed. As a result, we have to quickly determine whether these plans are being implemented by owners and operators to better protect our critical infrastructure.

It is not enough to create large, nearly unreadable documents and to discuss processes. Instead, we must focus on implementation and execution. For instance, we must have effective and efficient communication between private sector owners and operators of critical infrastructure at all levels of government.

On September 26, Chairman Thompson and I sent a letter to Assistant Secretary Stephan and Director Caboli about the implementation of the SSPs and the standards of the national annual report that is supposed to describe the implementation of protection efforts. Based upon the Department's responses, we are quite concerned about whether verifiable action is being taken by the private sector.

I am not here to reprimand the private sector or to officially call for its regulation; but as I indicated, can we collaborate and can we work together? Because of the mission, however, I believe that all options should be on the table, and I believe that we need to give these partnerships a chance. We need to know whether the Department is executing them effectively; and what can we do to help make them work better?

I believe the owners and operators of these assets will in most cases act without regulation if an effective case for action is made and there is adequate and necessary follow-through by the Department, oversight, and the opportunity to share how we can do better.

I want to learn from our witnesses, from the private sector how the Department can be more effective in encouraging this necessary and urgent activity.

It is now time for an open and honest conversation about protecting our critical infrastructure. We are done with documents and verbiage; it is time for action. It is time for us to learn about the tools that you need and how this Congress can be helpful.

We may not need a regulatory hammer, but we certainly need a national discussion about civic and corporate responsibility and cooperation.

I believe, Chairman Langevin, that today's hearing is the beginning of establishing that cooperation and dialogue on behalf of the American people. I thank you.

Mr. LANGEVIN. I thank the gentlelady for her comments, and particularly the sentiment of our cooperation, I know that will continue, and I look forward to that.

[The statement of Ms. Jackson Lee follows:]

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, CHAIRWOMAN, SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

I would like to take this opportunity to thank all of you for joining us this afternoon to discuss the urgent topic of private sector participation in protecting our country's critical infrastructure. I am particularly grateful to Chairman Langevin for inviting the Subcommittee on Transportation Security and Infrastructure Protection to participate in this hearing, and I look forward to future collaboration where our issues of concern intersect.

Today's hearing regards the implementation—or existence—of the cyber security elements of the 17 Sector Specific Plans (SSPs) under the National Infrastructure Protection Plan (NIPP). Ranking Member Lungren and I take particular interest in this topic as DHS' infrastructure protection efforts fall under our subcommittee's jurisdiction. We have been—and continue to be—very vigilant about the Department's protection of our nation's critical infrastructure beyond cyber security, to also address physical and human considerations.

Thanks to Chairman Langevin, however, we will learn today about how the Department is protecting critical infrastructure from a cybersecurity perspective, and I look forward to seeing how the lessons learned today apply to other critical infrastructure protection (CIP) programs. Thus far, I have not been very impressed with DHS' CIP efforts.

CIP is a massive and unprecedented undertaking. According to the Homeland Security Act of 2002, "critical infrastructure" includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, nation public health or safety any combination of these matters," Based upon this definition, "critical infrastructure" is not just bridges and water utilities, but also financial centers and transactions. It is, therefore, clear that when such a vast and important mission is combined with a young agency, it is incumbent upon it and its oversight committee to have frank and honest discussions about the efficacy of our CIP efforts.

Protecting theses systems and assets from natural—and human-made disasters is exacerbated by the fact that approximately 85 percent of the country's critical infrastructure is owned and operated by the private sector. Furthermore, this Administration did not encourage the government to regulate and mandate private sector owners and operators protect their critical infrastructure but, instead, it encouraged voluntary partnerships. How well the Department manages this voluntary relationship with the private sector to protect our critical infrastructure is—and will continue to be—a major priority for our Committee, and my subcommittee specifically.

Recently, Chairman Thompson and I directed Committee staff to investigate the implementation of the NIPP and SSPs to learn whether they are motivating private industry to protect our critical infrastructure. Because such a large task is based upon a voluntary partnership, we need to give great attention to whether actions are, indeed, being taken. That will be the focus of my attention at today"s hearing.

The release of the NIPP and the SSPs was delayed significantly. Unfortunately, the threat to our critical infrastructure was not simultaneously delayed. As a result, we have to quickly determine whether these plans are being implemented by owners and operators to better protect our critical infrastructure. It is not enough to create large, nearly unreadable documents and to discuss processes; instead, we must focus on implementation and execution. For instance, we must have effective and efficient communication between private sector owners and operators of critical infrastructure and all levels of government.

On September 26, 2007, Chairman Thompson and I sent a letter to Assistant Secretary Stephan and Director Caverly about the implementation of the SSPs and the status of the National Annual Report that is supposed to describe the implementation of protection efforts. Based upon the Department's responses, we are quite concerned about whether verifiable action is being taken by the private sector.

I am not here to reprimand the private sector or to viscerally call for its regulation. Because of the mission, however, I believe that all options should be on the table. I believe that we need to give these partnerships a chance. We need to know whether the Department is executing them effectively. I believe the owners and operators of these assets will, in most cases, act without regulation if an effective case for action is made and there is adequate and necessary follow through by the Department. I want to learn from our witnesses from the private sector how the Department can be more effective in encouraging this necessary—and urgent—activity.

It is now time for an open and honest conversation about protecting our critical infrastructure. We are done with documents and verbiage. It is time for action. It is time for us to learn about the tools you need and how this Congress can help. We may not need a regulatory hammer, but we certainly need a national discussion about civic and corporate responsibility. Perhaps today's hearing begins that conversation and will lead to concrete steps that will make america truly safer.

Mr. LANGEVIN. The Chair now recognizes the ranking member of the subcommittee, the gentleman from California, Mr. Lungren, for the purpose of an opening statement. And, likewise, I look forward to working with the gentleman from California.

Mr. LUNGREN. Thank you very much, Mr. Chairman. And I thank the gentlelady and I thank the gentleman from Texas, Mr. McCaul.

First of all, let me say that I believe that the Department of Homeland Security did a good job in putting together the sector-specific plans and coming up with the National Infrastructure Protection Plan under the direction of Colonel Stephan. I know, when he first came in, he was dissatisfied with what was then in the works, and asked us for extra time to make sure that we could put a good product together. And I think the Department has; I congratulate you on that. Frankly, it is a good piece of work.

I am, as my colleagues are, dismayed by the recent GAO review which did find that most of the sectors lacked a process for identifying the consequences of cyber attacks against their assets. That is probably not surprising, because most Americans and most in Congress look at guns, gates, and guards as the traditional means of protecting our critical infrastructure; and it is only after stepping back a ways that we realize the importance of the cyber world in all of this.

It is my feeling that a public-private partnership is absolutely essential, not just because 85, 86, 87, whatever percentage you want to say of our critical infrastructure is privately owned and operated; but the agility with which the private sector is able to adapt in the area of technology is at least the equal of those of us in gov-

ernment. We would do ourselves a disservice if we in any way followed procedures on the bureaucratic side or the regulatory side which denied us that agility, that creativity, and that ingenuity in responding to what are threats that change, not yearly, not monthly, not weekly, not daily, but, frankly, minute by minute.

So I am very interested in the testimony we will receive today from both the public and the private sectors. But I hope that we will find a way to reach that balance that is necessary between government regulation and private ingenuity and effectiveness.

Thank you very much, Mr. Chairman.

Mr. LANGEVIN. I thank the gentleman for his opening statement.

Mr. LANGEVIN. Other members of the subcommittee are reminded that under the committee rules, opening statements may be submitted for the record.

I now welcome our first panel of witnesses. I want to begin by thanking the panel for their patience and willingness to stick around. We wish we had a little more control over the schedule around this place, but it doesn't seem to work out that way.

But I do want to begin by welcoming our first witness, Mr. Greg Garcia, Assistant Secretary for Cybersecurity and Communications. Assistant Secretary Garcia oversees the Department of Homeland Security's mission to prepare for and respond to incidents that could degrade or overwhelm the operation of the Nation's information technology and communications infrastructure.

So I welcome you, Mr. Secretary.

Our second witness, Dave Powner, is the Director of Information Technology Management Issues at the Government Accountability Office.

Thank you for your participation, and we welcome you here today, Mr. Powner.

Our third witness is Mr. J. Michael Hickey, the Chairman of the Communications Sector Coordinating Council. Mr. Hickey is also the Vice President of Government Affairs and National Security Policy at Verizon.

Welcome, Mr. Hickey.

Our fourth witness is Mr. George Hender, the Chairman of the Banking and Financial Sector Coordinating Council. Mr. Hender is the Vice Chairman of the Options Clearing Corporation.

Welcome to you, Mr. Hender.

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

Mr. LANGEVIN. And I now ask each witness to summarize his statement for 5 minutes, beginning with Assistant Secretary Garcia.

The floor is yours.

**STATEMENT OF GREG GARCIA, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND TELECOMMUNICATION, U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. GARCIA. Thank you, sir.

Mr. Chairman, Madam Chairwoman, members of the subcommittees, thank you very much for inviting me again to speak about the Department of Homeland Security's effort to strengthen the security and resilience of our Nation's critical infrastructure.

My comments today will focus on three areas: first, how my office has worked with each of the 17 critical infrastructure and key resource sectors to ensure cybersecurity is integrated into their sector-specific plans, or SSPs;

Second, I will report on the findings from our cybersecurity review of each SSP; and

Third, our plan for continuing to increase attention that each sector gives to cybersecurity.

Under the National Infrastructure Protection Plan, or NIPP, my office, the Office of the Cybersecurity and Communications, works to reduce cyber risk and enhance cybersecurity in two ways. We serve as the Federal lead for the IT and communications sector infrastructure protection efforts, and as the lead for addressing the cross-sector cyber element for all sectors.

Throughout the development of the SSPs, my office provided cybersecurity guidance and support to the sectors. This included providing sector-specific agencies with resources for identifying cybersecurity practices and protective programs, helping them identify cyber R&D priorities, and developing a comprehensive cyber guidance checklist which gave each sector a framework for integrating cybersecurity into their SSPs.

In addition, sectors asked us to review drafts of their SSPs, and we provided recommendations on ways to address cybersecurity. My office also conducted a review of the cyber elements in each plan to determine sector-specific efforts and identify cross-sector trends. Our review was generally consistent with the findings of the GAO's analysis.

In particular, I am pleased that the GAO found that 12 out of the 17 sectors were comprehensive in addressing cybersecurity and their SSPs. This is clear evidence of all the hard work that has been done to date. Since the development of the SSPs, sectors have been implementing their plans and enhancing efforts to address the security of their cyber infrastructure.

Our review of the 2007 sector annual reports revealed an increased integration of cybersecurity considerations across the sectors. For example, more than half of the sectors identified at least one cybersecurity goal and/or priority. This is a significant improvement from the 2006 sector annual reports, and it is a strong indication of increased understanding about the importance of cybersecurity.

Additionally, sectors are incorporating DHS-sponsored cybersecurity measures, such as our cybersecurity vulnerability assessment tool, into their risk assessment efforts.

I would add, no discussion of cybersecurity and infrastructure protection efforts would be complete without mentioning the cross-sector cybersecurity working group. This group is composed of experts from each sector and serves to enhance cross-sector understanding of mutual dependencies and interdependencies. It is currently focused on addressing common cybersecurity challenges identified in each sector's initial SSP and developing improvements that can be leveraged across the sectors.

Overall, while we are seeing greater attention given to cybersecurity, there is still more work to do. Each sector must consider their own cybersecurity posture and balance against other sector-specific

risk management efforts. Specifically, sectors should continue to focus on identifying their critical cyber infrastructure, assessing their cyber risk, implementing protective programs, and measuring the effectiveness of their efforts.

My office is currently engaging with sectors that may not have fully captured the good cybersecurity work they are already doing in their initial SSPs. We will work with them to more fully document their efforts as they update their SSPs and develop their 2008 sector annual reports.

We will also continue to work with individual sectors to implement the cyber aspects of their SSPs in order to measurably enhance security within their sectors. We will conduct workshops with sectors to identify incentives, cyber metrics, and current and future cyber R&D requirements.

The development of the SSPs represented a significant milestone for public and private sector national protection and preparedness activities. My office is committed to promoting cybersecurity strategies that can address the evolving risks we face. We are thankful for the work that has been done to date, and we encourage all sectors to continue working with us to address cybersecurity and their infrastructure protection activities.

Thank you all for your time today, and I am happy to address any questions that you may have.

Mr. LANGEVIN. Thank you, Secretary Garcia, for your testimony.

[The statement of Mr. Garcia follows:]

PREPARED STATEMENT OF GREGORY GARCIA

Good afternoon, Chairman Langevin, Chairwoman Jackson–Lee, Ranking Member McCaul, Ranking Member Lungren, and Members of the Subcommittees. Thank you for inviting me to speak about our efforts to work with all 17 critical infrastructure and key resource (CI/KR) sectors to address the security of the cyber elements of their infrastructures, including the incorporation of cyber security into their Sector–Specific Plans (SSP), progress in advancing mitigation actions, and plans for continuing to engage with the CI/KR sectors to further address cyber security.

One of the most pressing challenges facing the Department of Homeland Security (DHS) is preparing for cyber attacks against our CI/KR. Threats to the Nation's CI/KR are numerous and constantly evolving. The ability of threat actors to exploit vulnerabilities is facilitated by the widespread availability of tools, techniques, and information. A variety of cyber threats could exploit vulnerabilities in the Nation's CI/KR assets, systems, networks, and functions, potentially threatening national and economic security, public health and safety, and confidence in the government. The President's *National Strategy to Secure Cyberspace* recognized the importance of assessing threats and vulnerabilities and determining how likely or significant those attacks could be on critical infrastructure. It called for public-private partnerships to address five critical priorities: (1) a national cyberspace security response system, (2) a national cyberspace security threat and vulnerability reduction program, (3) a national cyberspace security awareness and training program, (4) securing governments' cyberspace, and (5) national security and international cyberspace security cooperation. The first three priorities speak directly to the development and implementation of the SSPs.

In implementing the *National Strategy* DHS' Office of Cybersecurity and Communications (CS&C), working in partnership with the Office of Infrastructure Protection (OIP), Sector-Specific Agencies (SSAs), and public- and private-sector security partners, is committed to preventing, preparing for, responding to, and recovering from cyber attacks and their consequences. CS&C's strategic goals include preparing for and deterring catastrophic incidents by achieving a collaborative risk management and deterrence capability with a mature partnership between government and the private sector. One example of this partnership is CS&C's National Coordinating Center (NCC). Since 1984, the NCC has served as a forum through which the Federal government and private sector communications providers can interact face-to-face on a daily basis. This strategic goal also encompasses tactical efforts to

secure and protect the Nation's cyber infrastructure from attacks and disasters by identifying and mitigating threats, vulnerabilities, and consequences.

Our vision, philosophy, and strategy for preventing, responding to, and recovering from cyber attacks reflect the expanding and widespread importance of the cyber infrastructure. Policies that advance a safe and secure infrastructure rely on the valuable relationships between the public and private sectors and on public trust and confidence.

The key to continued success is partnering strategically with the private sector to identify, prioritize and protect critical cyber assets, systems, networks and functions. Even though the private sector builds, owns and operates most of the cyber infrastructure, CS&C takes an active role in its protection by building public-private partnerships that are vital to our strategy to secure cyberspace and to facilitating efforts to raise cyber security awareness, train personnel, stimulate market forces to secure cyberspace, improve technology through the identification of cyber research and development requirements, identify and remediate vulnerabilities, and exchange information.

CS&C works to reduce cyber risk and enhance cyber security in two primary ways under the National Infrastructure Protection Plan (NIPP) framework: (1) as Federal lead for the Information Technology (IT) Sector's infrastructure protection and preparedness responsibilities (in partnership with the Communications Sector); and (2) as a cross-sector cyber element that involves DHS, the SSAs for each of the 17 CI/KR sectors, and public and private sector owners and operators.

Homeland Security Presidential Directive 7 designates DHS as the SSA for both the Communications and IT sectors. CS&C's National Communications System (NCS) and the National Cyber Security Division (NCSD) carry out the SSA responsibility for the Communications and IT Sectors, respectively. Both sectors recently released their Sector Specific Plans (SSPs), which are planning documents that focus on overall sector preparedness, including managing risk to the sectors' critical functions and infrastructures that support homeland, economic, and national security. Under the NIPP framework, the Internet and its associated services are identified as a shared key resource of the IT and Communications Sectors, reflecting the convergence of voice and data communications networks and services. In their respective DHS-designated roles for the Communications and IT infrastructure sectors, the NCS and NCSD share responsibility with public—and private-sector security partners for the availability of the Internet and its associated services. Recognizing the synergies between IT and Communications, the chair of each sector's Government and Sector Coordinating Councils also participates in the other sector's council. In addition, representatives from the IT and communications sectors participate in each other's risk assessment methodology development efforts.

**Cyber Security in the Sector–Specific Plans**

In support of the cross-sector cyber responsibility, NCSD is working closely with OIP, the SSAs, and other security partners to integrate cyber security into the CI/KR sectors' protection and preparedness efforts.

During the SSP development process, NCSD provided cyber expertise to the sectors, including reviews of draft SSPs and participation in sector-specific cyber security meetings. Specifically, as sectors were developing their SSPs, NCSD developed and provided information to SSAs on resources for cyber security practices and protective programs that are applicable across all sectors, as well as some that are more focused on individual sectors, to help inform the identification of cyber security-related protective programs. For each protective program, a brief description and the specific activities they supported within the preparedness spectrum were provided. NCSD also developed information on cyber research and development (R&D) requirements and priorities to help SSAs in the identification of cyber-related R&D priorities. A description of Federal organizations that support cyber R&D and several references to R&D documents that outlined specific cyber security initiatives were provided. NCSD also offered to work directly with any sector that requested assistance and worked with responding sectors to develop and review cyber security content for the SSPs.

NCSD also developed a comprehensive SSP Cyber Guidance Checklist, which provided sectors with a framework for integrating cyber security throughout each section of their SSPs. The checklist complemented DHS' 2006 CI/KR Protection SSP Guidance developed by OIP and was intended to provide a starting point for SSAs as they integrated cyber into their SSPs. The checklist included an outline and guidance for the development of cyber content for the SSPs. NCSD shared the checklist in OIP-sponsored technical assistance sessions with SSAs to provide expertise and answer questions regarding the inclusion of cyber security in the SSPs. NCSD personnel also met individually with those SSA representatives who expressed an inter-

est in determining approaches for incorporating cyber security into their SSPs and sector risk management efforts.

In December 2006 and January 2007, NCSD conducted a review of the final draft SSPs as part of OIP's review process to (1) assess each sector's plan for securing its cyber infrastructure and (2) understand the coordination between NCSD and the sectors needed to better secure the sector's cyber infrastructure. In addition to considering the full content of the SSPs, this review focused on specific areas where future coordination between NCSD and the sectors might be necessary to address the security of the cyber elements of the Nation's CI/KR, including the critical initial action to identify the sectors' cyber security partners that NCSD should engage with to manage cyber risk. NCSD also determined that coordination may be required in understanding how each sector plans to identify and assess risk to its cyber infrastructure. Coordination is also required when assisting sectors in the development or refinement of methodologies intended to identify critical cyber elements and to assess cyber risk. Finally, the review identified protective programs specific to cyber security that fall within NCSD's responsibility and cyber R&D priorities requiring coordination across the sectors and with DHS' Science and Technology Directorate.

After the SSPs were finalized, NCSD conducted a second review of the documents on behalf of the Cross-Sector Cyber Security Working Group (CSCSWG). The CSCSWG provides a forum for exchanging information on common cyber security challenges and issues (i.e., threats, vulnerabilities, and consequences) and enhancing the understanding across sectors of mutual dependencies and interdependencies. The working group includes cyber security experts from the CI/KR sectors collaborating to identify systemic cyber risks and mitigation strategies for the Nation's CI/KR sectors. The CSCSWG held its inaugural meeting on May 30, 2007, and determined that an initial area of focus would be reviewing the cyber security components of the SSPs to better understand the various efforts to protect cyber elements of the 17 CI/KR sectors and identify trends in cyber infrastructure protection that cut across the sectors. Using the NCSD review as a starting point, the group provided input on sectors' cyber content and on cyber activities not fully captured or initiated after the drafting process. The group has begun to share successes, best practices, and lessons learned to help the development and implementation of more effective cyber risk management activities across the sectors. For example, through the CSCSWG, members learned about the Roadmap to Secure Control Systems in the Energy Sector. As a result, the Water and Chemical Sectors have chosen to initiate similar efforts to address the unique concerns of control systems security within their sectors.

**Progress in Advancing Mitigation Actions**

Many of the SSPs were created in summer and fall of 2006. Sectors have been implementing the plans, continuing or initiating efforts to address the security of their cyber infrastructure. Sectors are not uniformly comprehensive in their cyber security efforts and should not necessarily be. Each sector must consider its cyber security posture and balance that against other risk management efforts, in consideration of the unique aspects of its infrastructure. Cyber risk varies by sector, based on its dependence on cyber elements. For example, the extensive use of control systems in the Energy Sector and of business systems in the Financial Services Sector must factor into the extent, sophistication, and unique implementation of mitigation and protection strategies within those sectors. Other sectors do not have cyber infrastructure integrated as ubiquitously in their essential services, a fact that influences the focus and maturity of their cyber security efforts. The length of time a sector's public and private partners have been working together on infrastructure protection issues is another factor in the comprehensiveness of their plans. These observations regarding the cyber security position of the SSPs are generally consistent with the findings of the Government Accountability Office's (GAO) analysis.

The integration and maturing nature of cyber security across the 17 CI/KR sectors was clear when NCSD reviewed and contributed to the Sector Annual Reports (SARs). The sectors' 2007 SARs were much improved over their initial 2006 efforts. For example, more than half of the sectors identified at least one cyber security goal and/or priority in their second SAR. This represents a significant increase in the number of sectors from the 2006 SAR, suggesting that the understanding of the importance of cyber security is becoming more pervasive in the sectors.

Further, more sectors are implementing DHS-sponsored protective measures, such as the Comprehensive Review, the Risk Analysis and Management for Critical Asset Protection (RAMCAP), and the Site Assistance Visit programs. NCSD collaborates with OIP to incorporate cyber security into these DHS risk and vulnerability assessment programs so that sectors implementing them would address the cyber elements of their infrastructure. We encourage sectors to assess cyber risk by using

the Cyber Security Vulnerability Assessment (CSVA), a flexible and scalable approach that analyzes an entity's cyber security posture and describes gaps and targeted considerations that can reduce overall cyber risks. It assesses the policies, plans, and procedures in place to reduce cyber vulnerability in 10 categories (e.g., access control, configuration management, physical security of cyber assets, etc.) and leverages various recognized standards, guidance, and methodologies (e.g., International Organization for Standardization 27001, Information Systems Audit and Control Association Control Objects for Information and related Technology, and the National Institute of Standards and Technology Special Publication 800 series). The CSVA tool is being used by six sectors in their tailored vulnerability assessments: five through their sector specific RAMCAP modules and another, the Transportation Sector, in its customized cyber security assessment.

**Plans for Continuing to Engage with the CI/KR Sectors to Further Address Cyber Security**

Our review of the SSPs and SARs found that sectors are paying attention to cyber security, but more needs to be done. Over the next year, sectors need to focus on identifying their critical cyber infrastructure, assessing cyber risk and promoting voluntary assessments, implementing protective programs, and measuring the effectiveness of their efforts.

NCSD has created an action plan and is engaging with sectors in addressing cyber security issues not fully addressed in those sectors' initial SSPs. This action plan includes working with sectors to review cyber security priorities, assess effects of cyber attacks, develop protective programs, and evaluate R&D requirements and initiatives to identify areas where additional capabilities are needed. NCSD has already worked with the cyber experts of the Chemical Sector Coordinating Council (SCC) and the SSA to identify cyber security content needed for the 2008 update to their SSP. Some of the opportunities for engagement are based on sector specific needs, but others address more common challenges. The action plan will address both individual and more universal steps.

While all sectors have established SCCs and Government Coordinating Councils (GCCs), the degree of examination of specific cyber risk and of cyber information sharing varies. Some sectors—such as Financial Services—consider cyber security as critical to their core business functions and integrate cyber security into all of their SSP implementation activities. In fact, the Financial Services SSA, the Department of the Treasury, sits on the IT GCC because of its interest and expertise in cyber security. Other sectors have historically had less focus on cyber security due to the lack of prominence of IT in the business of the sector. Representation from the sectors' SCCs and GCCs are participating in the CSCSWG provides a mechanism for two-way information flow on cyber concerns across all sectors. Participation in the CSCSWG may help less-mature sectors make more rapid progress in identifying cyber goals, gaps, and interdependencies, as well as developing programs to deter, respond and recover from cyber attacks by enabling them to leverage the experiences, work, and cyber functional expertise that exists in many sectors.

In addition, the reliance of some sectors on control systems highlights an area for increased coordination of risk management efforts. NCSD's Control Systems Security Program (CSSP) and the Process Control Systems Forum (PCSF) are resources to help address control systems risk. The CSSP coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors, to improve control system security within and across all critical infrastructure sectors. In support of risk mitigation efforts, the CSSP developed the Control Systems Cyber Security Self Assessment Tool and provides training in control systems cyber security. The PCSF, a standing group under the CSCSWG, works to develop solutions for process control systems security, aggregate information, connect decision makers, and leverage other groups' work.

Sectors may leverage the United States Computer Emergency Readiness Team (US–CERT) to share information on cyber threats and vulnerabilities and enhance situational awareness. The timely detection and analysis of cyber attacks further helps to assess operational risk and mitigate the impact on our Nation's critical infrastructures of cyber vulnerabilities. US–CERT is working with the Information Sharing and Analysis Center Council to expand this operational interaction.

Finally, most sectors are taking on the challenge of identifying or developing metrics to measure the effectiveness of all infrastructure protection efforts, including those for cyber. Since sectors have different overall approaches to infrastructure identification and risk management, NCSD will work with the sectors to develop some cross-sector qualitative measures that correlate to cyber security to help measure the effectiveness of sectors' cyber security efforts.

**Conclusion**

The development of the 17 CI/KR SSPs represented a significant milestone in sectors' protection and preparedness activities. Sectors varied in how they addressed the security of the cyber elements of their infrastructures, including the incorporation of cyber security into their SSPs, but demonstrated increased understanding of the importance of cyber security in the SARs and implementation activities.

As the sectors work to address the feedback from the GAO on the cyber security aspects of the SSPs, CS&C, and specifically, NCSD will continue to execute its cross-sector cyber responsibility to work with sectors to reduce cyber risk and enhance cyber security. Our goal is to create a clear and actionable path forward with the sectors and to work together to secure our critical cyber infrastructure.

NCSD will continue to schedule regular interactions with individual sectors as well as meetings with multiple sectors. For example, we plan to meet with each SSA at least twice a year, once before the sectors update their SSPs and once in early spring of 2008 as sectors are preparing their SARs. NCSD will develop guidance on cyber elements that should be considered for inclusion in the SSPs and SARs. This guidance will complement guidance from the Office of Infrastructure Protection. NCSD will also work with sectors through their coordinating councils to identify cyber subject matter experts within their sectors and raise awareness of the sectors' reliance on cyber infrastructure. NCSD is piloting this approach by convening a small group of cyber security experts with security clearances from across the sectors to support the SSA risk assessment process for the 2008 National CI/KR Protection Annual Report.

NCSD also plans to offer workshops in 2008 with sector partners and other invited subject matter experts to address incentives to encourage voluntary risk assessments, develop cross-sector cyber metrics, and identify existing cyber research and development projects. The outcome of these workshops will provide sectors with ideas for incentives for investing in cyber security, metrics that enable realistic evaluation of cyber security, and cyber R&D priorities. NCSD will also continue to support the efforts of the CSCSWG as it addresses opportunities to enhance cyber security across the sectors and share information about strong cyber programs and practices. Further, NCSD will continue to roll out important efforts like the CSVA, software assurance, and control systems acquisition guidance, training, and cyber exercises to our sector partners.

We encourage sectors to continue to work collaboratively with NCSD on addressing cyber security in their infrastructure protection activities. Through participation in the CSCSWG, individual meetings with NCSD, and various NCSD-sponsored workshops and programs, sectors can make significant progress in the future to address or more fully address cyber security.

We must reinforce a culture of preparedness, shift from a reactive to a proactive stance, and prepare by promoting effective cyber security strategies that evolve as the risks evolve. There is much work to be done, but progress continues every day. We rely on the support and expertise of the sectors to advance this mission.

I would like to thank the Subcommittees for their time today, and I appreciate this opportunity to discuss these important cyber security priorities.

Mr. LANGEVIN. I now recognize Mr. Powner to summarize his statement for minutes.

Welcome.

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

Mr. POWNER. Chairman Langevin, Chairwoman Jackson Lee, Ranking Members McCaul and Lungren, and members of the subcommittees, we appreciate the opportunity to testify on our report being released today on cybersecurity elements of the sector plans to protect our Nation's critical infrastructures.

Chairman Langevin and Ranking Member McCaul, I would like first to thank you for your leadership and oversight of the Nation's cyber critical infrastructure.

As the focal point for SSP, DHS has many cyber-related roles and responsibilities that are called for in law and policy that we have previously testified on before this subcommittee. These are

highlighted in detail in my written statement. One of these is the development of a comprehensive national plan that requires each of the 17 sectors to develop sector-specific plans that include how each sector will identify, assess, and protect its cyber assets. Today's request is—I will discuss how well these plans address key cyber aspects of cybersecurity and GAO's observations and recommendations to move beyond the planning phase.

The extent to which the sectors address aspects of cybersecurity and their plans varied. The strongest plans were the ones from the IT and communications sectors, while the weakest included the agriculture and commercial facilities sectors. The banking and finance sectors assessment fell near the middle of these plans.

DHS has acknowledged these shortcomings and has stated that these are only early efforts by sectors to develop their respective plans. DHS attributed the variations to several items, including the maturity of the sector and the extent to which the sector worked with DHS to develop their plans. Nevertheless, until these plans fully address the key cyber elements, infrastructure sectors may not adequately identify, prioritize, and protect critical cyber assets.

Another reason why these plans are incomplete is that based on our broader work for the full committee and for the subcommittee chaired by Ms. Jackson Lee, some of the sectors claim that these plans are not that useful. In particular, some sectors believe that they have progressed beyond these plans. In these cases, then, this is just a paper exercise.

It is important to note that these are just plans. They do not identify actual assets and vulnerabilities; rather, they identify approaches the sectors will pursue. Moving forward, if in fact these plans are truly to be used to identify gaps in our Nation's cyber protection efforts on a national level, as intended, these plans need to be improved, meaning that they comprehensively address cyber elements and, even more importantly, the plans need to be effectively implemented.

From an oversight perspective, it will be important to track how these plans evolve and are implemented in the critical infrastructure protection annual report due to the Executive Office of the President each September, although we hear that this year's report will be issued in November.

Beyond its involvement with developing and implementing these plans, DHS's national Cybersecurity Division needs to continue to bolster its capabilities so that it is viewed as a valuable service provider to infrastructure owners. Today, this is not necessarily the case.

To its credit, DHS's efforts to lead cyber exercises, like Cyber Storm, provide valuable information to participants to improve response, and coordination mechanisms. However, our Nation still lacks a national threat assessment and a mature analysis and warning capability, an area that we are currently reviewing for you, Mr. Chairman. If DHS is to effectively fulfill its role as the focal point for cyber critical infrastructure protection, it must fulfill more of its responsibilities and build more capability.

Our Nation continues to progress at a slow pace in implementing this sector-based approach to protecting our Nation's critical infrastructures. We are almost 10 years into this approach, and al-

though there is some progress in areas, we are not where we need to be. Unless we start making more progress and actually protecting our critical infrastructures, we may want to consider alternative approaches such as prioritizing and protecting by asset criticality regardless of sector.

In summary, Mr. Chairman, and Madam Chair, if the sector-based approach to protecting our Nation's critical infrastructures is to be effective, we will need comprehensive plans. However, ultimately our Nation needs to move beyond the planning stages and into implementation of effective protective and recovery programs. Implementation of these plans is more likely if DHS can successfully fulfill its responsibilities and become a provider of valuable information on threats and analytical products to our Nation's critical infrastructure owners.

This concludes my statement. I will be pleased to respond to questions.

Mr. LANGEVIN. I thank you, Mr. Powner, for your testimony.

[The statement of Mr. Powner follows:][1]

M. Langevin. And the Chair now recognizes Mr. Hickey for his statement for 5 minutes.

**STATEMENT OF J. MICHAEL HICKEY, CHAIRMAN, TELECOMMUNICATIONS SECTOR COORDINATING COUNCIL**

Mr. HICKEY. Good afternoon, Chairman Langevin and Chairwoman Jackson Lee, Ranking Members McCaul and Mr. Lungren. It is a pleasure to be here representing the communications sector and to testify on behalf of the sector in terms of what we are doing day in and day out to advance not only cybersecurity, but business continuity and emergency preparedness practice within our sector.

What I would like to do in my few minutes with you is to discuss four areas of involvement. The first is focused on what companies like Verizon do day in and day out that really addresses not only cybersecurity, but broader asset protection within our companies.

I would also like to spend a few minutes talking about the collaborative activity that is under way, again day in and day out not only within our sector, but with our partners in government.

Third, I will speak briefly to the Communications Sector Coordinating Council structure and the work that we are doing on our sector-specific plan.

And I will conclude with a few observations in terms of what I think we can do, what we must do, with government, going forward.

Effective industry and government collaboration starts with the actions of individual organizations. The private sector owns and operates from 85 to 90 percent of this country's critical infrastructure. Because of industry's important role in national and homeland security, corporations like Verizon must dedicate the operations, experience, resources, and oversight necessary to be as self-aware and self-reliant as possible.

Verizon's communications, voice, data, and video networks are touched by over 100 million consumers and government and business customers daily. Because of this reach, we have a long-

[1]See *For the Record.*

standing and growing commitment to national security and emergency preparedness. For instance, we have designed, built, and managed networks that are resilient and redundant. We have adopted best-practice business methods and security procedures. We have created and tested business continuity and emergency preparedness programs. We have responded successfully to a wide range of crises and have provided leadership to industry and government organizations dedicated to national security and emergency preparedness.

From a structural standpoint internally, we have corporate policy statements that require attention to business continuity, emergency preparedness, and cybersecurity. We have a number of senior leaders within our business from a chief information officer, who is an executive vice president, to a new chief technology officer, again another executive vice president, to the announcement of a new chief security officer for Verizon Corporation who will start with us in January, who currently serves as executive assistant director of the FBI for Criminal, Cyber, and International Security.

We have groups within our IT organization that serve as service bureaus to all of our business units to make sure that cybersecurity practices are designed, engineered, and adopted business unit by business unit. We actually focus on security within our company from more of an organic standpoint.

We rely on ground-up business unit activity, identifying and dealing with issues; and beyond that, to coordinate activity across our corporation, we have executive security councils and a Verizon information security council that is responsible not only for oversight, but to make sure that best practices are implemented within our business organizations.

We have a cyber intrusion response team that provides 7-by-24 coverage for the entire enterprise, supporting all business units and organizational points of contact to assess intrusion impacts, contain and control further dissemination of problem areas across the company, and capture and preserve evidence for law enforcement and legal purposes.

So, within Verizon Corporation, as within many other corporations that I work with day in and day out, there are strong practices in place. There is a real focus day in and day out on cybersecurity and critical assets protection within our organizations.

I would like to address, just for a minute, sector collaboration. Verizon and its peer companies within the communications sector have a long history of cooperation on national security and emergency preparedness. We have a 40-year history that stems back to the aftermath of the Cuban missile crisis when the National Communications System was created to deal with issues of interoperability and sustainable communications.

Since that time, in 1984, the National Coordinating Center for Telecommunications was formed as a partner organization with the National Communications System. It was broadened. It was established when Executive Order 12472 created it, and it has focused since that time on making sure that industry and government work together closely day in and day out on a full range of asset protection measures. The focus is on facilitating information sharing among government and industry participants regarding vulner-

ability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure.

I might point to the recent Southern California fires where the NCC Watch took a real leadership role in coordinating private sector and government information, sharing real-time on what was happening within the field and how industry and government could respond together. That information developed there was shared with a joint field office when established on the West Coast.

There is a network reliability and interoperability council established by the FCC back in 1992. There have been a series of seven councils since that time. Most have focused on some aspect of security practice. Verizon and industry in general have been very active in working not only with the FCC, but with other government partners in advancing sound practice on a voluntary basis as a result of the work done within the NRIC.

There is another organization called the National Security Information Exchange. In 1990, the NCS focused on actions industry and government could pursue to protect critical telecommunications from the growing hacker threat. Ultimately, the NCS and NSTAC created national security information exchanges. These exchanges, since that time, have brought together expertise from government and subject matter experts on security practice from industry to address a full range of security practices relevant to the evolving risk environment.

Pertinent to the Communications Sector Coordinating Council, I am very proud to be its chair for this year, and it points out the complexities, I think, of working together not just within our sector, but on a cross-sector basis; and we have focused very much on our interdependencies not just within our sector, but across sectors.

The Communications Sector Coordinating Council became operational in calendar year 2006. It was chartered to foster the coordination of policy initiatives to improve the physical and cybersecurity of sector assets and to ease the flow of information within the sector, across sectors, and with designated Federal agencies.

We now embrace 35 member companies that are broadly representative of the sector. I think that is a real benefit of the Sector Coordinating Council's having been established, because we are not just traditional wireline and wireless; we are satellite, we are undersea cable. We represent the National Broadcasters, the Association of Public Television Stations, a wide range of companies.

To summarize, the sector has been very proactive through the Sector Coordinating Council, through other mechanisms, and we have really focused on our sector-specific plan, currently on the risk assessment which we plan to have complete by the end of this calendar year in draft form and in final form by the end of the first quarter next year. Thank you.

Mr. LANGEVIN. Thank you.

[The statement of Mr. Hickey follows:]

PREPARED STATEMENT OF J. MICHAEL HICKEY

**Overview:**

Mr. Chairman and Members of the Subcommittee, my name is Mike Hickey and I thank you for the opportunity to testify before you on measures we have taken to address cybersecurity in the Communications Sector Specific Plan. I serve as Vice President of Government Affairs for National Security Policy at Verizon and as

Chair of the Communications Sector Coordinating Council. I also serve as Vice Chair of the Internet Security Alliance and am an active member of the US Chamber of Commerce Homeland Security Task Force. Of these organizations, the Communications Sector Coordinating Council is uniquely chartered to represent the breadth of the communications sector on policy issues relating to the protection of critical communications infrastructure and key assets. Since 2005, it has emerged as an instrument for business engagement with government on policy matters relating to homeland security and emergency preparedness.

My comments will address the roles that have been established for industry and government in protecting the nation's critical physical and cyber communications assets, steps taken to protect these assets, what measures have worked effectively and what needs to be done to sharpen the collective focus as we move forward.

**Tiered Approach to Critical Asset Protection:**

Effective industry and government collaboration starts with the actions of individual organizations. The private sector owns and operates nearly 90% of this country's critical infrastructure. Because of industry's important role in national and homeland security, corporations like Verizon must dedicate the operations experience, resources and oversight necessary to be as self-aware and self-reliant as possible. Verizon is obligated to its shareowners and customers to take the steps necessary to secure its cyber, physical and human assets from disruption or attack. We cooperate with peer companies in order to support communications sector mutual aid obligations. We also proactively address our interdependencies with other sectors to ensure continuity of operations in time of crisis. Finally, we continue to work with government agencies at the Federal, State, regional and local levels to support appropriate security and emergency preparedness initiatives.

**Strength from Within:**

Verizon Communications Inc. is a Dow 30 company. It employs over 240,000 employees. In 2006, the company generated $88 billion in annual revenue and spent $17.1 billion on capital investments. Verizon's state-of-the-art voice, data and video networks are touched by over 100 million consumers and government and business customers daily.

Given its breadth of service and geographic coverage, Verizon's commitment to national security and emergency preparedness—grounded in corporate policy, sound business practice and hands-on experience—is long-standing and growing. In order to ensure the continuity of its own operations and to meet the requirements of its critical customers in time of crisis, Verizon has:

- Designed, built and managed network facilities that are robust and resilient;
- Embraced "best practice" business methods and security procedures;
- Created and tested business continuity and emergency preparedness programs that have served the corporation and its customers in times of stress;
- Responded successfully to a wide range of crises; and,
- Provided leadership strength to industry and government organizations dedicated to national security and emergency preparedness.

**Verizon's Internal Security Councils:** Verizon takes a holistic approach to addressing information security by coordinating business unit activity around network and information protection. This effort is led by the Verizon Executive Security Council (VESC), established in 1995 to oversee all aspects of information security within Verizon. Reporting to the VESC is the Verizon Information Security Council (VISC), an enterprise-wide, cross-organizational working committee comprised of lead security managers and information security teams. The VISC is charged with instituting a secure environment for company network, information management, processing, transport and delivery.

The Verizon business units that comprise the VISC are dedicated to providing coordinated information and network security services for Verizon. These services include firewall support, host (mainframe and distributed) management, virus protection, risk assurance, information security practices, information security awareness, Incident Response & Vulnerability scanning, and remote access security administration.

*Computer Intrusion Response Team (CIRT):* The Verizon CIRT provides 7x24 coverage for the entire enterprise, supporting all business units and organizational points of contact to assess intrusion impacts, contain and control further dissemination of problems across the company, and capture and preserve evidence for law enforcement/legal purposes. The CIRT also provides restoration options, identifies and closes security vulnerabilities (exploited or otherwise), and uses secure communication channels during response.

The CIRT's network of contacts and organizational breadth enable it to effectively work with the appropriate company personnel to coordinate incident response and

resolution. A single point of contact is designated for all network or computer related security advisories to the enterprise, thus eliminating duplication of information and effort by quality checking all data prior to distribution. A historical repository of advisory data is also maintained for reference.

*Management Structure:* Verizon has sharpened its focus in addressing its evolving challenges in network technology and security. Key internal organizations have been realigned to apply consistent, best practice solutions to IT and network technology across business units. Verizon's Executive Vice President and Chief Information Officer has oversight over a range of technical support organizations serving the company's major business units. Meanwhile, a newly created position of Executive Vice President and Chief Technology Officer has responsibility for establishing and managing the overall direction, technology and planning of all Verizon networks. The CTO in each of Verizon's business groups remains responsible for the day-to-day execution of their network deployment strategies.

*Technical Support:T1 A full array of internal technical, consulting and R&D services are available to guide decision making and strengthen best practice within all major business units. For instance, the Verizon Information and Network Security organization advances security strategies that integrate people, process and technology (such as firewalls, intrusion detection systems, virus protection, and remote access) with full adherence to information security policies and practices; while also providing technical and consulting services to business units—all with a primary focus on information asset protection.*

*Verizon Information Security Focus is Crucial:* In today's evolving threat environment, malicious insiders are the greatest threat to our critical national infrastructures. Today's geo-political climate will result in cyber attacks against national communications and control systems of economic, safety, or political significance. And politically (ideologically) motivated cyber attacks are increasing in volume, sophistication, and coordination. Verizon is addressing today's very real threats. Standards organizations must address carrier class security issues and architectures. The vendor community needs to produce equipment & software that meet Verizon's security objectives. And our customers and peer carriers need to work with us to mitigate security risks.

**Sector Leadership and Collaboration:**

Verizon, and its peer companies within the Communications Sector, have a long history of cooperation in national security and emergency preparedness. This history distinguishes the Communications Sector from most other critical sectors identified in the National Infrastructure Protection Plan. The sector personifies cooperation and trusted relationships that have resulted in the delivery of critical services when emergencies and disasters occur. A strong bond between the private and public sectors exists today in large part because of several organizations that were created in response to earlier threats to the nation's critical infrastructure.

*National Communications System:* The Sector Specific Agency for the Communications Sector is the National Communications System (NCS), currently housed within the Department of Homeland Security's National Cyber Security and Communications Division.

The NCS was established by President Kennedy in the aftermath of the Cuban missile crisis when communications problems between the United States and key international players threatened to further complicate the crisis. Since 1963, the NCS has worked to strengthen the communications facilities and components of various Federal agencies, focusing on interconnectivity and survivability.

*National Coordinating Center for Telecommunications:* In 1982, telecommunications industry and Federal Government officials identified the need for a joint mechanism to coordinate the initiation and restoration of national security and emergency preparedness telecommunications services. In 1984, Executive Order 12472 broadened the NS/EP role of the National Communications System and created the National Coordinating Center for Telecommunications as a central public-private sector organization to coordinate response to emergency communications situations.

In January 2000, the NCC was designated an Information Sharing and Analysis Center for Telecommunications in accordance with PDD–63. The NCC–ISAC facilitates information sharing among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure.

*The National Security Telecommunications Advisory Committee (NSTAC):* The NSTAC was created 25 years ago, in 1982, by Executive Order 12382. NSTAC provides another highly successful example of how the private sector helps direct government decisions around national security and emergency preparedness commu-

nications (NS/EP). This advisory committee to the President brings together 30 industry chief executives representing major telecommunications companies, network providers, information technology companies, finance and aerospace businesses. NSTAC provides industry-based advice and expertise to the President on a wide range of telecommunications problems related to implementing NS/EP communications policy issues. These include, but are not limited to, information security, information assurance, and critical infrastructure protection.

NS/EP communications enable the government to make an immediate and coordinated response to all emergencies, including cyber attacks. NS/EP communications allow the President and other senior Administration officials to be continually accessible, even under stressed conditions. The impact of today's dynamic technological and regulatory environment is profound with new technologies and increasing competition bringing both new opportunities and new vulnerabilities to the information infrastructure. The NSTAC is strongly positioned to offer advice to the President on how to leverage this dynamic environment to enrich NS/EP communications capabilities and ensure that new architectures fulfill requirements to support NS/EP operations; and to avoid introducing vulnerabilities into the information infrastructure that could adversely affect NS/EP communications services. The NSTAC's current work plan includes issues ranging from information sharing and the security and reliability of converged networks to research and development (R&D) issues related to converged networks.

*The Network Reliability and Interoperability Council (NRIC):* Government-imposed solutions may hinder the ability of business to adapt and respond effectively to the changing threat environment. So it becomes critical for business and government to work collaboratively towards solutions that are meaningful, adaptable and sustainable. The voluntary development of and compliance with "best/sound practice" approaches to physical and cyber security is a model that is time tested. It is illustrated through the work of the Federal Communications Commission's Network Reliability and Interoperability Council. The NRIC is a successor to the National Reliability Council, first established in 1992. Through the work of seven successive councils, subject matter experts from business and government have come together to address network reliability and interoperability issues of concern, develop best/sound practices and encourage voluntary adoption. The NRIC will soon merge with the Media Security and Reliability Council (MSRC) to create a new organization, the Communications Security, Reliability, and Interoperability Council (CSRIC).

*National Security Information Exchange (NSIE):* In April 1990, the Chairman of the National Security Council's Policy Coordinating Committee requested the NCS Manager identify what actions industry and Government should pursue to protect critical NS/EP telecommunications from the growing "hacker" threat. The NCS Manager subsequently requested that the NSTAC provide industry's perspective on the network security issue. Ultimately NSTAC created a mechanism for security information exchange and produce a corresponding implementation plan. The NSTAC and NCS Manager also established separate, but closely coordinated, Network Security Information Exchanges (NSIEs). In May 1991, the NSIE charters were finalized, and NSTAC companies and government departments and agencies designated their NSIE representatives, chairmen, and vice-chairmen. The NSTAC and government NSIEs held their first joint meeting in June 1991.

Industry and government coordinate through their respective NSIEs to voluntarily share sensitive information on threats to operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. Government NSIE members include departments and agencies that use national security and emergency preparedness (NS/EP) telecommunications services, represent law enforcement, or have information relating to network security threats and vulnerabilities. NSTAC NSIE representatives include subject matter experts who are engaged in prevention, detection, and/or investigation of telecommunications software penetrations or have security and investigative responsibilities.

**The Communications Sector Coordinating Council (CSCC) and its Sector Specific Plan (SSP):**

Verizon recognizes its critical operational dependence on other sectors and has established the necessary vendor relationships to meet both normal and extraordinary continuity of business requirements. In turn, all critical sectors are heavily reliant on the Communications Sector to support their own continuity of operations.

The Homeland Security Act of 2002 provided the basis for DHS' role in the protection of the nation's critical infrastructure and key resources (CI/KR.) The Act assigned DHS responsibility for developing a comprehensive national plan for securing CI/KR in conjunction with other Federal agencies, State and local agencies and authorities, the private sector and other entities.

The complexity of cross sector independencies was recognized in the 2006 National Infrastructure Protection Plan, resulting from Homeland Security Presidential Directive 7. HSPD–7 focused on the identification, prioritization and protection of the nation's critical assets. It prescribed the development of the National Infrastructure Protection Plan (NIPP) and corresponding Sector Specific Plans. Perhaps most significantly, the NIPP encouraged the establishment of sector coordinating councils. In so doing, it brought greater sector diversity to the table and significantly advanced the institutional capacity of sectors to formally and proactively address cross-sector dependencies.

*Communications Sector Coordinating Council (CSCC):* The Communications Sector Coordinating Council (CSCC) became operational in calendar year 2006. It was chartered to foster the coordination of policy initiatives to improve the physical and cyber security of sector assets, and ease the flow of information within the sector, across sectors and with designated Federal agencies. Through the CSCC, private-sector owners, operators and suppliers can engage Federal government entities to: identify and coordinate policy issues related to the protection of critical infrastructure and key resources; facilitate the sharing of information related to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices; and, address policy issues related to response and recovery activity and communication following an incident or event. The CSCC now embraces 35 member companies and has become more representative of the diversity of the Communications sector. Members include wireline, wireless, cable, satellite, information service providers, as well as commercial and public broadcasters, service integrators, and equipment vendors. Small and medium size companies are represented through CTIA, USTelecom, ITA and NCTA. Verizon currently chairs the CSCC.

CSCC members meet quarterly to review industry and government actions on critical infrastructure protection priorities, confer with Federal agency representatives, review cross sector CIP issues, and coordinate with industry participants in NSTAC and the NCC ISAC to ensure industry coordination. Council work groups meet frequently to engage industry and government SME's on task force initiatives. Top 2007 CSCC priorities include the sector's risk assessment of critical assets, cross sector pandemic planning and implementation of access and credentialing and emergency wireless protocols.

The CSCC and IT Sector Coordinating Councils maintain close coordination on a range of policy and operational initiatives. Both sectors participate in a recently formed cross sector cyber security work group. Both have worked to heighten industry's role in NS/EP exercises such as last summer's ESF2 exercise in New Orleans and in TopOff 4. In the aftermath of Katrina, the Councils met to discuss ways of strengthening industry preparation and response to major events. Both participate in ongoing sector risk assessment activity. Both organizations have elected sector liaisons to attend each other's coordinating council meetings and they meet annually to confer, with government counterparts, on ongoing sector activity.

*Partnership for Critical Infrastructure Protection (PCIS):* The Communications Sector Coordinating Council is a member of the Partnership for Critical Infrastructure Security (PCIS.), a private sector organization. PCIS is comprised of the leadership from each of the Sector Coordinating Councils, which represent the owners and operators of the critical infrastructure and key resources sectors identified by the government in HSPD–7. The mission of PCIS is to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services. This mission encompasses physical, cyber, and human security that rely on strong infrastructure integrity and resilience. Accordingly, the PCIS mission spans the full spectrum of critical infrastructure matters from prevention, planning, and preparedness to business continuity, mitigation, response, and recovery.

The PCIS has worked to encourage a productive industry partnership with the Federal government over the past six years. It was formally recognized as the Private Sector Cross–Sector Council in the National Infrastructure protection Plan when it was released in 2006. The NIPP states that the "cross-sector issues and interdependencies are addressed among the sector coordinating councils through PCIS. PCIS members, including the CSCC, continue to work with designated Federal agencies on implementation of their sector specific plans.

*Communications Sector Specific Plan (CSSP):* The CSCC completed work on the CSSP for critical infrastructure and key resource (CI/KR) protection, as recommended by the NIPP, in December 2006 the plan was subsequently released in May 2007. It was developed jointly by industry and the National Communications System, with input from Federal government agencies ranging from the US Department of Commerce to the Federal Communications Commission.

The CSSP provides a framework for protecting the Nation's critical communications assets and key resources. It addresses asset identification, risk assessment and mitigation, protective programs and government measurements.

The goals of the CSSP include the need to:

- Protect the overall health of the national communications backbone;
- Rapidly reconstitute critical communications services after national and regional emergencies;
- Plan for emergencies and crises by participating in exercises and updating response and continuity of operations plans;
- Develop protocols to manage the exponential surge in utilization during an emergency situation and ensure the integrity of sector networks during and after an emergency event;
- Educate stakeholders on communications infrastructure resiliency and risk management practices in the Communications Sector;
- Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decision makers in the sector;
- Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness, and cross-sector incident management.

The CSSP acknowledges the lead role played by private sector owners and operators in protecting critical assets. The communications companies that own, operate and supply the Nation's communications infrastructure have historically factored natural disasters and accidental disruptions into network resiliency architecture, business continuity plans, and disaster recovery strategies. The interconnected and interdependent nature of these service provider networks has fostered crucial information sharing and cooperative response and recovery relationships for decades. The CSSP also articulates the role of the Federal government in providing the support and resources necessary to identify threats and help mitigate risk.

The Communications Sector's strategy is to ensure the nation's communications networks and systems are secure, resilient, and rapidly restored after an incident. The approach outlined in the CSSP includes:

- Defining industry and government roles in protecting communications infrastructure by leveraging corporate capabilities and government programs;
- Adopting an architectural approach to infrastructure identification and risk assessment processes;
- Coordinating with other sectors and customers on critical infrastructure dependencies and solutions for mitigating risk; and
- Working closely with DHS to advance sector protection and mitigation measures.

The CSSP defines the three major arenas where risk assessments are conducted: industry self-assessments; government-sponsored assessments and government-sponsored cross sector dependency analyses. Industry self-assessments of risk are ongoing. Such assessments are conducted to verify compliance with company policies, industry standards, contract agreements and regulatory requirements.

Throughout 2007, industry has turned its attention to working with government to define relevant government sponsored assessments through a National Sector Risk Assessment (NSRA) process. Through this process, industry and government have undertaken a qualitative risk analysis of Communications Sector infrastructure and have narrowed the scope of risk assessments to nationally critical network elements. This process will result in a draft government assessment by December 2007, with a final report to be completed by March 2008. Based on the outcomes of this government assessment process, government may conduct more quantitative assessments of selected architecture elements in conjunction with industry.

The third and final element of the CSSP risk assessment process is the analysis that government will undertake with industry on cross-sector dependencies. Work will commence in 2008, the process will identify high-level critical sector communications dependencies and will leverage NCS risk assessment methodologies to identify communications dependencies specific to a facility or function. The goal will be to assist other sectors in the assessment of communications dependencies for high-risk assets.

The Communications and IT Sector Coordinating Councils have worked to ensure that respective risk assessment efforts, although distinct, are complementary where the sectors overlap. This cross-sector participation increases information sharing, including lessons learned. In each sector, cyber threats associated with the sector's functional or network elements will be identified and vulnerabilities and consequences associated with such threats will be assessed to determine risk.

Whatever success the CSCC has achieved in the development of the CSSP has resulted from industry's singular focus on developing a critical asset protection plan that is designed by industry for implementation by industry. In order to accomplish this, the NCS stepped forward to advocate industry positions within the Department of Homeland Security and with DHS project contractors. A strong element of social capital exists among industry representatives and Federal agency personnel within the Communications Sector. This trusted relationship helped to produce a practical, meaningful asset protection framework that can now be used by industry and government partners to better meet the country's security requirements. The CSSP is realistic and well-grounded.

**Critical Asset Protection Over the Long Term:** What cannot be underestimated by policymakers is the enormous amount of private sector resources that are being devoted to finding solutions—with government partners—to achieve greater effectiveness in our country's security and response programs. The Communications Sector continues to commit significant financial resources and subject matter expertise to strengthen critical business practices. It will continue to dedicate time and expertise to its work with the NCS and other Federal, state and local government partners to address emerging operational and policy issues.

To ensure even greater effectiveness in protecting the Nation's critical communications infrastructure—both physical and cyber—industry and government partners must be clear about their respective roles in getting the job done. Industry is the first line of defense in protecting assets and mitigating risks, and aggressive business continuity and security practice will remain critically important as the Nation's risk environment continues to evolve. Although the Communications Sector's long history of coordination will change as industry restructuring continues, close planning and coordination within the sector will continue to be a mainstay of efforts to fortify physical and cyber security programs.

Government must continue to ensure clarity of roles and responsibilities among all levels of government and the private sector. It should continue to advocate for strong sector and cross sector collaboration on operational and policy issues and in providing the necessary intelligence and operational support to ensure effective industry preparedness and response, in particular by refining and improving roles and responsibilities in the National Response Framework.

Although industry and government have made progress on long standing issues pertaining to protection of critical assets and key resources, much work lies ahead. There must be an even greater Federal government focus on effective engagement and integration of state and local authorities in all aspects of critical infrastructure protection and emergency response, including the rollout and coordination of initiatives "on the ground". For instance, practical steps on access and credentialing and emergency wireless protocols for shutdown and restoration of service must be taken to facilitate industry response to natural or man-made disasters. Myriad jurisdictional laws and requirements may be complex, but real world execution is overdue. Government must also continue to integrate industry more fully on operational planning, coordination and joint policy initiatives. Effective partnerships require early involvement of industry and direct engagement in government programs, including protection and response plans, which impact the private sector's critical industry assets. Although government has recognized the importance of sharing timely threat intelligence with industry, more needs to be done in this area to advance NS/EP interests. Finally, recent Congressionally mandated changes in organization and functions within DHS need to be fully implemented and understood by all stakeholders in the critical infrastructure protection and emergency response domain. In sum, Industry and the Federal government have much to do on the full array of critical infrastructure protection initiatives, while advancing transition plans for the upcoming change in Administration.

Mr. Chairman, this concludes my testimony. I would be happy to answer any questions you or the subcommittee might have about Verizon or the Communications Sector.

Mr. LANGEVIN. I now recognize Mr. Hender to summarize your statement for 5 minutes.

## STATEMENT OF GEORGE HENDER, BANKING/FINANCIAL SECTOR COORDINATING COUNCIL, AND MANAGEMENT VICE CHAIRMAN, OPTIONS CLEARING CORPORATION

Mr. HENDER. Chairman Langevin, Chairwoman Jackson Lee, Ranking Members McCaul and Lungren, and members of both sub-

committees, my name is George Hender, and I am Chairman of the Financial Services Sector Coordinating Council, also known as FSSCC. I am pleased to appear today on FSSCC's behalf to discuss the important topic of cybersecurity.

FSSCC was established by the Department of Treasury. FSSCC is a private sector coalition of the Nation's leading banks, financial firms, insurance companies, and their trade associations. FSSCC worked collaboratively with Treasury, our sector specific agency, and with FSSCC, our government coordinating council, to craft our sector-specific plan.

Our plan identifies three specific goals: first, to maintain a sector strong position of resilience, risk management, and redundant systems;

Second, to manage the risk posed by cross-sector interdependencies; and

Third, to work with law enforcement, the private sector, and our international counterparts to track and arrest criminals.

The remainder of my testimony will focus on FSSCC's efforts to meet these goals in the area of cybersecurity.

Modern financial services are built on a foundation of informational technology. Financial firms' systems are a target for cyber attack because that is where the money is. As the nature and the complexity of attacks grow more sophisticated, FSSCC continues to implement a number of cyber-related initiatives. I would like to highlight some of those initiatives.

A year prior to the National Infrastructure Protection Plan's release in 2006, FSSCC formed the first sector R&D committee. In April 2006, this committee published The Research Challenges, a report identifying eight specific R&D priorities. An overarching theme throughout this report is protecting the sector from cyber attacks.

In October 2006, the R&D committee published our research agenda to demonstrate how research challenges relate to the NIPP. Together with these two publications, the necessary steps to produce a robust cyber secure platform was formed.

Another vital asset of FSSCC is the Financial Services Information Sharing Analysis Center, or FS–ISAC. Our ISAC has been an effective information-sharing tool in the fight against cyber attacks. Every day our ISAC forwards cyber and physical security risk updates from over 100 sources to over 11,000 sector participants. Our ISAC also shares this information with Treasury and law enforcement to help stop and prevent attacks.

FSSCC and our ISAC have also been active participants in several business continuity exercises, including the congressionally mandated Top Off exercises. Additionally, ISAC represented FSSCC in Cyber Storm and Cyber Tempest, two exercises focused on cyber-related issues. Our ISAC is also helping us to plan for Cyber Storm II, which is scheduled for March 2008.

FSSCC believes exercise participation is critical, and we encourage the planners of these exercises to include the private sectors during the planning phases of these exercises.

FSSCC has been an active participant in the Partnership for Critical Infrastructure Security, PCIS. I am a member of the execu-

tive committee and board of PCIS. PCIS has a working group focusing on cross-sector collaboration on cybersecurity issues.

Many cybersecurity issues are ongoing and there are still several issues to address. Two issues relate to the GAO's SSP report and the DHS's R&D budget. According to GAO, the banking and finance sector SSP was ranked somewhat comprehensive in addressing cybersecurity. Because the GAO did not consult with the Treasury or FSSCC when preparing this report, I respectfully disagree with their conclusions.

Our SSP included the research challenge document which fully addresses the GAO criteria for cybersecurity R&D. For example, our R&D committee is identified as the primary mechanism to solicit information on R&D initiatives; and the research challenges report details the sector's goals and gaps related to cybersecurity. Examples of the SSP in my written testimony contradict GAO's finding that we failed to identify the programs to detect, deter, respond, and recover from cyber attacks.

The GAO report also stated our SSP failed to describe the process for R&D investment priorities, but the R&D committee clearly identified a number of priorities where investment dollars could be directed. Without further guidance, it is unclear how the GAO reached these conclusions. We will welcome a dialogue with GAO on these important issues.

Finally, FSSCC believes DHS should consult with the private sector when funding private research. FSSCC thinks it makes good economic sense to fund R&D industry experts and to use those experts to achieve this goal. Greater communication and consulting is necessary between DHS, Treasury, and FSSCC.

Another option would be to provide direct grant authority to the Treasury. Currently, FSSCC can only influence R&D projects through comment letters.

In short, FSSCC believes that the DHS cybersecurity R&D budget should be more closely aligned with the level of threat. An appropriation of only $11 million is clearly insufficient. Our Nation would be better served by providing additional budget discretion and dollars to projects identified by the industry under attack.

Thank you for the opportunity to provide FSSCC's views for this important hearing. I would be pleased to answer any questions.

[The statement of Mr. Hender follows:]

PREPARED STATEMENT OF GEORGE S. HENDER

Chairman Langevin, Chairwoman Jackson Lee, Ranking Members McCaul and Lungren, and members of the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology and the Subcommittee on Transportation Security and Infrastructure Protection of the House Homeland Security Committee, I am George Hender, Management Vice Chairman of The Options Clearing Corporation (OCC), which is the world's largest derivatives clearing organization.[1] OCC is a leader in business continuity planning in the financial services sector and was a founding member of the Financial Services Sector Coordinating Council (FSSCC) and ChicagoFIRST, a regional public/private partnership addressing homeland security and emergency management issues in the financial services industry. I am pleased

[1] OCC, founded in 1973, was the first clearinghouse to receive a 'AAA'credit rating from Standard & Poor's Corporation. Operating under the jurisdiction of the Securities and Exchange Commission and the Commodity Futures Trading Commission, OCC provides clearing and settlement services for the American Stock Exchange, the Boston Options Exchange, the Chicago Board Options Exchange, the CBOE Futures Exchange, the International Securities Exchange, NYSE Arca, OneChicago, the Philadelphia Stock Exchange and the Philadelphia Board of Trade.

to submit this statement on the very important topic of cybersecurity on behalf of FSSCC.[2]

On June 6, 2006, I was appointed to serve as Sector Coordinator for the Financial Services Sector by former Secretary of the Treasury John Snow. Thus, I am the Chairman of FSSCC. Prior to my appointment, I served as FSSCC's Vice Chairman from September 2004 through May 2006. Additionally, I am on the Executive Committee and Board of the Partnership for Critical Infrastructure Security (PCIS), which is the private sector organization that coordinates homeland security issues for all national critical infrastructures. I have also formerly served as Vice Chairman of the Financial Services Information Sharing and Analysis Center (FS–ISAC). This is the organization responsible for communicating key cyberspace, physical security, and Homeland Security information to the financial services sector.

I applaud the Committee for holding today's hearing on such an important topic. Before I focus on measures taken by FSSCC related to cybersecurity, I would first like to discuss the important role the financial services sector has in our economy and the role FSSCC plays in improving the sector's resilience through safeguarding its critical infrastructure and employees.

**Introduction and Background**

The United States financial services sector is the backbone of the world economy. With United States assets estimated to be in excess of $55 trillion,[3] this large and diverse sector accounted for over $1 trillion in 2006 gross domestic product (GDP) or 7.8 percent of total GDP.[4] The sector is primarily owned and operated by the private sector whose institutions are extensively regulated by Federal and, in many cases, state government. In addition to these public sector entities, self-regulatory organizations (SROs), such as the 1Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), and the National Futures Association (NFA), and exchanges, such as the Chicago Mercantile Exchange (CME), the New York Stock Exchange (NYSE), also play an important role in industry oversight.

Working together, the public and private sector regulators encourage a highly competitive market where identifying and managing a myriad of financial and non-financial risks is essential to success. Through numerous laws enacted by Congress over the past 150 years, federal financial regulators have implemented a complex regime that includes examinations of the sector's institutions' operational, financial and technological systems. These examinations are designed to determine the extent to which an institution is addressing its financial and non-financial risks, such as Internet and information technology vulnerabilities. They also evaluate the adequacy of controls and applicable risk management practices at the institution.

*Public-Private Partnership*

Both the public and private sector financial services organizations recognize the importance of business continuity planning in preparing for catastrophic events; however, our sector's organizations know they will not operate as independent entities during a real crisis. Therefore, planning for these events should be done in a coordinated fashion.

FSSCC was established at the request of the U.S. Treasury Department in response to Homeland Security Presidential Directive 7, which required sector-specific Federal departments and agencies to identify, prioritize and protect United States critical infrastructure and key resources. We are a private sector coalition of the nation's leading financial services firms and trade associations that are working to reinforce the financial services sector's resilience to terrorist attacks, man-made and

---

[2] The members of FSSCC are the America's Community Bankers (ACB); American Bankers Association (ABA); American Council of Life Insurers (ACLI); American Insurance Association (AIA); American Society for Industrial Security (ASIS) International; BAI; BITS/The Financial Services Roundtable; ChicagoFIRST; Chicago Mercantile Exchange (CME); The Clearing House (TCH); CLS Group; Consumer Bankers Association (CBA); Credit Union National Association (CUNA); The Depository Trust & Clearing Corporation (DTCC); Fannie Mae; Financial Industry Regulatory Authority (FINRA); Financial Information Forum (FIF); Financial Services Information Sharing and Analysis Center (FS–ISAC); Financial Services Technology Consortium (FSTC); Freddie Mac; Futures Industry Association (FIA); ICE Futures U.S.; Independent Community Bankers of America (ICBA); Investment Company Institute (ICI); Managed Funds Association (MFA); The NASDAQ Stock Market, Inc.; National Association of Federal Credit Unions (NAFCU); National Futures Association (NFA); NACHA—The Electronic Payments Association; The Options Clearing Corporation; Securities Industry Automation Corporation (SIAC); Securities Industry and Financial Markets Association (SIFMA); State Street Global Advisors; VISA USA Inc.

[3] http://www.financialservicesfacts.org/financial2/today/assets

[4] http://www.bea.gov/bea/dn2/gdpbyind__data.htm

natural disasters, and other threats, such as cyber attacks, facing the sector's critical infrastructure.

FSSCC closely interacts with its Sector Specific Agency (SSA), the Department of the Treasury (Treasury), and the Financial and Banking Information Infrastructure Committee (FBIIC), its public-sector counterpart.[5] We also strongly support regional public/private partnerships, such as ChicagoFIRST and DFW*first*. These organizations address homeland security and emergency management issues on a local level, where many catastrophic events are primarily managed.

The combined efforts and close interaction of these groups with FSSCC fosters a spirit of cooperation within our sector that facilitates effective preparation for a critical event, such as a cyber attack. Equally important, this collaboration creates a streamlined approach to working with other sectors where cross-industry interdependencies exist. The financial services sector is very dependant on a number of other sectors, especially the energy, telecommunications and transportation sectors.

At the beginning of my term as FSSCC Chairman, I personally met with representatives from nearly every FSSCC member to solicit their ideas on how to further strengthen the resilience of the financial services sector and reduce vulnerability to cyber threats, terrorist attacks, criminal or illegal activities, and manmade or natural disasters. These conversations, as well as the large number of formal and informal meetings taking place each year within FSSCC and between FSSCC and FBIIC, help show how our partnership model addresses threats and risks posed by the Sector's dependency upon other sectors.

FSSCC's general meetings provide an example of this model. Here members meet and hear from critical sectors on which our sector heavily relies. They also provide a venue in which to coordinate and prioritize sector initiatives. Another example is the FSSCC working group which is working with the Department of Homeland Security (DHS) to develop an emergency credential for FSSCC members' use in extraordinary emergencies. Development of such a credential is a priority reflected in our overall research plan. Just this last summer, the FSSCC credentialing working group participated in the cross-sector exercise known as "Summer Breeze." This exercise validated the use of First Responder Authentication Credential (FRAC) identification cards.

Arguably, the most important example of collaboration within the sector is the ongoing effort to plan for pandemic influenza. On October 12, 2007, FSSCC and FBIIC completed the most comprehensive exercise ever held for the U.S. financial services sector. This important exercise focused on the response of the sector's members to pandemic influenza; over 2,700 financial firms participated. FSSCC understands that effective business continuity planning must envision and prepare for a diverse range of issues and threats. This is encompassed in our mission statement and goals.

**FSSCC's Mission and Goals**

FSSCC's mission is to foster and facilitate the coordination of sector-wide voluntary activities and initiatives designed to bolster critical infrastructure protection and homeland security. FSSCC strives to improve sector awareness of critical infrastructure protection issues, to promote information sharing on these issues, and to find opportunities for improved coordination throughout the sector. Through its efforts, FSSCC seeks to enhance public trust and confidence in the sector's ability to withstand and recover from significant disasters.

Treasury, in close collaboration with FSSCC and FBIIC, completed the Banking and Finance Sector's Sector Specific Plan (SSP)[6] in December 2006. This plan, combined with the 16 other critical infrastructure SSPs, helps form the overall National Infrastructure Protection Plan (NIPP). Our sector's SSP outlines a strategy for working collaboratively with public and private sector partners to identify, prioritize and coordinate the protection of critical infrastructure. FSSCC believes DHS appropriately guides each critical infrastructure sector in coordinating their SSPs. However, each sector specific agency should retain control over SSP implementation.

---

[5] The members of FBIIC are the Commodity Futures Trading Commission (CFTC); the Conference of State Bank Supervisors (CSBS); the Department of the Treasury; the Farm Credit Administration (FCA); the Federal Deposit Insurance Corporation (FDIC); the Federal Housing Finance Board (FHFB); the Federal Reserve Bank of New York; the Federal Reserve Board (Fed); the National Association of Insurance Commissioners (NAIC); the National Association of State Credit Union Supervisors (NASCUS); the National Credit Union Administration (NCUA); the North American Securities Administrators Association (NASAA); the Office of the Comptroller of the Currency (OCC); the Office of Federal Housing Enterprise Oversight (OFHEO); the Office of Thrift Supervision (OTS); the Securities and Exchange Commission (SEC); and the Securities Investor Protection Corporation (SIPC).

[6] https://www.fsscc.org/reports/2006/Bank__Finance__SSP__061213.pdf

Also, DHS and each sector should view the SSPs as a starting point for developing a comprehensive, nationally-oriented, critical infrastructure regime.

The Banking and Finance Sector's SSP, including its Research and Development (R&D) appendices, outlines three sector-specific goals. First, the sector seeks to maintain its strong position of resilience, risk management and redundant systems, in the face of a myriad of intentional, unintentional, man-made and natural threats. Second, the sector aims to address and manage the risks posed by the sector's dependency on telecommunications, information technology, energy and transportation sectors. Lastly, the sector plans to continue to work with the law enforcement community, the private sector, and our international counterparts to increase available resources used to track and arrest criminals. Specifically, to track and arrest those persons responsible for crimes against the sector, including cyber attacks and other electronic crimes.

The remainder of my testimony will focus on FSSCC's efforts in addressing these goals in light of protecting against cyber attacks and other electronic crimes.

**Specific Actions for Cybersecurity**

Modern financial services are built on a foundation of information technology, including computing hardware, software and telecommunications. This foundation is afflicted by multiple vulnerabilities and an increasingly high level of threats. Our sector's cybersecurity strategy seeks to address these threats by generally focusing on people, process and technology. Ensuring our sector has the brightest minds, most efficient processes and state-of-the-art technology to protect against cyber threats is our highest priority because our sector understands our entities' systems and networks are a target because "that's where the money is."[7] In addition, as September 11, 2001, showed us, our sector is a focus of terrorists because of our iconic status.[8]

---

[7] The members of FBIIC expend considerable effort to ensure the information security platforms serving as our industry's cornerstone are not compromised. In the case of financial institutions, federal examiners are often permanently located within the entity being reviewed. The Federal Financial Institutions Examination Council (FFIEC) is the primary federal interagency body empowered to develop uniform principles and standards for the examination of financial institutions. The FFIEC operates an Information Technology Council devoted to addressing cybersecurity issues, and its recommendations are incorporated into the FFIEC Handbook. Examiners use the Handbook to determine the extent to which the institution has identified its financial and non-financial risks, such as Internet and information technology vulnerabilities. Also, it is used to evaluate the adequacy of controls and applicable risk management practices at the institution. Additionally, the federal financial regulatory authorities issue numerous guidance documents and Financial Institution Letters (FILs) specifically related to cybersecurity. Similarly, the Securities and Exchange Commission and the securities SROs review the cybersecurity programs of exchanges, broker-dealers and clearing organizations as part of their ongoing supervisory exams and related activities.

[8] For many years, the culture of our sector has emphasized strong internal controls, physical and cybersecurity, and a comprehensive approach to business continuity planning that recognizes the importance of recovering and resuming business operations as swiftly as possible. Business continuity planning in our sector follows an "all hazards" approach that focuses on the impact of a disruption, rather than its cause, to ensure that high impact but low probability events are incorporated into the planning process. After September 11, the Fed, Office of the Comptroller of the Currency, and SEC issued the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (Sound Practices Paper), Securities Exchange Act Release No. 47638 (April 7, 2003). This paper identified stringent resumption or recovery objectives for core clearing and settlement organizations providing services for critical financial markets or acting as large payment system operators, and for firms that play significant roles in one or more critical financial markets. The Sound Practices Paper sets out an objective of recovering or resuming clearing and settlement activities within the business day on which a disruption occurs and maintaining geographically dispersed resources sufficient to meet those recovery or resumption activities. Last year, the agencies that issued the Sound Practices Paper reported to Congress that "the core clearing and settlement organizations, which present the greatest potential risk to the operation of the financial system, have made significant investments in their operating infrastructures, and all have achieved substantial implementation of the sound practices." Joint Report on Efforts of the Private Sector to Implement the Interagency Paper on Sound Practices to Strengthen the resilience of the US. Financial System (April 2006).

GAO has also examined the preparedness of these organizations in the light of the Sound Practices paper, and has found continuing progress in protecting our nation's financial system from a variety of threats, including cyber attacks. *See Financial Market Preparedness: Significant Progress Has Been Made, But Pandemic Planning and Other Challenges Remain* GAO–07–399 (March 2007); *Financial Market Organizations Have Taken Steps to Protect Against Electronic Attacks, But Could Take Additional Actions* GAO–05–679R (June 2005): *Financial Market Preparedness: Improvements Made, But More Action Needed to Prepare for Wide-Scale Disasters* GAO–04–984 (September 2004).

Our sector faces a number of cyber-related threats such as, hacking, virus dissemination, software piracy, identity theft, account fraud, phishing,[9] spoofing,[10] and pump and dump[11] schemes. FSSCC's members have responded to these challenges aggressively. For example, FSSCC member organizations have prepared a document to help financial institutions develop and execute response programs when confidential and sensitive information is accessed or misused by unauthorized individuals. The Identity Theft Assistance Center, developed by a FSSCC member, provides a free victim assistance service and provides data about identity theft to law enforcement.

The financial services sector has always placed itself on the cutting edge of cybersecurity initiatives. Our institutions were among the first to have Chief Information Security Officers as part of their management teams. Also, the sector was among the first to use various authentication tools to protect against internet fraud. Similarly, many financial institutions embrace the concept of layered security by using multiple intrusion detection and prevention products. Firms regularly work with technology companies to improve these products. Without such security measures in place, customers would hesitate to use on-line products which are a central component of a financial firm's business model. In addition to the threat to individual customers, our sector is also focused on cyber-related threats to our financial structure. The nature and complexity of attacks are growing more sophisticated. As a result, our sector works in close collaboration with the nation's intelligence community to address this concern.

*FSSCC R&D Committee*

Prior to the NIPP's issuance in June 2006, FSSCC recognized cybersecurity as a critical issue and formed a standing R&D Committee. This committee was established to identify and prioritize areas of need, in which the most promising opportunities exist for research and development initiatives. These initiatives significantly improve the sector's critical infrastructure protection. The R&D Committee began developing a list of priorities in 2005. In April 2006, the committee published *Research Challenges,*[12] a document which identifies eight R&D areas the sector needs to address.[13]

An over-arching theme throughout our *Research Challenges* is securing the sector's information technology infrastructure to prevent intrusion from unauthorized sources. In October 2006, the FSSCC R&D committee, with Treasury advising, demonstrated for DHS how FSSCC's *Research Challenges* related to the NIPP by publishing FSSCC's *Research Agenda.* Together these two publications provide industry, academia, and the public with a shared insight into the opportunities and requirements necessary to produce a robust cybersecurity platform.

*FS–ISAC*

The FS–ISAC is another vital asset to FSSCC and the sector. It was created on October 1, 1999, as a means of meeting the sector's information-sharing obligation under the 1998 Presidential Decision Directive 63 on Critical Infrastructure Protection.[14]

The FS–ISAC channels information from more than 100 sources to reach over 11,000 sector participants daily and promotes information sharing between the public and private sectors. The FS–ISAC provides sector-wide knowledge about cyber and physical security risks faced by the financial services sector. Specifically, FS–ISAC's incident alerts notify members about the type of attack, its origin, and suggested remedial action. FS–ISAC information allows members to immediately receive threat and vulnerability information; share vulnerabilities anonymously and communicate within a secure portal; access new data feeds of threat and vulnerability information; and access a wide range of user data from which users can

[9] "Phishing" is a fraudulent scheme where an e-mail directs its recipients to Web sites where they are asked to provide confidential personal or financial information. Reports of phishing attacks have risen dramatically in the last year.

[10] "Spoofing" is an attempt to gain unauthorized system access by mimicking, impersonating or posing as an authorized user.

[11] "Pump and Dump" is a fraudulent scheme involving artificially inflating the price of a stock or other security through false or exaggerated promotion. Then the stock or security is sold at inflated prices.

[12] https://www.fsscc.org/reports/2006/Research__Challenges__Booklet061117.pdf

[13] The eight R&D projects are: (1) Secure Financial Transaction Protocol (SFTP); (2) Resilient Financial Transaction System (RFTS); (3) Enrollment and Identity Credential Management; (4) Suggested Practices and Standards; (5) Understanding and Avoiding the Insider Threat; (6) Financial Information Tracing and Policy Enforcement; (7) Testing; and (8) Standards for Measuring ROI of CIP and Security Technology.

[14] http://www.cybercrime.gov/white__pr.htm

produce their own reports and metrics. The FS–ISAC also uses this information to work with Treasury and law enforcement in helping to stop and prevent attacks.

Two important government information sources for the FS–ISAC's 24/7 Security Operations Center are DHS's Homeland Security Information Network (HSIN) and the U.S.-Computer Emergency Readiness Team (US–CERT). Relevant information from these data sources is monitored by the FS–ISAC and shared with trusted sector representatives through FS–ISAC's notification system and web portal. Then reports from FS–ISAC approved members are uploaded through the system. Both sources provide a valuable service to the FS–ISAC. FSSCC and the FS–ISAC continue to work with DHS to coordinate these reports into the sector's information sharing structure.

The FS–ISAC has been an effective tool in the fight against cyber attacks. For example, in November 2006, an FS–ISAC member detected an unusually large number of unauthorized log-in attempts against its systems and anonymously reported this information to the FS–ISAC. Soon after, the FS–ISAC issued an alert to its members. Later, five more financial institutions reported similar activity. This information sharing proved the financial institutions were under attack from a single source. While the attack was relatively insignificant in terms of its potential sector-wide impact, it demonstrates how the FS–ISAC's collaborative model can be an effective means to quickly deliver real-time information so financial institutions may be alerted to act against real threats.

The FS–ISAC was effective once again this past August when it alerted several member banks of suspicious web-site activity. The FS–ISAC then helped to avoid compromise of several major money center and regional banking institutions user accounts.[15]

*Cyber Syllabus*

In May 2006, the U.S. Department of Defense sought a private sector partner to help develop an undergraduate studies curriculum designed to provide exposure to information technology cybersecurity issues. FSSCC, through its R&D Committee, took the initiative to partner with the National Terrorism Preparedness Institute at St. Petersburg College in Florida to complete the project. I am pleased to report the syllabus was completed in May 2007, resulting in an on-line training program that can be made available to all universities. Additionally, FSSCC is working to identify an educational institution capable of making this program available to our members at no cost. It is our hope this type of public-private collaboration will help to inspire a new generation of ideas and resources devoted to protecting our nation's cyber space.

*Handbook of Science and Technology for Homeland Security*

Another joint DHS/FSSCC initiative currently underway is the drafting of a handbook designed to educate researchers on the critical needs of the homeland security and intelligence communities. It will also promote interdisciplinary dialogue in those fields. I am pleased to report FSSCC is on target to provide this information to DHS by year's end. Also, this handbook should be distributed worldwide in online and print formats next year.

*Cybersecurity Exercises*

FSSCC and FS–ISAC have been active participants in several business continuity exercises, including the congressionally mandated TOPOFF exercises and a number of regional and national cybersecurity exercises. In February 2006, FS–ISAC represented our sector in *Cyber Storm,* the first government-led, full scale cybersecurity exercise of its kind. Ten months later, in December 2006, FS–ISAC participated in *Cyber Tempest,* an exercise devoted to testing a wide area of cyber issues from a regional perspective. Both of these exercises provided positive benefits to our sector's business continuity planning, such as developing better integration between FSSCC and the FS–ISAC. FSISAC is now involved in planning Cyber Storm II scheduled for March 2008. These opportunities are a vital resource to leverage. We believe exercise leaders would benefit by increasing our level of involvement in future exercises.

*PCIS Working Group*

---

[15] FS–ISAC discovered use of Torpig Trojans, which use malicious code designed to place themselves into on-line banking applications for the purpose of stealing user login IDs and passwords. These Trojans evade detection by disabling security warning messages. Then they log open window sessions to capture user log-on information which is sent back to the attacker. After discovering use of the malicious code on several members' web sites, FS–ISAC was able to issue an incident alert that led to the discovery and eradication of this Trojan on web sites both in the U.S. and overseas.

FSSCC has been an active participant in PCIS, which was formally recognized in the NIPP as the Private Sector Cross-Sector Council. PCIS is dedicated to coordinating cross-sector initiatives aimed at promoting public and private efforts to improve the security and safety of our nation's critical infrastructure. PCIS has established a working group focused on cross-sector collaboration of cybersecurity issues. Each Sector Coordinating Council must appoint a sector representative to participate on the working group. The FSSCC has selected FS–ISAC Chairman, Eric Guerrino, for this task. The PCIS working group is another example of how the financial services sector is following a collaborative model to develop a strong cybersecurity network.

**Future Challenges**

FSSCC has achieved a great deal over the past few years. However, there are still many issues which must be addressed regarding cybersecurity. Some of these issues have been highlighted in a recent Government Accountability Office (GAO) report entitled *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cybersecurity Elements Varies.* Another less apparent, but equally important, issue includes increasing the level of consultation between DHS and its SSCs and SSAs over research and development initiatives. I will take a few moments to highlight each issue.

*GAO Report*

The GAO recently conducted a review of each SSP to determine if key aspects of cybersecurity related to the NIPP had been adequately covered. The GAO's preliminary results have found none of the plans fully addressed all 30 cybersecurity related criteria. Consequently, the GAO recommends that DHS require all SSPs be amended to address all cyber-related criteria by September 2008. Based on the cyber-related criteria established by GAO for its report, the GAO concluded the Banking and Finance Sector's SSP "somewhat comprehensively" covers cybersecurity. We respectfully disagree with the GAO's analysis. Because the GAO did not consult the SSAs or Sector Specific Councils when conducting its review, I would like to take this opportunity to explain our view on several areas the report concluded our SSP did not address.

Under section seven of the report, GAO stated our sector's SSP failed to (1) describe a process to solicit information on ongoing cyber R&D initiatives and (2) identifies existing cyber-related projects that support goals and identifies gaps. The sector's SSP highlights the R&D committee as the primary mechanism to solicit information on R&D initiatives, and the R&D Committee's *Research Challenges* outlines in detail the sector's goals and gaps related to cybersecurity. Further, our sector's priority on R&D is evidenced by the establishment of the FSSCC R&D Committee in 2005 and publication of its *Research* Challenges in April 2006, well before the NIPP was issued last year. FSSCC believes the SSP and the *Research Challenges* document, which was incorporated into the SSP in an appendix, adequately addresses the GAO's criteria. We welcome a dialogue with the GAO on this issue.

Additionally, GAO's review stated, under section five, that our sector failed to identify programs to deter, respond, and recover from cyber attack. The Banking and Finance Sector SSP used a deter, respond and recover approach throughout all sections. Our testimony today highlights a number of initiatives mentioned in our SSP aimed at this very issue—the R&D Committee, FS–ISAC, Cyber Syllabus, Cyber Threat Exercises, and PCIS. Consequently, without further guidance from GAO it is unclear how they reached a conclusion that our sector completely failed to address this issue.

The GAO report, under section eight, also stated our SSP failed to describe a process for investment priorities. Although FSSCC does not have any budget authority, we believe our R&D Committee's *Research Challenges* and *Research Agenda* highlight a number of priorities where investment dollars are most needed for our sector.

FSSCC, FBIIC and Treasury worked in close collaboration to develop our SSP, which we believe memorializes past and current initiatives into a living document serving as a guide for future action. In other words, we agree with DHS's assessment that the SSPs "represent only the early efforts by the sectors to develop their respective plans." Consequently, we welcome all comments and dialogue from interested parties on how to improve our nation's critical infrastructure protection regime and believe that our sector is a model for less regulated sectors with less mature cybersecurity plans.

*SSC/SSA R&D Budget*

FSSCC believes DHS should consult with the SSCs, and, at the very least, their SSAs, on business continuity research projects to ensure optimal resource allocation

is taking place. FSSCC would like to encourage the Subcommittees and Congress as a whole to work with DHS to ensure the same collaborative model used in our sector to generate business continuity information and reports extends to actual resource allocation for critical infrastructure programs. Failure to consult with experts from the organizations representing each sector severely limits the ability to maximize returns from investment dollars in an efficient manner.

Over the past few years, FSSCC and its members have devoted significant resources to generating information, developing plans, and identifying issues related to cybersecurity and opportunities for research for the public sector. While much information has been collected, FSSCC fears this information risks being lost in a "black hole." To avoid this result, FSSCC seeks to work with its public and private partners to develop a formal program that would channel resources to areas and programs that would provide the most positive impact for our nation's critical infrastructure. FSSCC thinks that it makes good economic sense to channel available sector and public research resources to programs supporting the *Research Challenges* and *Research Agenda* developed by industry experts on FSSCC's R&D Committee. To achieve this goal, greater communication and consultation about opportunities for R&D spending is necessary between DHS, Treasury and FSSCC. Another option would be to provide grant authority to SSAs such as the Treasury Department.

Currently, FSSCC is limited to influencing R&D project funding through support letters. Recently, FSSCC R&D Committee members visited Carnegie Mellon University (CMU) with a Treasury official to introduce CMU officials to the FSSCC R&D Agenda. While at CMU, the FSSCC R&D Committee reviewed CMU research projects that CMU judged to be of interest to the financial community. Committee members found that CMU projects focused on Operational Resiliency, Keystroke Pattern Analysis, Device-Enabled Authentication, and Insider Threat Analysis specifically addressed major FSSCC research challenges, as well as the corresponding NIPP research agenda themes. FSSCC could not fund these research projects but wrote letters of support to encourage funding from other sources.

FSSCC believes the DHS cybersecurity R&D budget should be more closely aligned with the threat posed. Twelve million dollars appropriated for this purpose is insufficient to cover the R&D demands within DHS and throughout the critical infrastructure sectors. Our nation would be better served by providing additional budget discretion and dollars to those most closely aligned with the work to be performed.

**Conclusion**

The financial services sector has a long history of thoughtfully and carefully preparing for threats to its critical infrastructure and employees. The members of FSSCC are proud of our progress since our inception in staying abreast of new and unexpected threats to the critical infrastructure of the financial services sector.

The financial services sector is working diligently to refine best practices, business continuity plans, and homeland security efforts to better protect employees and financial assets from cyber attacks. We are grateful for the collaboration and coordination with our public sector partners, the Department of the Treasury and the other members of FBIIC, as we develop these plans. We will continue to work diligently, and I am confident that the financial sector's preparation for cyber attacks will meet the high standards of planning for which our industry is well respected.

Thank you again for the opportunity to provide FSSCC's views for this important hearing. I would be pleased to answer any questions.

Mr. LANGEVIN. I want to thank the witnesses for their testimony. And I remind each member that he or she will have 5 minutes to question the panel.

I now recognize myself for 5 minutes for the purpose of questions.

Mr. Hender, thank you for your testimony. You discussed the R&D piece of your sector plan and your information sharing and analysis center. What I didn't hear, though, is how your sector protects its assets and what efforts are under way in that respect.

Would you address that?

Mr. HENDER. Certainly.

As I indicated in my testimony, our ISAC on a daily basis, a daily basis, receives well over 100 sources of independent informa-

tion which it analyzes, and then passes on that analysis every day before the markets open.

Mr. LANGEVIN. That is information sharing. What about—what steps do you take? What concrete steps are you taking?

Mr. HENDER. Well, part of the information that is fed to the 11,000 participants is, in fact, potential cyber attacks. They then take that information and use that information to look at their systems to see whether they have vulnerabilities.

Also, attacks take place and they are able to pass on to the other participants the attacks that are ongoing and how those attacks can be mitigated. We also use that information to pass on to the other government agencies to make sure that those attacks are taken seriously and the government agencies can use their best efforts to stop them.

Mr. LANGEVIN. I think, clearly, what would be helpful to this subcommittee, for better understanding of the situation, is more concrete steps—instead of action plans, steps that they actually take as opposed to just being notified and sharing information.

What steps are then taken to make sure that the attacks are not successful and then security mechanisms are actually put into place? I would have felt more comfortable—you spoke about intrusion detection devices and other beefing up, fire walls and things of that nature.

Mr. HENDER. Clearly, the members of FSSCC spend billions and billions of dollars building just those things that you have mentioned to prevent the attacks.

As we all know, these attacks are becoming more sophisticated every day, and the things that they have in place, which maybe were adequate a year ago or 6 months ago, we now know are not. So they are continuously spending money to make sure that those fire walls and other protection devices are in place to stop an attack.

When those protection things fail, it is very important to get that information out so it does not spread.

Mr. LANGEVIN. Secretary Garcia, let me turn to you on another topic. The White House has announced a few weeks ago a new initiative called the Cyber Initiative. It has been said that the Cyber Initiative will be a multi-year, multi-billion-dollar operation which will help protect government and private communication networks from cyber attacks. I have also heard that the DNI will be coordinating this effort with over 2,000 people from DHS, NSA and other Federal agencies.

It is extremely disconcerting, however, that everything that I have heard about this new initiative has come from newspaper articles, despite repeated requests for a briefing from DHS. Why won't the Department brief this committee on the Cyber Initiative?

Mr. GARCIA. Mr. Chairman, thank you very much.

First of all, we take very seriously our commitment to inform and engage the Congress on matters as important as cybersecurity. And along those lines, we are glad that we have had the opportunity to brief members of the committee on more than one occasion on the classified threats that we are facing as a Nation, and particularly as a Federal Government.

So the question becomes, then, what do we actually do about it? And this is—in fact, many of the issues that I have testified to you about we have a number of programs under way in DHS under my Office of Cybersecurity and Communications that are addressing this day after day. And one of the highest priorities that I stated at the outset of my tenure at the Department was to protect Federal networks, which are constantly under attack, cyber attack, on a day-to-day basis. So that has been well-stated as one of my highest priorities.

In terms of making that a comprehensive, holistic Government program that involves all members of the Federal Government on an interagency basis, it is a complex plan in process. And we would want to be sure that we have an accurate assessment of the way forward before we brief the Congress on this. The last thing we want to do is give you an incomplete or fragmented strategy.

Mr. LANGEVIN. Well, Secretary Garcia, you know, I just remind you that this is supposed to be a collaborative effort, and both the administration working with the Congress. And when you are talking about the Cyber Initiative, something this massive, involving this many people, with the direct involvement potentially of the NSA, along with billions of dollars that are going to be spent, the lack of being forthcoming and engaging in a full disclosure with the Congress, particularly with this committee, subcommittee, it is very upsetting, it is disconcerting, and I am not happy. I am not satisfied with that answer.

Now, according to an article in the Baltimore Sun, the Cyber Initiative calls for NSA to work with DHS and other Federal agencies to monitor critical infrastructure networks to prevent unauthorized intrusions. One presumes this would mean the monitoring of both Federal and privately owned critical infrastructure networks.

If this is true, what impact will this have, this initiative have, on the cybersecurity elements of the sector-specific plans? And beyond that, what impact will this have on the public-private partnership that DHS has been developing?

Mr. GARCIA. Sir, certainly I wouldn't want to comment on an article that is speculative before we really finalize our plans. But we certainly look forward to briefing the committee at the appropriate time when we have finalized our plans.

But let me tell you that everything that we have been doing over the past year and a half or 2 years has been focused on this public-private partnership, and that needs to continue. My emphasis, absent the public-private partnership, is in strengthening our Federal networks. And that really is one of the highest priorities. And that is what we are focusing on here for the purposes of this hearing. The NIPP and the sector-specific plan process is one that we are committed to, year after year, as we involve the private sector in our efforts.

Mr. LANGEVIN. Mr. Secretary, I certainly look forward to getting that briefing on the Cyber Initiative at the earliest possible opportunity.

With that, the Chair now recognizes the ranking member of the subcommittee, Mr. McCaul, for 5 minutes.

Mr. MCCAUL. I thank the Chair.

And I would also like to raise the issue—we have had several hearings on cybersecurity. And, Secretary Garcia, you have participated in many of those.

And it is my assumption that this plan that DHS is working on with the administration, you are in the process of developing that plan at this point in time? Is that correct?

Mr. GARCIA. That is correct, sir. It is an interagency process.

Mr. MCCAUL. Right. When do you anticipate that the plan will be fully developed so that you will be in a position to brief Members of Congress?

Mr. GARCIA. Sir, I wouldn't want to commit to a time at this point. We are still in the planning stages.

Mr. MCCAUL. Okay. Certainly, if it hasn't been finalized, I can see why it is an ongoing process at this point. But I would ask, as well as to echo the Chairman's remarks, that, to the extent when you are ready to share and coordinate with us on that, we certainly would like to know what the plan is.

In addition, the commission that was formed as of yesterday I am sure will be very interested in working with you on that, as well.

Mr. GARCIA. Sir, let me just say I appreciate and commend you and Chairman Langevin for the appointment of that commission. I think this really shows proactive thinking about an ongoing attention that needs to be paid to cybersecurity and what is working, where are the gaps, what do we need to be doing, going forward.

Mr. MCCAUL. And I thank you for saying that. I think as the Chairman mentioned yesterday, we see it as a forward-looking vehicle, not a "gotcha" exercise. It is a policy exercise, looking forward, what can we do to better protect our systems. And I think you will find it should be a very friendly, not hostile, relationship with the Department of Homeland Security and the administration.

Having said that, I think as you mentioned, Secretary, the 12 of 17, as I look at the report card, is actually some good news, that we have plans that are satisfactory. There are a few that are not.

And, Mr. Powner, I want to ask you about some of those, specifically the financial sector, which has some concern. If the financial networks were hacked into and the numbers were moved on the ledger, you can imagine the economic chaos that would cause. And we know that, whether they are criminal enterprises wanting to steal or whether it would be terrorists that would like to cause economic devastation in this country, you can imagine the consequences. So this particular sector is of some concern.

Mr. Hender has raised the issue that your review is not as thorough as it should have been on the financial sector, and I want to get your response on that. He specifically said you did not consult with Treasury on your analysis. Can you comment on that?

Mr. POWNER. Yes, a couple comments.

First of all, I would like to start by saying, do we think, based on our years of work looking at cyber critical infrastructure, that the banking and finance sector is one of the mature sectors? We do. Okay.

When we did our analysis, we were surprised, okay. The way we go about our analysis, I have a team that has actually looked at this for many years, and we had multiple folks where they inde-

pendently came up with the same assessment. Okay. So we stand by our assessment. I think Secretary Garcia mentioned that our assessment overall was consistent with his assessment. So I think there is a disagreement not with just GAO but perhaps with the DHS.

Now, going forward, I am more than willing to sit down with Mr. Hender. We have talked about this, and we will talk about the differences here. I think the larger question here is this—not to go over checkmarks in this category or this category when you look at 30—is, what is the value of the plans? Okay. Some mature sectors—and it wasn't the banking and finance sector, but in other work we have done, the water sector, for instance, has mentioned, we are beyond the planning phase; these plans are not that helpful for us. And my only question is whether that is similar with the banking and finance sector.

Mr. MCCAUL. Are you questioning the necessity for the plans or the——

Mr. POWNER. Well, I think as you heard from the two witnesses here, there is a lot going on, on an individual company basis. And when you look at the whole sector approach, we have been trying to do this well prior to the, you know, 9/11, the Homeland Security Act. This goes back to a Presidential directive in 1998. Okay.

So we are almost 10 years into this, and many would argue that we haven't made much progress. We are still in the planning and assessing phase, and we ought to be into the protecting and putting in place robust recovery plans.

So I am not saying that the plans necessarily aren't useful, because they could be useful. It is a question of whether we complete them and effectively implement them going forward.

Mr. MCCAUL. Just to follow up to that, what more needs to be done to the financial sector to put it in the passing category? I am of the view that mandates and regulatory actions should be a last resort, that we should allow the private sector to work with the public to work this out. What more, in your opinion, needs to be done?

Mr. POWNER. Well, in order to get their plan more comprehensive, I think there are probably only six or seven criteria that they could easily bump their plan up and they would be one of the most comprehensive. So it is matter of just making the plan complete at this point. And do we have confidence that will occur? Yes.

And we are more than willing to sit down with Mr. Hender, too, to make sure we didn't miss anything. But, once again, we stand by our analysis.

Mr. MCCAUL. Last question. My time has expired, but I would like to ask Mr. Hender, how vulnerable, in your opinion, is the financial sector to a cyber attack?

Mr. HENDER. Well, I would never sit here and tell you that a cyber attack could not happen against our sector, but I don't want to leave the impression with this committee that we are still in the planning phase in terms of cyber.

I think if the GAO had looked at our full plan and the appendices that were attached to that plan, and if they would have understood that we are way beyond the planning stage—we are a highly regulated industry. And back in 2006, there was an analysis

done by the Federal Reserve, the Office of the Comptroller of the Currency, and the SEC to see what progress our sector had made not only in physical but also in cyber. And I will tell you, I would like to submit for the record the results of their findings, because I think you will find, if you read that report, we are way beyond the planning stage. We have done an enormous amount of work to protect this sector, so that if it is a cyber attack or a physical attack, we are in as good of shape as we think we can be. That is not to say you can't be better, but we work at it every single day to try and get better.

Mr. MCCAUL. And what is the name of the report you mentioned again?

Mr. HENDER. The name of the report is the "Joint Report on Efforts of the Private Sector to Implement the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," and is dated April 2006.

Mr. MCCAUL. Mr. Chairman, I would respectfully request that report be entered into the record.

Mr. MCCAUL. I see my time has expired. Thank you.

Mr. LANGEVIN. The Chair now recognizes the gentleman from New Jersey, Mr. Pascrell, for 5 minutes.

Mr. PASCRELL. Did I hear you right, Mr. Hender, that the GAO did not take into account the appendix of the report?

Mr. HENDER. That is my impression. I don't know that for a fact. Because if you look at the appendix, it really answers the questions where they found fault with our sector.

Mr. PASCRELL. Mr. Powner, did you take into account the appendix?

Mr. POWNER. I would have to go back and revisit the full plan. A lot of these plans are quite comprehensive. Was there an appendix, or the one that Mr. Hender was referring to? I would have to look at that.

Mr. PASCRELL. When you are looking at the chart, you are looking at the chart that you presented to us, the five areas that need, really, some improvement and are still perhaps in the planning stage, as you go back before 9/11, this process started, correct, Mr. Powner?

Mr. POWNER. That is correct.

Mr. PASCRELL. We are talking about banking and finance, defense industrial base, national monuments, agriculture, food and commercial facilities are the worst. Aren't they?

Mr. POWNER. Correct.

Mr. PASCRELL. Why is agriculture and food the worst, one of the worst? Specifically?

Mr. POWNER. Specifically? I could go through in detail, you know, those areas.

Mr. PASCRELL. I read your testimony.

Mr. POWNER. Right.

Mr. PASCRELL. But you know that off the top of your head. What stands out? Is there any one thing that stands out?

Mr. POWNER. I would have to get back to you on that. I mean, we have details here in an appendix for each of the 30 criteria that we looked at, but clearly when you look at that, with as many cat-

egories that were not fully satisfied, there are eight overall categories, you know, do you have——

Mr. PASCRELL. Right.

Mr. POWNER. —do you have a methodology to assess your assets? Do you have a methodology to perform your risk assessments? There be would be weaknesses in all those. Are there appropriate methodologies for recovery plans?

Mr. PASCRELL. Might not the biggest problem be here, to go back to something stated earlier, that we do not have a national risk assessment? What is the relationship between that, Mr. Powner, and the results which you have come up with, in your estimation?

Mr. POWNER. A national cyber risk assessment?

Mr. PASCRELL. Right.

Mr. POWNER. Well, one of the things that is clear is we have never had a national cyber threat assessment. Okay. So we have not had that.

Mr. PASCRELL. Ten years into the plan, and we don't have a risk assessment.

Mr. POWNER. Correct.

Mr. PASCRELL. All right.

Let me ask Mr. Hender this question. Nothing changes under the sun. How are you verifying what companies are doing with the information you provide? How do you know what they are doing with it?

You are not just sending information, you are not just sending out an advisory. This is serious business, as you well know better than I do. So what are you doing with the information? What are the companies doing with the information you give them?

Mr. HENDER. Well, I have talked to the companies. And depending upon the threat level, the company either has a problem or doesn't have a problem.

Mr. PASCRELL. Do we have a list of what is done? Do we have a report to present to this committee as to what these companies are doing with the information that is provided?

Mr. HENDER. I think if you look at the report that I referred to earlier——

Mr. PASCRELL. Right.

Mr. HENDER. ——that report is very comprehensive. And it also deals with the companies that make up the sector. And I think the agencies that regulate them—I mean, we are highly regulated. These regulatory agencies——

Mr. PASCRELL. You are highly regulated about—what things are you talking about?

Mr. HENDER. We are highly regulated by a number of things, but cyber is one of the things that we are regulated by.

Mr. PASCRELL. And how are you regulated?

Mr. HENDER. We are regulated by examination. And, in fact, in some of the large companies, the regulators sit right in the offices to make sure that the things that you are worried about don't happen.

Mr. PASCRELL. So you think the assessment that was made by GAO is just a result of them not reading all the information that should be available and is available to them? If they read that information, they are going to change their assessment, they are

going to change the report. They are going to send back a report to this committee and say, "Oh, we missed three or four different things, and we really want to change the banking and financial assessment to comprehensive. We don't think they are somewhat comprehensive; they are comprehensive."

Is that what you want us to believe?

Mr. HENDER. I truly believe that. And I think our sector coordinating agency, the United States Treasury, truly believes that. I believe that we are one of the most mature sectors that are out there. We take this very seriously.

Mr. PASCRELL. No one is saying that you are not taking it seriously. You have been on this for 10 years.

Mr. HENDER. And we—

Mr. PASCRELL. Excuse me. You have been on this for 10 years, and I am not convinced, in what I have read and what I have heard today—I am asking you to convince me. You haven't so far; you might. I am asking you to convince me that there have been tangible actions on your part, not you personally, but in that sector, that would indicate that we have come a long way. I don't feel that. What am I missing?

Mr. HENDER. Maybe I am just not a good communicator.

Mr. PASCRELL. No, I don't think that is the case at all. You have to have something to communicate.

Mr. HENDER. I think the amount of money that the firms have spent since 9/11 in making our sector more robust and able to deal not only with the physical threats but the cyber threats are very, very impressive. As I said, they take this very seriously. Our regulators take it very seriously.

And I think that I would be surprised if the GAO, when we have our conversation and point to them the real efforts—not plans, but the real things that we have in place to protect this sector—would not change their opinion. I would be very surprised.

Mr. PASCRELL. Well, in conclusion, Mr. Chairman, we are 10 years into this, with this particular sector, and there is a very serious statement that Mr. Hender has made, that we respectfully disagree with the GAO's analysis.

Those are your words, Mr. Hender. And I respect those words. Don't get me wrong. I am more inclined, at this point—not you personally—I am more inclined to believe GAO, because they have a different part of this. They are involved in a very different part of this than you may be or I may be.

And I would hope that you will prove to them that they are wrong and so that this committee will get the report back, and maybe I will change my mind, or maybe some of the other committee members who feel like I do will change their mind.

But going back to what Mr. Powner said, we need a national risk assessment plan. And we cannot be honest with the American people about how safe they are unless we have that plan.

And that plan is overdue, is it not, Mr. Powner?

Mr. POWNER. Yes, it is.

Mr. PASCRELL. Thank you, Mr. Chairman. I appreciate your giving me those courtesies.

Mr. LANGEVIN. I appreciate the gentleman's line of questioning. His point is well-taken, and the Chair certainly agrees.

With that, the Chair now recognizes the gentleman from California, Mr. Lungren, for 5 minutes.

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

Let me ask both Mr. Hickey and Mr. Hender this. It seems to me that the nature of your industries are such that the cyber world is an essential part of it, an obvious, central part of it. It is part of what you do. It is part of what you are. It is part of how you provide your services. As opposed to some other sectors where cyber is important, extremely important, but it is not so transparent to the user that if you were to charge them for protecting the cyber aspect of their business the user would say, "Well, I understand that," in your industry it seems to me to be far more obvious.

So I would ask you this, in both cases. How do your respective industries view cyber protection as a part of the cost of doing business, such that your members can justify to your shareholders the bottom line? Because I happen to think that that is one of the most important things we are going to have to do in the private arena. And it would seem to me it would be more obvious in both of your cases to begin with. So I would say these may be the easy cases.

But can you give me an idea of how the companies that make up your organizations view that as part of cost of doing business and, therefore, part of the cost of being active competitors?

Mr. HICKEY. I think when you take a look at today's marketplace, our customers—which are enterprise customers, Government customers, and consumers—are demanding that companies like Verizon put in place safeguards to protect their business and their livelihoods within our organization. So the market is demanding that companies like Verizon invest, and invest very heavily, in technologies that will safeguard not just our physical assets and certainly our human assets but, very importantly, our cybersecurity assets.

Mr. LUNGREN. Let me ask you this, then. You can look at a whole array of potential attacks. They could be hackers. They could be mischievous college students. They could be the bad guys who want to be able to get into your company and therefore extract some economic benefit on their part or to harm you so that someone else is benefitted. Those, it seems to me, are, in terms of possibilities, greater than a terrorist attack, which has greater consequence but the likelihood is far less.

How do you calculate that such that you make a judgment to either insulate your operation from a cyber attack by a terrorist organization, transnational or national, or to create redundancies in the event that they are successful with an attack?

Mr. HICKEY. I think if we continue to focus on the blocking and tackling of cybersecurity practice, given the environment, given the fact that we are looking at an all-hazards environment, that we will continue to invest as necessary in the technology and the expertise to help secure the interests of our customers.

Verizon in 2006 invested over $17 billion in infrastructure buildout. And we are doing that certainly with an eye to our customer and our future customer base. And vendors that do business with Verizon know very clearly what our priorities are, in terms of the

technologies that we require to make our network more secure going forward.

So, again, going back to the marketplace, we are mindful of our customers' needs; our vendors are mindful of our needs as a major carrier. And companies like Verizon continue to invest very aggressively to make sure that we are addressing all hazards within the cybersecurity realm.

Mr. LUNGREN. I would say parenthetically, if Verizon were one of those companies that we asked to assist us after 9/11 on our efforts on foreign intelligence that we are now refusing to give immunity, it is kind of tough for us to tell you to trust us as we go forward. Hopefully, we will address that.

Let me ask both of you—and I know I asked both questions to you as well, Mr. Hender, but I am limited in time. Do you have, in the private sector, among the companies that would receive information that would be of value to them from the Government, do you have or do those companies have their people that have the proper clearances that they could receive that information? And is it at the CIO level? And if a CIO has that information, has that clearance, how does the CIO interact with the CEO if the CEO doesn't have that clearance? And what have we done in terms of recommendations, if any, in your sectors to deal with that?

Mr. HENDER. I think our sector—Specific agency, Treasury, has been very responsive in getting the right people in our sector the necessary clearances that we need and, in addition to that, giving us access to the people in the Federal Government who are charged with collecting the intelligence information and passing that information on to us.

You ask a very important question, though. And that is, what can the person who has the clearance do with that information? Clearly, if there is a life-threatening event that is going on that is classified, that person has an exemption and can pass that information on to anyone to make sure that those lives are not lost. Also, that person, with the permission of the agency, can work and make sure that the appropriate people within that company or within that entity know what is going on to protect that entity.

It has never really been a challenge, to date, where something has come to our attention that has been classified where we have not been able to use that information to protect the sector.

Mr. LUNGREN. Mr. Hickey, you feel the same way?

Mr. HICKEY. Our sector-specific agency is the National Communications System. And just as Mr. Hender said, the NCS has been veryμattentive to the needs of not just my company but others, in making sure we have the right clearances for the right individuals.

I can say that, from a Verizon standpoint, our CEO, Ivan Seidenberg, has just received his top-secret clearance. So, right to the top within our organization. If we, at the ground level, if my team becomes aware of information shared within the NCS or, you know, within the HITRAC organization, within the IP division, we can share that at the very highest levels of the business with the appropriate individuals to make the right decisions, from a response standpoint.

Mr. LUNGREN. Thank you.

Mr. LANGEVIN. I thank the ranking member.

The Chair now recognizes the Chairwoman of the Subcommittee on Transportation Security and Infrastructure Protection for 5 minutes.

Ms. JACKSON LEE. Thank you very much.

And I thank the witnesses.

And I am having trouble with double appointments and hearings that we have responsibility for, but I am delighted that the testimony has contributed to, I think, a very important discussion.

I am going to start on this debate that is going on with the initial offering to work with the private sector. Again, the private sector holds 85µpercent of the infrastructure. And, certainly, cybersecurity being a seamless part of that, there is a dialogue going on about the question of the voluntary cooperation, which I made mention of in my opening remarks, or a regulatory framework.

So I would like to ask Mr. Hender, based upon your experience—let me pose the question first to Mr. Powner, and then, Mr. Hender, you might want to comment.

But based upon your experience in critical infrastructure work, protection work, do you think the Department of Homeland Security should continue to work with the private sector, or providing the private sector with an adequate value proposition to encourage it to effectively protect critical infrastructure?

In essence, are we giving them enough of a carrot to do it voluntarily, or should there be some form of a regulatory framework in this partnership?

Mr. Powner?

Mr. POWNER. I think when you look at what was envisioned in national policy going back pre-HSPD–7, one of the things that the Federal Government needs to do a better job—and Assistant Secretary Garcia and I have talked about this—if there were more products, analytical products coming out of the US–CERT, more information on national threat information that was of value to the critical infrastructure owners, I think that would improve the partnership. Okay.

So in order to have an effective partnership, you have to be offering something that these sectors want. Okay. Historically, when you look at where it has really worked, I think there were times when we provided grants to the water sector to do vulnerability assessments. That opened up the communications, okay, because the Government was paying for certain vulnerability assessments, so they were more inclined to open the discussion.

I think there are pockets of sectors, due to the maturity of them working in regulated environments, that are more mature and have worked more effectively together, like the banking and finance sector.

So I think regulation should be considered if we don't make more progress. But there is also—if you stay the course with the NIPP and the sector plans, the Federal Government needs to offer more and provide more of a service to the infrastructure owners.

Ms. JACKSON LEE. And that is service in what form?

Mr. POWNER. The service—the things that the Government controls more, when you look at the roles and responsibilities of the NCSD under Assistant Secretary Garcia, is threat information and it is analytical products on vulnerabilities and incidents. Okay.

We have a US–CERT that we continue to attempt to build out capability with the vision that we are going to have more robust analytical products that we can provide to these infrastructure owners. As an example, if you go to DOD or some parts of the intelligence community, you will see some fairly robust analysis and warning capability, when it comes to cyber. Okay?

So there are pockets in the Federal Government where we have this. All right? What we need to do is we need to build that out and transfer that information to the infrastructure owners. That would help with the partnership.

Ms. JACKSON LEE. And the pockets in the Federal Government are just scattered, or there is some order to them?

Mr. POWNER. I think there is order, but it depends on where it is at. If you look at DOD and some of their capabilities in this area, some of it is fairly robust.

Ms. JACKSON LEE. We need to harness it. We need to get some sort of organized way of connecting.

Mr. POWNER. Absolutely. If you look at HSPD–7 and if you go back to analysis and warning pre-DHS, we had this capability, and we were building it within the FBI. There was something there called the National Infrastructure Protection Center. With the creation of DHS, we moved it from the FBI and it now became the US–CERT.

So, clearly, we have had some starts and stops. We have progressed forward; we have taken some steps backward. But if we really want to build out that capability, that is one way to build a more effective partnership, if you offer more on the Government side that was of value to these sector owners.

Ms. JACKSON LEE. Let me, Mr. Hender——

Mr. HENDER. It is very clear that, unless there is a partnership between the private sector and the public sector, the things that we have discussed today are never going to be solved. I think a good example and a model is to look at the partnership that we have with Treasury. It is so critical to have information that flows both ways.

And if I could make a recommendation, I would think it would work very well and be very important to take people from the private sectors, just not our sector but all the sectors, and house them in some form or fashion within CERT or some other intelligence organizations, so, as this information comes in, it can be analyzed, not only by the Government, but you have the private sector sitting there and saying, "This is important information. This is a threat. This is what this means, this information." Unless you have that partnership and unless you have those people sitting there working together, a lot of information that maybe flows into these intelligence organizations, I think we are missing a golden opportunity. And I think we are missing it.

Ms. JACKSON LEE. We are missing it.

Mr. GARCIA—MR. Chairman, if I can, I just have a couple of quick questions, probably not quick on the answers.

Secretary Garcia, let me thank you for your service. This is a tough business that we are in. And I think there are some tough concerns that we have as members.

You know that I expressed my concern about the national annual report regarding the status of critical infrastructure protection nationally and within each of the sectors. The report is due on Novemberμ5th. And my question is, is it ready? Is it something that we can expect? And you might want to acknowledge whether this is still the case, that we will have a full report.

And I have another question for you that I would like to just offer so that you can answer it. The incident at the Idaho laboratory provided you with an opportunity to showcase how effectively you can reach out to the private sector with best practices. My concern, though, is how you verify the implementation of these advisories. And I think this was mentioned by one of the witnesses.

How do we have a two-way street? How are you measuring such implementation? And into what obstacles are you running, so that the private sector can become vested in what you do?

Mr. GARCIA. Absolutely. Thank you, Madam Chairwoman.

On the first point, I believe we are on track for delivering that report to you.

And on the second issue, you are correct that one of the most important things for us to achieve over time is the ability to measure progress. Where DHS is not empowered to compel reporting back from the private sector on the extent to which they have implemented best practices or other——

Ms. JACKSON LEE. DHS is not compelled to report back to the private sector?

Mr. GARCIA. No, to the extent that DHS cannot compel the private sector to report back to DHS.

Ms. JACKSON LEE. To report back. So there is a lack of either oversight or regulatory structure.

Mr. GARCIA. Right. And for those sector coordinating councils that we have worked with, for example, they, in turn, are not necessarily empowered to demand from their member companies that they report back to them. So, much of this is, in fact, voluntary.

I would point out, I think the fact that, through this whole NIPP process and the sector-specific plan process, the fact that there are 17 critical sectors that have come to the table with DHS and other sector-specific agencies without actually being compelled to do so is, I think, in fact, a testament to the importance that the entire private sector, sector-specific agencies give to this issue of the joint public-private partnership.

Ms. JACKSON LEE. Quickly, Mr. Hickey, has the DHS given enough incentives to the business community to do what Mr. Garcia says is missing, which is to come back and report back on best practices? Apparently, there is a schism there, in terms of being able to do this in a voluntary manner.

Mr. HICKEY. I would respond to that by saying that there are a great number of forums that companies like Verizon participate in, from the National Security Telecom Advisory Committee to the President, where you have 30 companies coming together from a full array of sector participants, that come together regularly to develop plans and policy and recommendations to the President on global infrastructure resiliency, on network security, on GPS issues, on a full array of issues where we feel an obligation to bring

our subject-matter expertise to the table to work with Government and support Government initiatives.

The NSIE, the National Security Information Exchange, where Government and industry come together, again, it is voluntarily, but willingly, to share best practice around cybersecurity and other security practice.

My sense is that companies like Verizon are there because we feel an obligation to Government and to the country to participate not only in planning but in operationalizing security practice to protect the country's best interests. So we are there willingly.

I think, from an incentive standpoint, the issue of real-time sharing of threat intelligence is very important. And that is helpful for companies like Verizon, to have a good, accurate source of timely information regarding threats, cybersecurity and otherwise, that we can then internalize and deal with from an operational standpoint.

Within Assistant Secretary Garcia's organization, he has made, I think, a positive move toward bringing together, even more closely, the information-technology sector and the communications sector by collocating our NCC ISAC, our National Coordinating Center for Telecommunications ISAC, with the IT ISAC and with the US–CERT. That brings us closer together, physically, day in and day out. We can address, as things evolve, operational issues much more quickly on a day-to-day basis.

So threat intelligence would be a major incentive, but I think there is a real willingness there to assist our Government partners. And we are, I think, continuing to move in the right direction.

Ms. JACKSON LEE. Thank you. I think we have a lot of work that we can look at that you have done that we need to do. Thank you.

Mr. LANGEVIN. I thank the gentlelady.

There is a vote on right now, but we will go to Ms. Clarke for the final question before we dismiss this panel. Ms. Clarke is recognized for 5 minutes.

Ms. CLARKE. Thank you very much, Mr. Chair.

This question is to Mr. Powner.

You just suggested to Chair Jackson Lee that the Federal Government could assist these sectors to ensure greater consistency through partnership, if you will. Clearly, there is a lack of consistency in the quality of the various sector-specific plans.

Do you feel that DHS is doing enough to work with each respective set of public-private stakeholders to ensure greater consistency? And have your offices recommended or determined a good way for them to do this?

Mr. POWNER. Well, clearly, Assistant Secretary Garcia had mentioned his office and the interaction they had with various sectors in putting those plans together.

I think what is important is, when you look at this next annual report that is due out, the annual report should be providing some assurance, Madam Chairwoman, that you mentioned, that, one, the plans are now complete and, two, that we are actually moving down the road toward implementation.

Ms. CLARKE. Mr. Garcia, Assistant Secretary Garcia, good to see you again.

In response to Representative Pascrell's questioning, Mr. Powner said that there needs to be a national risk assessment for cybersecurity. Five months ago, the Department stood up the Risk Management and Analysis Division. Have you engaged with that office to date?

Mr. GARCIA. That is part of the National Protection and Programs Directorate, to which my office belongs as well. CS&C is part of that, as well as the Risk Management Analysis Office. So, yes, we interact regularly.

The national risk assessment that we are focusing on is, in fact, the National Infrastructure Protection Plan, the sector-specific plans that go with it. And I think, as we implement these plans, as Mr. Powner says, we are going to have a national risk assessment with metrics in place that we can measure how well we are doing.

I would emphasize that it is important to note that this is the first time we have done this, that 17 sectors, industry sectors, have organized themselves around a common mission, and then to organize themselves to interact with the Government in a collaborative process, a framework by which we are going to measure the vulnerability, assess the vulnerability of our infrastructure nationwide, and then take the steps to actually mitigate those vulnerabilities and strengthen our infrastructure.

So I think we have come a long way in just a year-and-a-half worth of time. And the fact that most of these sector-specific plans were written around the middle of last year, there has been a tremendous amount of effort and resources put into infrastructure protection since then in the cyber area.

Ms. CLARKE. Assistant Secretary, I recognize that, you know, this is a major, major undertaking, and some would say just putting together the Department of Homeland Security has been a major, major undertaking.

The concern is that there be some sort of a driving force that puts some, you know, some energy behind getting this done in a timely fashion, and that we are not sort of leaving it up to inertia to get us there.

You know, with each passing day, people are concerned that we have, you know, the critical infrastructure, particularly with respect to cybersecurity, in place. Because it seems like there is a generation of intelligentsia out there that just lives to get ahead of us, with respect to cyberspace.

So I hope that you will certainly recognize the urgency from which you hear this committee speaking, because we certainly believe time is of the essence but, at the same time, understand that haste can make waste. So we hope you will take that under advisement.

And this question is—really, my final question is to anyone on the panel. Although there are many differences between each sector represented in the NIPP and there is merit to the idea that each area tailor its own plan, when it comes to cybersecurity, many of these sectors deal with some of the same problems. For example, organizations of every sector have to deal with the possibility of data theft or that systems can be brought down. Therefore, if planners in one sector figure out a useful solution that can apply to

other sectors, it would be useful if this information were disseminated.

Is there any information-sharing occurring between the coordinating councils for each sector? And is this a role that DHS plays or could play?

Mr. GARCIA. Absolutely, Congresswoman. Thanks very much for that question.

We, last May, set up—my office set up the Cross-Sector Cybersecurity Working Group. And it is composed now of experts in cybersecurity from all of the 17 sectors. And we meet at least monthly and, I think, more frequently on conference call. And this is the forum precisely for those various sectors to share their experiences in cybersecurity and see where there are dependencies on one another in their cyber infrastructure and interdependencies, and see where are there are common problems across all of them.

Control systems, a subject that this committee held a hearing on on Octoberμ17th, is a prime example, where there is a nexus between cybersecurity and physical security. That the process control systems that enable us to purify water, manufacture chemicals, to run the electric grid, all of these digital control systems have a nexus to information networks or communications networks.

And so, the fact that these sector representatives are coming together on a regular basis to share those concerns, identify common vulnerabilities, this is taking us a long way down the track of doing that national risk assessment that we are heading toward.

And I think this is a perfect example of how the sector-specific plans, the NIPP process, is working.

Ms. CLARKE. You want to say anything?

Mr. HICKEY. I would just like to comment that the Communications Sector Coordinating Council and the IT Sector Coordinating Council work very closely together, day in and day out. We have cross-membership. We work together in a number of forums. Actually, the chair of the IT Sector Council is in today's audience. So there is a very close relationship.

As was pointed out earlier by one of your colleagues, it is hard to distinguish where pure providers end and information service providers start. Companies like Verizon and other companies, large and small, are aware of the fact that, with convergence of technologies, cybersecurity has to remain a real focus. And I can assure you that, both within the IT sector and com sector, we work very, very closely together.

Mr. HENDER. I would just like to comment that we just finished a 3-week pandemic exercise. Part of the component of that exercise was cyber, because if the Internet is not there, then the work-at-home programs that the firms have put together are going to be useless.

It is our intention to make those findings public in 2008, early in 2008, not only to our sector, but to all the sectors in this country and to the international countries that are interested in learning the experiences we had during this pandemic exercise.

Ms. CLARKE. Thank you.

Thank you very much, Mr. Chairman.

Mr. LANGEVIN. I thank the gentlelady.

And I thank the witnesses for their testimony.

There is one last thing I am going to pose. Unfortunately, we don't have time for the answer since there is a vote on right now. We have about 2 minutes.

But, you know, when we talk about the risk assessment—Secretary Garcia, I would ask you to respond to this in writing. And, Mr. Powner, if you would comment.

You know, a risk assessment is composed of threat and vulnerability and consequence. You know, how will the national report be a risk assessment, when it is lacking these critical issues?

So I pose that to you. And we will have some other questions that we would like you to respond to in writing.

Again, I thank the witnesses for their valuable testimony, the members for their questions.

The members of the subcommittee, as I mentioned, may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to those questions.

At this time, the first panel of witnesses is dismissed.

And the Chair now recesses for what will be one vote, and we will reconvene in approximately 15 minutes.

Thank you.

[Recess.]

Mr. LANGEVIN. The committee will come to order. As we call up the second panel of witnesses, I want to thank the panel for your patience and willingness to stick around. We do appreciate it, and I know you have valuable testimony to offer. Unfortunately, Mr. O'Hanlon was not able to stick around. He was going to be on this panel as the lead-off. Mr. O'Hanlon specializes in U.S. national security policy and is the co-author of a book called Protecting the Homeland 2006, 2007, and he would have been discussing one of his articles in that book. But he has submitted a statement for the record, and we will certainly forward look forward to reviewing that and hearing from Mr. O'Hanlon on a later date. In the meantime, of course, we are very grateful for the rest of our panel being here.

Our first witness will be Ms. Sally Katzen, faculty member of the George Mason School of Law and a senior consultant to the Critical Infrastructure Protection Program at George Mason University. We thank you, Ms. Katzen, for being here.

Our next witness is Mr. Larry Clinton, president of the Internet Security Alliance. We are grateful for you being here as well, Mr. Clinton.

And our next witness, the last witness is Dr. Larry Gordon, Ernst & Young Alumni Professor Managerial Accounting Information Assurance at the Robert H. Smith School of Business at the University of Maryland. Dr. Gordon is also an affiliate professor with the University of Maryland Institute for Advanced Computer Studies.

Mr. LANGEVIN. Again, we want to thank you for being here. Without objection, the witnesses' full statements will be inserted into the record. And I now ask each of the witnesses to summarize their statement for 5 minutes, beginning with Ms. Katzen.

And before I turn the floor over to, Ms. Katzen, I understand that it is your anniversary today. Let me take the prerogative as

Chair to wish you a happy anniversary, and thank you for spending your anniversary with us today.

Ms. KATZEN. My husband thanks you as well. Thank you.

Mr. LANGEVIN. I don't know if that was sincere or not. He may question it as well. Thank you.

**STATEMENT OF SALLY KATZEN, GEORGE MASON SCHOOL OF LAW, SENIOR CONSULTANT TO THE CRITICAL INFRASTRUCTURE PROTECTION PROGRAM, GEORGE MASON UNIVERSITY**

Ms. KATZEN. Chairman Langevin, Chairman Jackson Lee, Ranking Members McCaul and Lungren, other distinguished members of the subcommittee. My background and qualifications and the credentials of the George Mason Law School CIPP program are set forth in the written testimony. Given the lateness of the hour, I want to condense my oral comments to the bare essentials.

First point. You have heard it before, but it cannot be overemphasized. One of the problems that we have had with cyber CIPP is that for too long and in too many places, both in the private sector and in government, the task of identifying and addressing cyber CIPP risks has been confined to those in the enterprise that own, operate, maintain the computers, the servers, the networks. In other words, the IT department. But viewing cybersecurity as an IT problem with an IT solution greatly understates the problem and misperceives the solution.

As we explain in the written testimony, even the best technical defenses are no better than the physical security and personnel security elements that must accompany them. And not only are these elements typically outside the direction and control of the IT department, but also they like the IT department typically fall on the operations side of the enterprise which generally is not well represented at the highest levels of corporate accountability and governance.

Based on the extensive work that the CIPP program at GMU has done, we are impressed with what is called the ERM, the Enterprise Risk Management program. The emphasis in ERM is on the enterprise as a whole and raising cyber CIPP issues to the highest corporate level of accountability. And we have got a lot of discussion in our written testimony about how it works and what it does. I hope you like the cowboy graphic.

Second point. Six years and billions of dollars since 9/11, how much progress have we made? Now, the headlines from the GAO study say 12 of the 17 SSPs have comprehensively addressed the 30 cybersecurity criteria. We think that may be an overly rosy summary if you look at the individual cyber criteria, plan by plan and sector by sector.

In the written testimony, we highlight section 6 of the GAO criteria, which speaks to the measures of progress. And in that connection, the representative from GAO in the earlier panel said, well, we are passed the plans. We are now into implementation. Fine. In fact, good. But if you don't have quality metrics to establish benchmarks at the outset and over time, how to you measure this implementation? How do you evaluate the implementation? And we think the verification of that is also essential.

To our mind, the problem is the dearth of data, the absence of valid information. And I have heard from some that the Paperwork Reduction Act is part of the problem. I think it is part of the solution. And this is something that we can get into another time, but I think it is really important to focus on getting good information.

Third point. What should we do to improve the situation? We propose that the government provide incentives for the private sector to do the right thing. To be sure, companies already have lots of incentives in terms of smoother, more efficient operations and in terms of marketplace acceptance. There is the Ernst & Young study which shows the correlation between success in risk management and success on Wall Street. But, again, the GAO report, and again just looking at the plans, Section 3 which says incentives—that is where the bottom fell out. Only three sectors have fully addressed incentivizing vulnerability assessments.

We gave five different carrots for you all to chew on. Carrots are good for your diet. They are part of my diet, if I get dinner tonight. In any event, many of them are actually discussed in Mr. Clinton's testimony, and I am going to defer to him on virtually all of them but I want to make two comments.

I do want to distance myself from his discussion of liability limitations, limitations on liabilities for companies. I disagree with that approach. And, also, the reinsurance program at DHS. I don't think it should be a government-sponsored reinsurance program. I think he hits the nail on the head when he talks about government leading by example and the importance of the government getting its act together.

One of my responsibilities while I was in Federal service at OMB was the Y2K experience. Now, that is a very different order of magnitude from what we are talking about now. But if you think about the Y2K adventure as a mini pilot of how the government can face these problems and work within, we had no additional command and control authorities, we had no regulatory authorities. We were nonetheless able to work collegially with the groups. We were able, with the various sectors, to share best practices, to work through the problems that had to be done on a cooperative basis, and to use trusted established relationships that already exist between members of the private sector and their State or local regulators or their Federal regulators or their colleagues.

And the problem, in answer to Chairman Jackson Lee's question, what do we do? How do we solve, how do we change this relationship? We do not recommend any additional commands and control authorities. We do not think you should go the regulatory route either with respect to making DHS the SSA for the other sectors or with respect to even the sectors that it has.

But DHS should not be trying to do it alone. DHS should not be dictating to others to "do it my way." Rather, as we experienced in Y2K, DHS should adroitly use its convening powers, take advantage for its opportunities for collaborative work together and collegially work through programs with their partners.

In our written testimony, we give an even more recent example than Y2K. DOE has done this very successfully on a smaller scale.

That is it. Smash the stove pipes, develop metrics, and gather quality data, and have the government help in a noncommand and control regulatory way.

I look forward to any questions you may have. Thank you so much.

Mr. LANGEVIN. Thank you, Ms. Katzen, for your testimony. And we enjoyed hearing what you had to say.

[The statement of Ms. Katzen follows:]

PREPARED STATEMENT OF SALLY KATZEN, ESQ

Chairman Thompson, Subcommittee Chairman Langevin, Ranking Member McCaul, and Distinguished Members of the Subcommittee:

Thank you for providing me the opportunity to testify before you today on a subject that is vitally important to the American people – enhancing and implementing our plans to better protect our Nation's critical infrastructures from computer or cyber-related attacks, as well as other threats, natural or man-made. I am Sally Katzen, and I am here today by virtue of Chairman Thompson's invitation to Daniel D. Polsby, Dean and Professor of Law at the George Mason University School of Law, and Acting Director & Principal Investigator for one of its affiliated centers, the Critical Infrastructure Protection (CIP) Program, to appear before you today.

The CIP Program at the GMU School of Law is unique in that it fully integrates the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the Nation's critical infrastructures. The Program began in 2002 as the result of a grant from the National Institute of Standards and Technology (NIST) at the U. S. Department of Commerce. Since that time, the CIP Program has undertaken a broad range of Critical Infrastructure-related research projects and sponsored many workshops and events through the on-going relationship with NIST. See http://cipp.gmu.edu/history. A key principle of the CIP Program is its outreach to the public sectors (federal, state and local), private industry – including but not limited to the private sector owners and operators of critical infrastructures/key resources (CI/KR) – the academy, and non-governmental organizations. Such inclusive, participatory and diverse "public–private partnerships," as Members of the Subcommittee well know, are essential to better protecting and defending the Nation's CI/KR.

The CIP Program also has conducted research, surveys, studies, and workshops supported by grants and contracts from two other federal agencies; the financial details for these and the NIST grant are provided in the financial disclosure form filed by the CIP Program on my behalf with the Committee. They cover published and non-published research and analysis for the U.S. Department of Homeland Security (DHS) and for the Office of Electricity Delivery and Energy Reliability at the U.S. Department of Energy (OE-DOE). It was through the CIP Program's contract with DHS that I became affiliated with the Program as a senior consultant. For one project under the contract, I led a multidisciplinary team of CIP Program researchers and legal interns from GMU School of Law in an examination of the DHS's authorities in the context of the Homeland Security Act of 2002 (as amended) and other laws. In particular, we looked at the National Infrastructure Protection Plan (NIPP) and Sector Specific Plans (SSPs) that were then in draft form. We studied CI/KR information collection, sharing, use and protection issues, including what is commonly referred to as the "NIPP metrics collection program." More information on this project can be found on the CIP Program website, http://cipp.gmu.edu/projects/NIPPMetricsProj.php.

For the record, I am speaking today as a faculty member of the School of Law and as a senior consultant to the CIP Program. However, the views and opinions expressed are my own and also reflect those of two senior CIP Program research staff members, Mr. Michael Ebert and Dr. Christine Pommerening, who have led or participated in a number of CIP Projects related to the interests of this Subcommittee and the full Committee. In addition to teaching constitutional and administrative law at the School of Law and my work with the CIP Program, my remarks today draw from my career in the federal government during the 1990s.

It is perhaps appropriate to note at this point that during the 1990s, critical infrastructure protection issues became part of the national debate. In 1996, the President signed Executive Order 13010, creating the President's Commission on Critical Infrastructure Protection (PCCIP). In the fall of 1997, the Commission released a report, *Critical Foundations*, which, among other things, identified cybersecurity risks associated with interconnected computer systems, networks, and electronic devices that, in turn, control critical infrastructure assets such as those found in energy, water, dams, nuclear power, and other CI/KR sectors as particularly serious and significant for our Nation. John McCarthy, the CIP Program's Director from 2002 until August

2007, was then serving in the federal government and made major contributions to that report and other CIP initiatives.

From 1993 to 1998, I was Administrator of the Office of Information and Regulatory Affairs (OIRA) at the Office of Management and Budget (OMB), which was tangentially involved in these issues. I then served as Deputy Assistant to the President for Economic Policy and Deputy Director of the National Economic Council, and then as the Deputy Director for Management of OMB until 2001. Among my responsibilities during my federal service that are relevant to my appearance here, I oversaw an interagency process that implemented the Paperwork Reduction Act of 1995 (PRA); was involved in various preparedness activities; and was instrumental in setting up a cooperative, collaborative public–private sector partnership to prevent a less nefarious but potentially serious failure of computer networks and digital control systems known as "Y2K." In many ways, Y2K provides a model for how the federal government, faced with a complicated set of problems that cut across government agencies, state and local governments, multiple industries, and thousands of firms both regulated and unregulated, can use its people, its convening powers, and offers of its considerable resources to successfully address an urgent situation the resolution of which was far bigger than any one institution or corporation. During Y2K, the federal government showed leadership in addressing the vulnerabilities in its own computers, networks, and systems at the same time as it offered help to the private sector. This, in my view, is the kind of positive, effective approach we now must put into action to protect critical infrastructures from malicious cyber attacks.

**Challenges Facing DHS and the other Federal Sector-Specific Agencies**

Although no one seems to know for sure the origin or accuracy of an oft-cited statistic, it is generally believed that the private sector owns and operates roughly 80 percent of the Nation's critical infrastructures, as these assets have been defined by Acts of Congress, Homeland Security Presidential Directive 7 (HSPD-7) and particularly the NIPP. As this Subcommittee heard on October 17th with respect to cyber and physical CIP standards that soon may apply to all owners, operators and users of the bulk electric power system, critical infrastructures are just as likely to be under the ownership and/or control of small and medium sized businesses as large corporations. And one of the challenges now facing the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) is to identify all relevant players – particularly small businesses that have heretofore operated under the radar of NERC – so as to determine those responsible for the reliability and security of our Nation's electric power grid.

Across the 17 CI/KR sectors established by HSPD-7, there is a great variety of business structures, organizations and cultures, practices, regulatory requirements, and standards. Some of the 17 sectors, such as energy or nuclear reactors, have long histories with government regulators at the federal level; typically, these public–private relationships are well established and have produced networks of people and channels of communication. In other sectors, such as chemicals, federal CIP regulation is relatively recent and private–public trust relationships are not yet well formed. In still others, such as commercial facilities, regulation is largely non-existent. To further complicate the matter, enterprises may have lines of business in more than one CI/KR sector. Moreover, some of an enterprise's CI/KR activities may be regulated, others not – and the enterprise may well have several other formal (mandatory) and informal (voluntary) policies, guidelines and standards; these other frameworks may have degrees of nexus to CIP, but also are distinct from it.

DHS has sole Sector-Specific Agency (SSA) responsibilities for ten of the 17 CI/KR sectors. Internally, DHS's Office of Infrastructure Protection (OIP) is responsible for five sectors (chemicals, commercial facilities, dams, emergency services, and nuclear reactors). The Office of Cyber Security and Communication (CS&C) is responsible for two more sectors (communications and information technology); and the Transportation Security Administration (TSA), the U.S. Coast Guard, Immigration & Customs Enforcement, and the Federal Protective Service serve as SSAs for postal and shipping, transportation systems and government facilities. For all seven other CI/KR sectors, Agriculture and Food, Banking and Finance, Defense Industrial Base, Energy, National Monuments and Icons, Public Health and Healthcare, and Water, DHS must rely on other federal SSAs – of which there are eight.

Meanwhile, the states are vital partners in CIP. Traditionally, state (and often local) governments have been at the front line of awareness, preparedness and response when it comes to CI/KR companies within their jurisdictions. Some of these companies are regulated at the state level; others have developed informal but nonetheless effective relationships with state and local officials. Whether such relationships can survive where there are fears of impending federal preemption is an open question.

So, DHS has to coordinate (a) within DHS – itself an amalgam of existing federal pieces and new homeland security requirements; (b) with other federal agencies – some with regulatory authorities, others not; and (c) with state and local agencies – again, some with regulatory authorities, others not. Consider nuclear power reactors. Some of these facilities are owned by the federal government, but most are in the hands of the private sector. DHS is the SSA for this sector, but the Nuclear Regulatory Commission (NRC) has CIP-like operations and safety regulatory reach, and FERC and the states have concurrent or overlapping authorities over other aspects of nuclear power.

For DHS to successfully navigate these waters requires an almost unprecedented level of constructive interplay between and among many federal and state agencies. For the most part, DHS has few authorities to force its federal or state partners or the private sector owner/operators of CI/KR to "do as we say" with regard to cyber and physical CIP. And we are *not* suggesting that DHS be given any new "command and control" authorities in the short term or possibly even the long term. Indeed, we believe that the situation would not be improved either by giving the Department additional SSA responsibilities for the seven other CI/KR sectors or by giving it any additional authorities over private-sector owners or operators of CI/KR. Rather, we believe that DHS should adroitly use its convening powers, take full advantage of its collaborative opportunities, and work collegially through problems with those federal and state agencies that have not only the expertise but also the experience and relationships with their private sector counterparts in the various CI/KR sectors.

Regrettably, the track record to date indicates that DHS has not taken advantage of the remarkable authorities and informal leadership opportunities it already has. Six years and billions of dollars expended after September 11, 2001, where do we stand? Part of the answer to this question is revealed by the title of today's hearing, "Enhancing and Implementing the Cybersecurity Elements of the Sector Specific Plans." In other words, we are still, for the most part, talking about plans. The SSPs were written by SSAs, with critical inputs and expertise from the private sector, and are necessarily only as good as the levels of collaboration and trust that went into them. And how good are they? According to the U.S. Government Accountability Office (GAO) as well as other experts, these plans fall short in many respects, including but not limited to cybersecurity. For that reason, we are here today talking about enhancing plans and then implementing them. We have a long way to go.

**The Special Challenges of Cybersecurity**

Turning to the special challenges of cybersecurity, the most fundamental challenge for better protecting the Nation's CI/KR from cyber attacks is understanding as best we can the full panoply of existing, emerging, and likely future cyber exploits that could be launched against enterprises and systems that are extremely complex, technically diverse, and operate within and across corporate cultures – that cover a vast range of cyber (and physical) security awareness, experience and protection – and within and across sovereign jurisdictions with very uneven laws, regulations, and cyber capabilities. Given this, the Congress, the executive branch, and DHS in particular are to be commended for not embracing a command and control, one-size-fits all approach to cybersecurity. The velocity of technological change, knowledge and progress in information technologies, particularly cyber defenses, is very rapid, perhaps exceeded only by the developmental velocity of cyber threats. For these reasons, policymakers should continue to avoid establishing or otherwise anointing a highly prescriptive set of cybersecurity standards.

Another challenge that may not fully be appreciated is the trend mentioned by some Members and witnesses at the October 17th hearing. That trend, within the corporate world generally and particularly in firms that have CI/KR, is that companies are replacing older, private analogue networks with newer, faster and more efficient networks and intranets. These are based upon IP protocols, whose primary design considerations were *not* security, and the public Internet. In the past, many regulated vertically integrated electric power utilities with CI/KR assets in generation, transmission and distribution used private microwave networks to communicate and control this triad of electricity production and delivery elements. Technological advances, industry restructuring (whether or not driven by wholesale or retail competition laws), and market pressures changed this. Particularly where generation, transmission and distribution were intentionally if not legally "unbundled," the old private networks went away. In many ways, these changes have been beneficial to producers and consumers of electricity, but the move to public networks based upon IP protocols has engendered a host of new cyber-CIP risks. Another manifestation of this trend is that many companies are building seamless intranets and internet sites that intentionally provide access to consumers, commercial partners (upstream and downstream) and investors who are outside the enterprise itself. These seamless systems may also be hooked into hitherto "back office" operations that control and secure a company's critical infrastructures. From a perspective of efficient business integration and exploiting the benefits of technology, this makes sense – but, again, it brings with it a host of new cyber-CIP risks.

Finally, we are presented by the challenge caused by the fact that responsibility for understanding and protecting against cyber-CIP risks – both in the private sector and in government – has too often been confined to those in the enterprise who own, operate and maintain computers, servers, and networks – *i.e.*, the corporate or government IT department. Viewing cybersecurity as "an IT problem" that only can be fixed by a company's IT department greatly understates the problems and seriously misperceives the solutions. Stated another way, stove-piping cybersecurity into IT prevents it from being recognized and treated as part of an enterprise-wide set of cybersecurity risks. Nearly "bulletproof" cyber protection could be assembled by technical experts in IT departments – if sufficient funds are allocated for this purpose. But even if there is funding for bullet-resistant technical cyber, the very best technical defenses are no better than the physical security and personnel security elements which must accompany them. These elements are almost always outside the control and direction of IT, involving, for example, the human resources or the physical security departments of (or often contractors for) the company.

The importance of recognizing and effectively addressing the human aspects of cybersecurity cannot be overemphasized, for well-trained personnel are the first line of defense against threats that are more likely to come from internal sources as from threats outside the enterprise. Clearly, taking effective actions to protect critical infrastructures from cybersecurity risks known and unknown involves more than a company's chief information officer or chief privacy officer or chief security officer – provided the firm is so organized and is of a scale sufficient to afford such "C-level" structures and human expertise.

**Comments on the GAO Report's Findings**

This leads us back, then, to the question of how much progress we have made to date in protecting CI/KR, with particular attention to cybersecurity. The report presented by representatives of GAO in the first panel today provides qualitative and quantitative assessments of the 17 SSPs and how well each of these plans is addressing – or not addressing – 30 cybersecurity criteria. The GAO finds that 12 of the 17 plans have "comprehensively" addressed the 30 criteria. Three plans – Banking & Finance, Defense Industrial Base, and National Monuments – are characterized by the GAO as being only "somewhat comprehensive;" two SSPs – Agriculture and Food and Commercial Facilities – were found by the GAO to be "less comprehensive."

On its face, this does not sound so bad – assuming, of course, that the 30 criteria are methodologically sound measures of cybersecurity. But beneath the GAO's "highlights," a somewhat more troubling picture emerges when one looks at each and every one of the criteria – plan by plan, section by section. According to the GAO's scoring for the eight sections it has broken out in Attachment 2 of its

report, the average (mean) of the number of plans that have "fully addressed" the GAO cyber criteria is as follows:

**Table 1: Average Number of Sector-Specific Plans that "Fully Addressed" GAO Criteria**

| Cyber Criteria Section | Average (Mean) Number of SSPs that "fully addressed" | Lowest Scoring Cyber Criteria in Section |
|---|---|---|
| Section 1:Sector Profile & Goals | 15.0 | N/A |
| Section 2: Identify Assets, Systems, Networks & Functions | 13.0 | N/A |
| Section 3: Assessing Risks | 9.5 | describes incentives to encourage voluntary vulnerability assessments = only 3 SSPs "fully addressed" |
| Section 4: Prioritizing Infrastructure | 11.5 | identifies entity responsible for prioritization of cyber assets = 11 SSPs "fully addressed" |
| Section 5: Developing & Implementing Protective Programs | 11.5 | identifies programs to deter, respond & recover from cyber attacks = 9 SSPs "fully addressed" |
| **Section 6: Measuring Progress** | **9.0** | **includes developing and using cyber metrics to measure progress = only 8 SSPs "fully addressed"** |
| Section 7: Critical Infrastructure Protection R&D | 12.4 | describes process to solicit information on on-going cyber R&D initiatives = 7 SSPs "fully addressed" |
| Section 8: Managing & Coordinating SSA responsibilities | 15.8 | describes process for investment priorities = 14 SSPs "fully addressed" |

We have emphasized Section 6 because being able to measure progress is essential to evaluating results for the time and money spent. Again, analyzing GAO's take for the four cyber criteria in Section 6, we find a mixed message at best:

**Table 2: Examination of GAO's Section 6 Individual Cyber Criteria**

| Section 6 Cyber Criteria | No. of SSPs that "fully addressed" | No. of SSPs that "partially addressed" | No. of SSPs that "did not address" |
|---|---|---|---|
| Ensures that integration of cybersecurity metrics is part of the measurement process | 9 | 3 | 5 |
| Describes how cyber metrics will be reported to DHS | 9 | 6 | 2 |
| Includes developing and using cyber metrics to measure progress, [emphasis added] | 8 | 5 | 4 |
| Describes how to use metrics to guide future cyber projects | 10 | 4 | 3 |

One of the most important criteria in Section 6 – developing and using cyber metrics to measure progress – had one of the lowest indicators of "plan goodness." Only eight SSPs fully addressed this criteria, according to the GAO, while five SSPs were found to have partially addressed it and four SSPs did not address it at all. Given that interdependencies exist among the 17 critical infrastructure sectors, the weakest plans are the weakest links in the chain, again suggesting that serious gaps exist and much work remains to be done.

**Examples of Cyber Attacks and Gaps in Cybersecurity**

Detailed and credible information on cyber incidents that is in the public domain corroborates this charge. This Subcommittee was provided a list of selected case histories of cyber breaches in the electric power sector during the hearing on October 17th. Consider two other incidents outside this sector:

First, it is generally well known that in the Fall of 2006, email servers for the National Defense University (NDU) were completely shut down by a successful external cyber exploit – not just for a few hours or a day, but for several weeks. Faculty, staff, and students had to rely on non-NDU email systems. What is not as well publicized is that the cyber attackers who took down the NDU email system were able to do so because they had successfully hacked into the "dot-mil" architecture.

Second, on February 6, 2007, two coordinated back-to-back cyber attacks were launched against the 13 "root servers." These root servers form the backbone of the Internet; if attackers can compromise, clog or cause to shut down enough of the root servers, all Internet traffic can be affected and – worst case – the backbone could break. In February, six of the 13 root servers were "adversely affected" by "distributed denial of service [DDoS] attacks" that appear to have originated in the Asia–Pacific region. Ironically, a new and proven protective technology developed with US leadership known as "Anycast" was available but had not been deployed on all 13 root servers. ICANN stated that the "two [root servers] worst affected do not have new Anycast technology installed." These two servers were in the United States.

Attached to this testimony as Exhibit A is a CIP Program "Cybersecurity and Liability Workshop White Paper" which references four additional cybersecurity breaches at private sector companies as the result of both external and internal exploits. Again, the facts on the ground indicate that more work needs to be done to protect cyber-CIP.

**Making Sense of the Many Applicable Frameworks and Standards: A Case for an Enterprise Risk Management (ERM) Approach**

When we consider possible solutions, we begin with Congress, which has required specified elements of data and information technology security in a number of laws, such as the Public Company Accounting Reform and Investor Protection Act of 2002, commonly referred to as "Sarbanes–Oxley," the Health Insurance Portability and Accountability Act (HIPAA), and Gramm–Leach Bliley. These and similar laws and the regulations implementing them require that *certain* companies must do *certain* things, and *some* of those required actions involve cybersecurity. The Congress has also imposed specified requirements on federal agencies and federal employees for cybersecurity, data and information sharing, privacy protection and personnel security.

NIST has developed several "Special Publications" (SPs) on computer, information, and cybersecurity. These SPs include 800-53, *Recommended Security Controls for Federal Information Systems (Rev. 1, Dec. 2006*, which is binding on federal agencies). 800-53 was frequently mentioned at the October 17th Subcommittee hearing. The Federal Emergency Management Agency (FEMA) within DHS offers a set of useful concepts and tools that companies may use to advance their own critical infrastructure protection plans and associated voluntary measures such as vulnerability assessments. [See, *e.g.* http://www.training.fema.gov/emiweb/IS/is860.asp.] Other federal agencies may offer other frameworks.

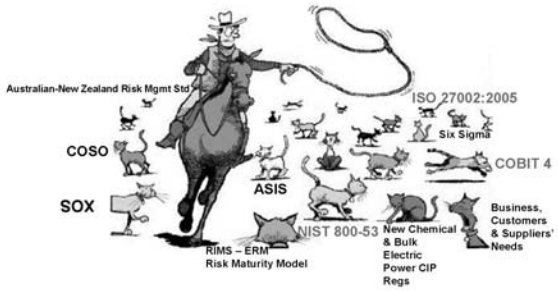
Voluntary frameworks, standards, and tools have also been developed by such respected nongovernmental organizations as the IT Governance Institute [ITGI, co-developers with the International Systems Audit and Control Association (ISACA) of the highly-regarded "COBIT 4.0" framework]; the Committee of Sponsoring Organizations of the Treadway Commission (COSO, which has developed financial reporting, business ethics, internal controls and corporate governance frameworks); ASIS International (an organization that focuses on "Chief Security Officer" issues, including physical and personnel security frameworks); and the International Standards Organization (ISO), which develops

international standards and frameworks that are ostensibly voluntary but often are codified and binding, in whole or in part, by ISO member countries. ISO 27002:2005, for example, establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management. Subsets of ISO 27002:2005 have frameworks for human resource security, asset management, physical and environmental security, and incident management. Other organizations and professional associations have developed training and certification tracks that are grounded in these frameworks and standards.

Earlier this year in support of a DHS project, the CIP Program catalogued selected existing standards, training and certification tracks, and policies and procedures that could be helpful to the SSAs and private sector owner/operators of CI/KR in developing better plans and engendering higher levels of cyber, physical, and personnel security. Fortunately, there is no shortage of excellent and evolving contributions to the field. Multiplicity of security contributors is a good thing in that there are formal and informal competitions to be recognized as a leader in promoting effective levels of security, and to the extent such offerings are generally in the public domain, learning and knowledge developed by one organization can stimulate progress in others. The downside to this wealth of cyber-related guidance, standards, and education and training resources is that it makes it harder for companies to be aware of the many offerings, know how to choose among them, and, most importantly, to properly integrate them to improve cybersecurity.

The CIP Program is convinced that the key to this dilemma is integrating standards into Enterprise Risk Management (ERM) principles and techniques, represented in the picture below as the "Cowboy in the White Hat."

Using Enterprise Risk Management (ERM)
to Integrate Frameworks & Standards



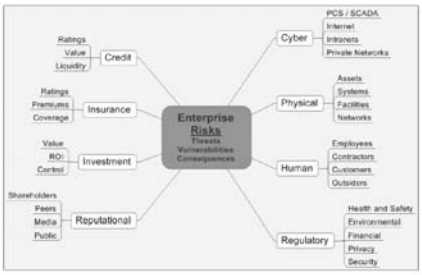

Adapted by the CIP Program from an original © Risk & Insurance Management Society (RIMS), 2006-2007. RIMM, ASIS, Six Sigma, ISO 27002:2005, COBIT, COSO *,et al* are trade- service- marks of their respective organizations.

**ERM in a Nutshell: Core Principles and Processes**

Based upon a review of the literature, the CIP Program developed the following definition of ERM:

> *ERM is the systematic application of strategic and operational management policies, procedures and practices aimed at identifying, analyzing, evaluating, treating and monitoring all risks to the business processes of an enterprise.*

The emphasis is on the enterprise as a whole. There is wide-spread acknowledgment that there are vulnerabilities – in turn, risks – of interdependencies among the 17 CI/KR sectors and within each of the sectors. Equally important but often not fully appreciated, especially when the discussion of risk is artificially confined to cyber-CIP and the IT department, is that corporations themselves have many risk interdependencies. Consider the following diagram that illustrates these various risk interdependencies and where they may reside:




To assess and address the applicable risks for a given enterprise, ERM models typically include the generally recognized core principles and processes set forth below. We note that many students and practitioners of ERM point to the Australian–New Zealand Standard for Risk Management, AS/NZS 4360:2004, as one of the best contemporary expressions of what ERM is; other organizations, such as the non-profit Risk and Insurance Management Society (RIMS), have developed ERM models conceptually similar to AS/NZS 4360:2004. These are just two ERM resources; in Exhibit B, *Enterprise Risk Management for Critical Infrastructures*, we provide supplemental information and examples of ERM. Common to all of these are the following ERM principles and processes:

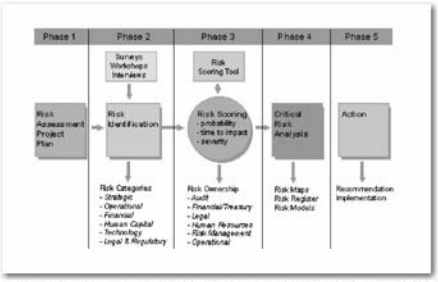
1. **Establish the context for ERM** as determined by a firm's unique business needs, regulatory environments, organizational structures, and assets of the company. Establishing the context sets up the "Risk Assessment" stage.
2. **Identify all risks** through a variety of risk identification techniques and tools. These can include interviews, surveys, on-line tools, workshops and the like, and should appropriately involve downstream and upstream stakeholders.
3. **Analyze all risks.** Whatever modest differences exist among the various ERM models, each of them stresses that risk identification, analysis, and the next step – evaluation – are not confined to a single area of the company. Thus, risks and vulnerabilities are not "stove-piped."
4. **Evaluate all risks.** This means vulnerabilities are evaluated, criticalities quantified, priorities established and mitigation roles/responsibilities assigned at an enterprise level. After this step, the enterprise's Risk Assessment (steps 2, 3, and 4 or "vulnerability assessment" in the language of the NIPP and the SSPs) leads to . . .

5. **Treat All Risks!** In other words, implement the plan.

Throughout the five steps, two other core ERM principles/processes are constantly in play:

- **Communicate and consult;** and
- **Monitor and review.**

These two are particularly important during steps 2, 3 and 4, and provide a loopback to significantly modify or merely tweak the whole exercise wherever changes may be called for. There is a helpful graphic, available on the Internet, which provides a visualization of ERM phases:




Source: http://www.aon.com/us/busi/risk_management/risk_consulting/ent_risk_mgmt/default.jsp. Accessed on 21 October 2007.

Two additional aspects of ERM should be emphasized. First, ERM requires the development and implementation of risk assessments and analyses based upon criteria and metrics that are uniformly documented; these assessments generate data (internal trails) and are verified through periodic audits. While the firm will probably not disclose to external audiences, regulatory or otherwise, the stream of data and information that assists and informs both managers and owners of risk, aggregated ERM data can inform external audiences and can provide useful indices of risk reduction over time. Second, and flowing from the first, a commitment to ERM includes a commitment to update the analysis on a periodic basis (quarterly, annually, whatever is appropriate for the enterprise) for the long haul.

The CIP Program found ERM particularly attractive because ERM shines a light on cyber-CIP risks and all other enterprise risks at very high levels of accountability in the corporation, including the boardroom. The benefits of ERM are not limited, of course, to the private sector; governments, most notably municipalities, are looking to ERM as a valuable tool. Equally obvious, ERM has benefits beyond cyber-CIP, but we believe this integrated, enterprise-level approach to the identification, assessment, and mitigation of *all* risks has particular merit in addressing cyber risks that permeate an organization's many internal structures.

For most firms that own and operate CI/KR, a good percentage of the risk-pieces are likely to fall on the operations side of the enterprise, which often is not well represented at higher levels of corporate governance. When cyber-CIP is confined to one area of the enterprise (*e.g.* the IT department), its voice, vote and authority – including "budgetary authority" – may not be adequate to the task. Therefore, placing cyber-CIP into ERM does not diminish critical infrastructure protection within a company but instead elevates it.

As awareness and corporate acceptance of ERM has grown, some firms have created broader functional responsibilities and a name for the cowboy, such as Chief Risk Officer (CRO). The CRO typically

has direct lines of communication with the CEO and the firm's other C-Levels. The CRO typically has ready access to, is seen and is heard by the board of directors. Because the points of accountability for management of all risks are consolidated, ERM in theory provides the cowboy – the Chief Risk Officer or equivalent – with authorities and tools to herd several cats and thus reduce risks. Corporate resources can be more efficiently allocated by using ERM, which, after all, is an "All Hazards" approach to risk that is part of the NIPP–SSP lexicon.

**Recommended Next Steps and Incentives to Get There**

At the heart of enhancing and implementing the SSPs is getting firms to "do the right thing" even when there is no requirement in law for them to do so, and to repeat what we said earlier, we are *not* recommending any additional command and control authorities for DHS. We recognize that doing the right thing may provide firms with benefits and these extend beyond security. But it is also important to recognize that it will cost firms time and money; voluntarily collaborating with government on cyber-CIP is not cost free.

To be sure, companies already have many incentives to better and more comprehensively manage their risks in terms of smoother, more efficient operations. In addition, a company that lets it be known that it practices effective enterprise risk management often is rewarded in the marketplace. In 2006, Ernst & Young (E&Y) published a cross-stakeholder study entitled, "Managing Risks: Shareholder Perspectives." E&Y interviewed over 700 senior decision makers representing three distinct stakeholder groups – investors, executive management, and independent non-executive board members – to gain their perspectives on risk and risk management. The report's key findings are:

- Risk mitigation and compliance are the top risk management priorities across all three stakeholder groups.
- All stakeholders consistently state that clear ownership of risk and effective communications are key factors for successful risk management.
- All stakeholders will exercise their influence in the face of *perceived* poor risk management.
- Investors will either not invest . . . or divest in the face of poor risk management.
- High-performing companies place more emphasis on risk mitigation, compliance and seeking competitive advantage from risk management.
- High-performing companies are four or five times more likely to have a risk-aware culture.

In other words, if a firm is perceived to be, or is in fact, *not* engaging in effective risk mitigation and compliance, investors stop investing or sell off; firms that do risk management, compliance, and communications well are considered high performers who will have the confidence of investors. That is a powerful incentive government can't provide.

Having said that, but keeping in mind the criticality of advancing the ball on protecting CI/KR from cyber and conventional threats and the need to gain awareness and effective involvement from those in the small and medium business space, Congress and the federal government should consider developing incentives that will further encourage firms to do the right thing. The need for such incentives is underscored by the fact that GAO found that only three of the 17 SSPs fully addressed incentivizing vulnerability assessments.

Our suggestions for incentives include the following:

1. **Sponsor "ERM for CIP" workshops –** As part of the on-going work in providing training, conducting simulations and exercises, and convening workshops, DHS as well as the non-DHS SSAs should partner with established and recognized providers of ERM education, training and certification to develop a workshop (or series of workshops) that would be offered to private-sector

owner/operators of CI/KR. The federal government should underwrite most or all of the cost of the workshops (*i.e.*, no fee or minimal fee for those eligible to register and attend), thus providing incentives for firms to develop and implement ERM plans. If this incentive is to be offered, we strongly recommend that Congress insist on a few important qualifying criteria:

- Provide that the workshops be "customizable-off-the-shelf" (COTS) offerings from institutions and organizations that have developed well-established and accepted ERM products. Introducing high-level awareness of critical infrastructures and cybersecurity into these off-the-shelf products is an acceptable customization. An unacceptable customization, in our view, is for the federal sponsor to subordinate core ERM principles by pushing CIP to center stage. For ERM-CIP to work, it is the cowboy, not the cats, who runs the show.
- Develop selection criteria to determine companies that are eligible to attend. Preliminary research by the CIP Program using Census data indicates that the establishments in the 17 CI/KR sectors would encompass roughly 50 percent of the U.S. economy in terms of value, number of employees, and number of establishments. However, while many businesses are technically part of one or more of the 17 sectors, not all of those businesses or the assets they own and operate are truly critical for national security, economic security, or public health and safety. It is an understandable tendency for officials to seek, and the public to support, an expansive definition of what we as a Nation should protect, but in trying to protect everything we run the risk of not protecting anything truly well.
- Establish prerequisites for participants from an eligible company. The participants should be invited based on (a) qualification as measured by university degree, technical/professional certifications, or demonstrated and documented experience and proficiency; (b) enterprise-wide roles and responsibilities; and (c) diversity – the ideal workshop audience is from several CI/KR sectors.

2. **Alternatively, provide a tax credit** to qualified companies that obtain education, training, and credentialing in ERM. Congress should consider providing sufficient guidance to the Treasury Department (which will write the implementing regulations) that speak to the important criteria outlined above.

Either way, the federal government could test the feasibility and value of ERM incentives at relatively little cost, particularly if the important COTS principle and other qualifying criteria are respected. At a minimum, the Congress could authorize and fund a limited "proof of concept" pilot program, consisting of 10 or so workshops given over six months; course evaluation instruments could be developed that will provide useful feedback to the DHS, the ERM workshop vendor(s) and the Congress.

3. **Establish a public recognition and rewards program** for companies that have raised the bar on cyber-CIP. A useful analogy is the *Energy Star* program, which recognizes companies that produce energy-efficient products. To receive *Energy Star* recognition and use of its marketing symbol, products must meet certain efficiency requirements that are grounded in verifiable measurements. To receive what we might call *Cyber Star* recognition and rewards, qualifying criteria should be measurable and raise the bar over time.
4. **Provide preferences in federal government contracting** for companies that own/operate CI/KR and have obtained training and certification in "ERM for CIP" (our first incentive suggestion) and/or received the recognition/reward (our second incentive suggestion). Preferences should be sunsetted to incentivize continual improvement and continued education and training.
5. **Government leading by example.** If 80 percent of the Nation's CI/KR is owned/operated by the private sector, then governments – federal, state and local – own and operate the other 20 percent. Governments must be models of enhanced cyber-CIP if for no other reason than that failing to adequately protect 20 percent of critical infrastructures that governments own/operate for the American people is not acceptable. But there is another reason: one proven way to incentivize is to lead by example. Every successful coach, teacher, executive, or parent knows this, and it was one of the most important lessons I took from my experience at OMB during Y2K. A potent incentive for the private sector is for the public sector to clean up its act and protect the people's CI/KR – first.

**Concluding Thoughts**

Another very important lesson we learned from Y2K is the importance of collaborative, collegial, and effective public–public partnerships – that is, the incredible value of respectful federal–state–local government partnerships. Let me provide another even more recent example of a good public–public partnership between the U.S. Department of Energy and the states.

An obscure provision of the "State Energy Efficiency Programs Improvement Act of 1990" (P.L. 101-440) requires states to prepare and submit to the Secretary of DOE "energy emergency planning programs" if they accept federal funds for this purpose. These "state energy emergency response plans" (SEERPs), as they are now called, are in many respects state equivalents of the federal energy sector SSP. By design, these SEERPs should contain emergency planning coordinating and response components, including cyber-CIP, that are complementary to the federal energy SSP. In 1990, Congress clearly stated that the Secretary has *no* authority to dictate planning details to the states; he could review and comment, but "for informational purposes only." Recognizing the importance of SEERPs as a means to better protect CIP and cyber-CIP, DOE chose to view its limited authority as an opportunity, not an impediment. It worked collaboratively and informally with the states, engaging them through established institutions which the states knew and trusted, such as the National Association of State Energy Officials (NASEO) and the National Association of Regulatory Utility Commissioners (NARUC). The result: highly detailed NASEO guidelines for preparing SEERPs that was published in November 2005. DOE offered funding and more: it used its convening powers to bring state officials and regulators together, and DOE offered workshops, simulation exercises and the considerable expertise and experience of the department's resources. When the CIP Program evaluated 47 of these SEERPs for DOE a few months ago, it was clear that states that took advantage of DOE's offers of assistance tended to have better plans than those that did not, and plans developed after NASEO published its voluntary guidelines were, overall, better than SEERPs drafted before. Good public–public partnerships can produce valuable results.

This brings me to my final point, which goes to often obscure or seemingly arcane other federal laws, such as the 1990 energy law. I mentioned earlier that one of my responsibilities during my service at OMB was a responsibility for implementing the Paperwork Reduction Act of 1995 (PRA). I also mentioned earlier that the SSPs are written by the SSAs with input from the private sector and are necessarily only as good as the input provided. I recognize that the quality of the information provided by the private sector is dependent on many factors, several of which came to light in the controversies surrounding the NIPP metrics generally and the security-related metrics specifically. Undoubtedly, the primary concern centered on how DHS will use these metrics and whether DHS can and will provide strong assurances that the sensitive "raw data" behind metrics – if shared – will remain secure in the hands of the federal government. But the development of the metrics and collection of associated data also implicated the PRA. Some are now suggesting the PRA is an impediment to enhancing and implementing the SSPs, and that the PRA must be substantially amended for this project to proceed. That is *not* my view. The PRA provides an opportunity to enhance and implement the SSPs because it provides a known, trusted process – involving the private sector and an interagency review – to develop and collect data and information – CIP and cyber-CIP metrics – that are useful and methodologically sound.

We thank the Subcommittee for convening this hearing. As I said at the outset, six years and billions of dollars after 9/11 we are still talking about plans. If, as appears to be the case, the SSPs, taken as a whole, have not yet comprehensively developed a set of quality metrics that allow measurements and comparisons of progress or lack of progress in addressing cybersecurity criteria, then the Congress and the American public will have no meaningful benchmarks at the beginning of implementation or over time. Stated simply, unless these deficiencies are systematically addressed, we will have no idea if the expenditures and efforts we are committing to the effort are translating into measurable improvements of security. I appreciate the opportunity to testify today, and look forward to answering any questions you may have.

GEORGE MASON UNIVERSITY | School of Law

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

3301 Fairfax Drive, MS 1G7, Arlington, Virginia 22201
Telephone: 703-993-4840; Fax: 703-993-4847

**EXHIBIT A: Summary & "Moving Forward" Issues from a Critical Infrastructure Protection Program Workshop on Cybersecurity & Liability**

**Friday, 20 July 2007**
**Dean's Suite**
**George Mason University School of Law**

**Introduction**

On July 20, 2007, the Critical Infrastructure Protection Program ("CIP Program") at the George Mason University School of Law held a workshop on cybersecurity and issues associated with liability. Those attending the invitation-only workshop were representatives of academia (law, economics and public policy), the US Congress, the federal government, think tanks and trade associations, and senior level executives of major insurance underwriters and reinsurance companies. A focus of the workshop was how the insurance and reinsurance industries measure and assess the cyber risks of firms seeking to mitigate their exposure to cyber-related losses.

This paper provides an overview and assessment of the workshop, and suggests steps that might be taken going forward to promote higher levels of cybersecurity awareness and protection. Reinsurers and insurers ("the industry") may play a crucial role in advancing the state of cybersecurity practices of the Nation's businesses. To use an analogy from the "bricks and mortar world", the industry has played a vital role in advancing the physical security of buildings, assets and people through the development of building and safety codes and product standards. Progress – risk reduction – has been documented through data and information often required by contractual and regulatory structures. However, at this time, there are several impediments to creating a similar, economically viable market for cyber insurance/reinsurance, most of which are associated with identifying and measuring cyber risks. As one participant remarked, the state of the industry's knowledge in writing policies for cyber risks does not readily transfer from its 150-plus years of experience in the bricks and mortar economy, and "cyber underwriting remains an art rather than a science." Another attendee pointed out a significant distinction between cyber and conventional physical risks: "Ordinarily, a fire in Cincinnati doesn't burn buildings in Indianapolis," but "cyberfires" in one location can and do burn first parties and third parties often in multiple locations and sometimes across legal jurisdictions.

**Structure of the Market**

The insurance/reinsurance market for cyber liability is relatively immature and evolving, starting some ten years ago with a focus on "dot-com" types of exposures. Insurance/reinsurance has the potential to become an important tool in protecting vital data/information systems and networks, thus increasing the overall security of the nation's economy. Currently, however, "cyber insurance" is a catch-all term for many different kinds of insurance, covering both first-party and third-party risks such as damage from computer malfunctions, viruses, network outages or congestion, external hacking, internal sabotage and theft, web content liability, copyright infringement, and other areas of potential loss related to technology. Companies often found that their losses in these areas were not being covered by their existing business insurance, and the courts passed conflicting judgments on where cyber-related liability resides. Insurers usually responded by narrowing the terms of ordinary liability and property insurance, and sometimes offered a new product that covered these nascent cyber issues.

**Comparable Markets:** Other insurance products illustrate how new risks, or perceptions of risks and responsibilities, can change markets. For example, when legal liability for environmental harm first arose, insurers fought coverage because the risk had not been calculated and premiums had not been collected to cover the loss. After the initial shock, insurers began to offer environmental risk insurance, which evolved from a small niche offering in the 1960s to an accepted facet of business risk to be covered today. However, this only happened because government statutes and regulation set standards, making loss calculation possible and widening the risk pool to the point that insurance was profitable to offer. At the same time, regulatory standards and associated business reporting requirements provided data and information needed by the industry to model and appreciate risks and to develop appropriate environmental liability products. In the field of property insurance, the idea that a building can and should be insured against a range of risks has become so commonplace that building codes now parallel the standards for insurability. Such is the potential with cyber liability.

Around 2003, carriers began to expunge the dot-com "internet language" from policies and, driven largely by major events/litigation[1] and new state privacy laws, issued approximately $350 million in total cyber liability coverage by late 2005. While the market has grown in dollar volume over the last decade, cyber liability insurance remains a very small and unsustainable slice of the industry's portfolio. Several impediments to growth of the market – and thus higher levels of cyber protection – were identified and discussed:

- In many larger companies, cybersecurity issues have not emerged "from the server room into the board room." (i.e. Business continuity and risk managers are not aware of the need to buy cyber insurance, and IT managers all think that their own security is adequate. Nonetheless, companies have lost millions of dollars in data losses and other cyber liabilities.)
- Corporate accountability for cyber liability has been unclear, and in smaller firms "O-Level" structures (chief security officer, chief risk officer, chief information officer, *et al*) often do not exist. Such small business can store large amounts of data (e.g. patient information, individually identifiable customer data, etc.), yet do not know that they thus have a cyber-liability or how to minimize it.
- Consensus on what constitutes "best cyber practices" is fragmented across industries.
- Lack of demand for cyber liability products also is inhibited by lack of a comprehensive body of cybersecurity standards.
- The nature of cyber threats and thus risk evolves at an extremely high velocity.

---

[1] *E.g.*, Ingram Micro, AOL v. St. Paul, Seagate v. St. Paul, Choicepoint, and TJ Max.x. "Nutshell" summaries on these cases are provided as a supplement to this document.

**Cybersecurity Metrics**

Issues associated with cyber metrics were raised frequently and throughout this workshop. A facilitator read a quote from a transcript of a previous CIP Program event that neatly framed the metrics issue:

*Issues of homeland security are of critical importance, but concerns should not be exclusive to government agencies and entities. Like first responders, when bad things happen people immediately look to the government or the insurance/reinsurance industry to maintain or preserve liquidity. The private sector has a critically important role to play in emergency preparedness and in ensuring that our national infrastructure is as secure as possible. The government has data, the scope of which is difficult to imagine. If we could develop a way to work with the government to mine [that data] effectively, we can build even more sophisticated models that will help to provide insurers and reinsurers with additional confidence.* [Mr. Harrison Oellrich of Guy Carpenter & Company, 27 September 2006]

Metrics are data and information that, if readily available, would inform the industry, its actual and potential clients, and policymakers about cyber risks. Over time, cyber metrics could form an actuarial body of data that would allow the industry to produce accurate models for, and thus define and price, cyber insurance coverage. This data would facilitate a better understanding of risks, predict behaviors associated with cyber threats, and even construct models of catastrophic "cyber-hurricanes." More importantly, the availability of cyber metrics allows improvement over time to be measured and drives the development of better cybersecurity standards and practices. Workshop participants discussed the following questions:

- What kinds of data are needed?
- Is the data being collected?
- If so, what entities are collecting the data and are there restrictions on industry access to the data?

Though workshop attendees did not pinpoint specific answers to these data questions, anecdotes discussed during the workshop strongly suggest that data that is "cyber-analogous" to the kinds of "bricks and mortar" actuarial metrics upon which the industry has historically relied and used either is not being collected or currently is not accessible to the industry. Data might be available from cyber devices and networks, but it may be technically difficult or too costly to collect. One participant suggested that the cyber metrics challenges were reminiscent of problems faced by the electric power industry in collecting and providing data that enables modeling and post mortems of large disturbances and outages.[2] One attendee noted that the manufacturers of cybersecurity software and appliances often incorporate automatic-remote threat reporting into their products. It was suggested that the industry might seek partnerships with these manufacturers so that the industry could have conditional, secure access to *aggregated* threat reports. Such information might allow the industry to see the intensity, duration, frequency, location (jurisdiction), nature and resolution of cyberthreats. Such aggregated data also may have uses in modeling.

In addition, for certain types of risks the data does not exist because the relevant event has never occurred; as with terrorism data in general, insurers lack and will continue to lack meaningful data on a large-scale successful terrorist cyberattack. If the industry had better data on non-cataclysmic losses, however, it would be possible to model larger attacks using methods now employed by reinsurers and risk management groups.

[2] The US – Canada Task Force's report on the August 2003 outage that hit the northeastern US and Canada provides an excellent examples of the impediments to obtaining and normalizing disturbance and outage-related data even when it is being collected and maintained by utilities.

**Modeling**

Professor Kevin McCabe of GMU's Center for the Study of Neuroeconomics ("CSN") and the Mercatus Center made a presentation over lunch during which he suggested a neuroeconomics modeling technique that the industry might consider in lieu of the conventional actuarial data based models. Neuroeconomics is an "experimental study of how emergent mental computations in the brain interact with the emergent computations of institutions to produce legal, political, and economic order."[3] Emilia Siravo from Guy Carpenter stated that combining neuroeconomics with game theory might produce cyber liability models that provide value to insurers and reinsurers given the metrics limitations discussed above. Additional discussion of this topic is provided in the final section of this paper, **Moving Forward**.

**Cybersecurity Standards & Professional Certifications**

Issues associated with standards and certifications were on the workshop agenda for discussion after lunch, but due to discussion overflow on the luncheon topic, such issues were not thoroughly discussed at the workshop. Cursory mention was made of voluntary and mandatory regimes such as COBIT, COSO, ISO 17799 and 27001, NIST, Section 404 of the Sarbanes – Oxley Act, and others. Two participants suggested that as a next step consideration should be given to the mandatory cybersecurity standards that have been developed by the North American Electric Reliability Corporation (NERC) and which will be approved by the Federal Energy Regulatory Commission (FERC).[4] These cyber standards apply to over 500 entities identified by NERC and FERC as owners-users-operators of the "bulk electric system" and, as such, fall under the scope of new section 215 of the Federal Power Act. A broad spectrum of stakeholders developed the NERC cybersecurity standards by using an American National Standards Institute (ANSI[5]) process. In the Energy Policy Act of 2005 (EPACT-2005), the Congress specifically required the inclusion of cybersecurity standards in the larger body of electric power reliability standards.[6] On the same day the workshop was held, the Federal Energy Regulatory Commission (FERC) published a proposal to adopt eight of the NERC Critical Infrastructure Protection ("CIP") cyber standards and further proposed to direct NERC to make specific modifications to other cyber standards. A couple of workshop participants suggested that while statistically significant data and information flowing from these cyber standards may not be available for some time, the insurance/reinsurance industry may find it useful to engage NERC and its members as part of the industry's effort to develop and expand cyber liability insurance.[7]

Another participant suggested that the industry, in its quest for data and information that would better inform the market and models, may wish to examine the role of recognized professional certifications. For example, the industry could identify professional certifications and certifying organizations that are relevant to a company's development and implementation of robust cybersecurity. If these certified professionals could be linked to specific companies (or industries), case studies and models could be developed that advance cybersecurity's knowledge base. The CIP Program recently completed a review of these and other

---

[3] http://www.neuroeconomics.net/

[4] For more information, please refer to the FERC Notice of Proposed Rulemaking, *Mandatory Reliability Standards for Critical Infrastructure* Protection. 120 FERC ¶ 61,077, 19 CFR Part 39, Docket No. RM06-22-000 (20 July 2007).

[5] The following is taken verbatim from the ANSI website (http://www.ansi.org): "The ANSI coordinates development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. The Institute oversees creation, promulgation and use of thousands of international norms and guidelines that directly impact businesses in nearly every sector: from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more. ANSI is the official U.S. representative to the International Organization for Standardization (ISO)."

[6] A summary of the revised cyber standards implementation plan is provided on the NERC website at ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Revised_Implementation_Plan_CIP-002-009.pdf.

[7] If any workshop participant seeks an introduction to NERC cybersecurity experts, please contact Michael Ebert of the CIP Program at (703) 993-2288 or email mebert@gmu.edu.

standards/certifications/risk management issues for a federal agency. We offer to assist workshop attendees with contact information for organizations and selected vendors who set certification requirements and implement training curriculae to those requirements.

**Moving Forward**

CIP Program Director John McCarthy opened this final section of the workshop by returning to the alternative models theme articulated by Professor McCabe and Emilia Siravo. McCarthy recommended establishing an experimental working group that would employ game theory, neuroeconomics and other concepts to develop a model prototype of cyber insurance markets. Workshop participants who are interested in participating in such a group are asked to call Michael Ebert at the CIP Program, (703) 993-2288 (email mebert@gmu.edu). Experimental models might allow the industry to identify risk categories, market conditions and data needs for different cyber insurance products, thus potentially bypassing the problems identified of unavailable or unusable data. Mr. Leigh Williams of the BITS Financial Services Roundtable and others weighed in favor of further examination and experimentation with "scenario-based game theory models." If nothing else, working through alternative models may help inform a fundamental data question the answer to which remained illusive at the end of the workshop: *Exactly what kind of data are needed to populate cyberliability models that are acceptable to the industry and its clients?*

Mr. Williams and Dr. Kenneth Friedman of the US Department of Energy also suggested that the insurance/reinsurance industry actively seek partnerships with the US Department of Treasury, the National Labs (specifically DOE's Sandia Lab), and to "talk directly with [the US Department of Homeland Security]." Williams and Friedman[8] volunteered to facilitate these partnerships, and McCarthy offered the possibility of using an existing CIP Program contract vehicle with DHS as another possible means to engage the agency and its sector specific critical infrastructure planning elements. Time is of the essence, as the Sector-Specific Plans are slated to be sent to the White House around the first of September.

Michelle Boardman, Assistant Professor of Law at George Mason University School of Law who holds both practitioner and government experience, notably with insurance and contract law, suggested that central to the future of cybersecurity third-party insurance, both for gathering data and modeling, is the ability of insurers to forecast how liability for breaches of security will be assessed under the law. In the absence of clear industry standards or legal/regulatory requirements, courts may find that businesses are not liable in tort because their security systems met a bare minimum of industry practice. Moreover, this uncertainty about the finding and amounts of liability make it difficult for insurers to forecast loss amounts and frequency. The insurance industry, she concludes, should consider leading the way in setting standards for cybersecurity. Leadership could take many forms. Initially, insurers could require certain standards of their policyholders in order to maintain cybersecurity coverage and favorable rates. Professor Boardman recommends that insurers could offer to certify those with coverage who meet these goals and such certification might have value in assuring the public that a business is responsible. Moreover, while the industry is hesitant about seeking particular governmental standards, where standards will inevitably be adopted, the industry should contribute its knowledgeable views to their formation.

Another suggestion made is to examine the "14 FTC consent decrees" as being possible sources for developing a cybersecurity best practices template. Lastly, several participants urged the industry to very carefully consider whether the political, policy and technical environments would support an industry-backed federal legislative initiative to engender a regulatory framework for cyber. Seeking this kind of federal intervention may be premature and/or produce unintended results.

---

[8] Dr. Friedman may be contacted at (202) 586-0379 or email kenneth.friedman@hq.doe.gov.

**EXHIBIT B: Enterprise Risk Management (ERM) for Critical Infrastructures (ERM – CIP)**

**1) Defining ERM in the Context of the National Infrastructure Protection Plan (NIPP)**

The U.S. Department of Homeland Security (DHS) is specifically charged, among other things, with establishing a common framework among public and private sector stakeholders to address the overall management of risk, and communicate the value of a risk-based approach.[1] The principal framework for public-private sector coordination in matters related to critical infrastructure security is the National Infrastructure Protection Plan (NIPP), which also defines a Risk Management Framework for identification, prioritization, measurement and mitigation of risks.[2]

Indeed, companies in the private sector have been employing various forms of risk management for a number of years to protect their assets and revenue. Businesses routinely face operational (physical, cyber, human) and financial (market, credit, insurance) risks. They are also very susceptible to extreme events. It is estimated that "43 percent of businesses that close following a natural disaster never reopen [and] an additional 29 percent of businesses close down permanently within 2 years of a natural disaster."[3]

The following chart summarizes the types of risks an enterprise in a CI sector typically faces:


There are numerous definitions for both risk management and enterprise risk management (ERM).[4] Synthesizing all of them into one sentence, we suggest the following:

*"ERM is the systematic application of strategic and operational management policies, procedures and practices aimed at identifying, analyzing, evaluating, treating and monitoring all risks to the business processes of an enterprise."*

---

[1] U.S. Department of Homeland Security, "Directorate for National Protection and Programs," *U.S. Department of Homeland Security*, 2007, http://www.dhs.gov/xabout/structure/editorial_0794.shtm (cited April 10, 2007).
[2] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 105.
[3] *Gulf Coast Back to Business Act 2007*, 110th Congress, 1st Session, S. 5371S.
[4] See Appendix B: Definitions of Risk Management and ERM for a list of quoted risk management and ERM-related definitions.

The ERM approach differs from traditional business risk management and continuity planning in two dimensions:

1. **Holistic Dimension.** ERM promotes a holistic view of the entire company, as opposed to risk affecting only an internal process or a particular division. This view became necessary because of the increasing integration of internal and external business processes through information technology.
2. **Compliance Dimension.** ERM is being used to provide transparency to analysts, auditors, and stakeholders, as well as to support regulatory compliance. This function is a result of legislation to stop financial and accounting breaches that led to corporate collapses.

**2) Providing Education and Training in ERM to CI/KR owners and operators**

Targeted education and training courses that integrate government-led risk analysis efforts with private sector standards are a prime mechanism to increase the security of physical assets and cyber systems, since large parts of the Nation's critical infrastructure and key resources (CI/KR) are owned and operated by the private sector.[5]

The NIPP itself outlines an educational program that conveys the type of expertise and awareness essential for CI/KR protection, and "recognizes the importance of leveraging existing accredited academic programs, professional certification standards, and technical training programs" to provide individuals with up-to-date risk management knowledge and skills to perform their roles and responsibilities as CI/KR owners and operators.[6]

A very rough estimate of the number of establishments, value, and paid employees in 13 sectors reveals that close to 50% of economic activity in the U.S. takes place in businesses that are part of current CI/KR sector definitions.[7] Clearly, not all of these businesses are indeed critical to national security, economic security, and public health and safety in the sense of the Patriot Act.[8] Also, not every small establishment has a dedicated security function tied into a risk management process.[9] However, even if only 10% of all sector establishments fulfilled those criteria of criticality and size, there would still be a pool of close to a half million potential participants for ERM and related curricula.

**3) Improving Qualifications and Certifications to Support the NIPP Process**

There is little harmonization in either roles, responsibilities, qualifications, or experience of security managers. Even the overall number of officers in this field is difficult to determine since these positions have no single job classification or particular degree requirement. The Bureau of Labor Statistics, which maintains extensive occupational records by industry sector, counts more than

---

[5] The common estimate is 85%, even though this number still needs to be substantiated. For example, it is unclear whether this means 85% of infrastructure facilities, or employers, or employees, etc. See Table 1 for a differentiated approach.

[6] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 80.

[7] In mid-2006, the CIP Program prepared a research brief for DHS entitled "Estimating the Economic and Employment Value of Critical Infrastructure Sectors in the United States," which is available upon request.

[8] Here, the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Critical Infrastructure Protection Act of 2001, 42 USC 5195c).

[9] Establishments are economic units, such as a farm, a factory, a store or an agency that usually is at a single physical location.

200,000 Computer and Information Systems Managers.[10] Some, but not all of them, may be Chief Information Officers (CIO). A different source estimates the number of CSOs in the U.S. as being close to 27,000.[11]

In terms of security budgets and expenditures, estimates range from $22 to $47 million in companies that have $8 to $10 billion revenue, and 15,000 to 20,000 employees.[12] Other sources contend that enterprises, regardless of size, spend between three to ten percent of revenues on technology, and one to three percent of those technology expenditures on security.[13]

Despite this lack of standardization in roles and responsibilities, there are a number of security-related certifications that are offered by industry associations, vendors, or academic programs. For example, ASIS International (ASIS), formerly known as the American Society for Industrial Security, has created optional certification programs such as Certified Protection Professional (CPP) and Physical Security Professional (PSP). Some have gained quasi-industry standard prominence, in particular the Certified Information Systems Security Professional (CISSP) by the International Information Systems Security Certifications Consortium (ISC2), and the Certified Information Systems Auditor (CISA) by the Information Systems Audit and Control Association (ISACA).[14]

**4) Introducing Industry Standards, and Best Practices**

**Risk Management – AS/NZS 4360**

The Australian Standards organization has developed a risk management standard that employs a method of identifying, analyzing, evaluating, treating, monitoring, and communicating risks in order to minimize losses and maximize opportunities for an organization.[15] This standard may be applied at all stages in the life of an activity, function, project, or asset. The documentation is very short and simple, and thus particularly useful for smaller companies.

**Information Risk Management – ISO 27002**

The International Organization for Standardization (ISO) has developed a code of practice for information security management, which is published as ISO 27002.[16] It is an internationally recognized information security standard consisting of a set of controls representing best practices in information technology.[17] While IT systems-centric, the strength of ISO 27002 is that it is accepted internationally, and sector-independent. This might be of significant appeal to those

---

[10] SOC code 113021, May 2005. Bureau of Labor Statistics, "Occupational Employment Statistics," *Bureau of Labor Statistics*, 2005, http://data.bls.gov/oes/search.jsp (cited April 10, 2007).
[11] "CSO Audience," *CSO* (May 6, 2002), http://www.csoonline.com/marketing/audience.html.
[12] Ibid.
[13] Packer, Ryon, "Battling for budget: Diverging perspectives," *SC Magazine* (cited March 1, 2003), 1.
[14] Additional professional organizations provide valuable information for ERM and risk professionals, including: Global Association of Risk Professionals (GARP; http://www.garp.com), The Institute of Internal Auditors (IIA; http://www.theiia.org), and The Risk Management Association (RMA; http://www.rmahq.org).
[15] AS/NZS 4360: 2004. *Australian/New Zealand Risk Management.* Standards Australia, 2004.
[16] ISO 17799 was renumbered ISO/IEC 27002:2005 in July 2007. ISO/IEC 27002:2005 has a companion standard, ISO 27001, a specification for information security management systems. Hereafter, both standards are collectively referred to as "ISO 27002." ISO/IEC 27002:2005 (E). *Information Technology-Security Techniques-Code of Practice for Information Security* Management. International Standards Organization, Geneva, 2005.
[17] ISO standards are voluntary. As a non-governmental organization, ISO has no legal authority to enforce their implementation. However, some standards have been adopted in member countries as part of their regulatory framework (mainly consumer safety standards), and others have become a market requirement (such as ISO 9000 quality management systems. ISO 9000:2000. *Quality Management Systems – Fundamentals and Vocabulary*. International Standards Organization, Geneva, 2000.)

CI/KR owners and operators that have establishments in the United States and overseas. The standard addresses the following areas of information security management:[18]

- Security policy;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Information systems acquisition, development and maintenance;
- Access control;
- Organization of information security
- Information security incident management;
- Business continuity management;
- Communications and operations management;
- Compliance

Included in the standard documentation are business impact analysis, disaster recovery, business continuity, internal audit review procedures, and detailed checklists that allow for the establishment of metrics and benchmarks, thus facilitating longitudinal assessments of compliance and progress. Organizations can choose to go through an ISO certification process, which means third party evaluators review the organization's business processes. Overall, ISO 17002 can be used to determine and improve upon a company's information security posture.

**Financial Risk Management – SOX**

The Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as the Sarbanes-Oxley Act (SOX), was intended to regain the public trust in corporate governance and financial practices in the wake of corporate scandals.[19] The Act is arranged into 11 titles and applies to various topics including:

- Compliance;
- Auditor independence;
- Corporate governance; and
- Enhanced financial disclosure.

The aim of SOX is to, among other things, "enhance corporate governance through measures that will strengthen internal check and balances."[20] To reach that end, the Act and subsequent regulations require continued reporting and, ultimately, continuous oversight of all company operations. Since all of this is enabled through information technology, SOX has become as much a guideline for IT systems as it is for auditing systems. Corporate security executives have started to redesign their asset, system, and network security to meet the requirements of SOX by:

- Assessing the current state of the IT control environment;
- Designing controls necessary to meet the requirements of Sarbanes-Oxley;
- Developing an approach for testing and sustaining controls into the future;
- Identifying exceptions and related remediation plans and adding; and
- Compensating controls for exceptions identified.[21]

---

[18] ISO/IEC 27002:2005 (E). *Information Technology-Security Techniques-Code of Practice for Information Security Management.* International Standards Organization, Geneva, 2005.
[19] Sarbanes-Oxley Act of 2002. HR 3763, 107th Congress, 2d Session (July 30, 2002) PL 107-204; 116 Stat 745.
[20] *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, IT Governance Institute, 2006.
[21] Ibid.

Due to the size of and complexity of the reports required under SOX, a great deal of information about the internal operations of a company are continuously gathered and analyzed. Compliance with the Act thus lays a foundation for implementing enterprise risk management capabilities that did not previously exist for many companies; an organization cannot manage its risk when it suppresses information about business realities.[22]

**5) Defining the Role of DHS**

Measurable risk management improvements for critical infrastructure sectors, as laid out in the NIPP, require effective ERM practices on the enterprise level. Industry standards, metrics, and best practices, such as SOX and ISO, are promoted through professional certifications, such as the CISSP and CPP, and through academic degree programs.

A DHS-sponsored curriculum that contains elements from existing education and training programs used by the private sector has two advantages:

1. It allows DHS to integrate methods and metrics laid out in planning documents with private sector enterprise risk management approaches, including assessments costs and benefits of security investments.
2. It will attract private sector participants who may use the instruction provided as continuing education leading to certification of their security personnel.

As a result, the participants in the courses will have a better understanding of the DHS risk framework and metrics requirements, and will be able to select and implement one or more enterprise risk management processes that are geared towards increasing their asset and system security consistent with the national protection framework.

**6) Integration**

Within DHS, a number of initiatives have been developed to assist in establishing baseline knowledge of sector security postures, evaluating ongoing CI/KR protection activities, and making informed decisions about future CI/KR protection activities, such as a Metrics and Reporting Program (NIPP Metric Collection Program or NIPP Metrics Survey).

Ideally, sector-level metrics would be aligned with standard data already gathered by individual companies in the course of their enterprise risk management process. Provided on a voluntary basis, and aggregated through the sector coordinating mechanisms, they would contribute to a better understanding of the state of security in critical infrastructures. Appendix D (Metrics for IT Security) contains a list of metrics that are used in the context of ERM. Further research is required to a) identify what companies use which of these metrics, and over what period of time, and b) develop categories, filters, and algorithms to match up the individual company metrics with the sector-level categories.

---

[22] James DeLoach, "Building Enterprise Risk Management on the Foundation Laid by Sarbanes-Oxley," *KnowledgeLeader*" (August 25, 2003), available at: http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/Sarbanes-OxleyActBuildingEnterpriseRiskManagement!OpenDocument (cited April 26, 2007).

Mr. LANGEVIN. The Chair now recognizes Mr. Clinton for 5 minutes. Welcome.

## STATEMENT OF LARRY CLINTON, PRESIDENT, INTERNET SECURITY ALLIANCE

Mr. CLINTON. Thank you, Mr. Chairman, Mr. McCaul.

The Internet Security Alliance believes the threat to our economy, our Nation, and our citizenry from cyber attacks is real and growing. We also believe that government and industry must work much more aggressively to address these threats. We are past the time for simple education. Now is the time for action.

However, for industry and government to create a sustainable and effective cyber defense system, we need a fundamental rethinking about how we address these issues.

First, the Internet is unlike anything we have ever dealt with before and, hence, securing it will require a solution unlike anything we have done before. In its June 2006 GAO report, they cited the number one challenge to developing a public-private sector partner-

ship for cybersecurity was the innate characteristics of the Internet itself. The Internet is just different. It transmits phone calls but it is not a phone line. It makes copies but it is not a Xerox machine. It houses books but it is not a library. It broadcasts images but it is not a TV station. Is critical to our national defense but it is not a military installation.

The Internet is international, interactive, constantly changing, constantly under attack. We cannot simply cut and paste old governing systems and realistically expect that we are going to be able to manage this new system effectively.

Even if Congress were to enact an enlightened statute, it would reach only to our natural borders and hence would not be comprehensive enough. Even if some agency wrote a brilliant regulation, it would probably be out of date before it got through the entire process.

Second. Information security, as Ms. Katzen has pointed out, is not a static and merely technical problem. The threats to the Net have recently morphed from the broad, benign, and well publicized attacks like Love Bug and Blaster, to Designer Now-ware that is constructed to target specific systems where it can reside undetected for a long time while causing significant economic and physical damage.

As a result, traditional antivirus software and viral solutions are becoming inadequate. To adequately address the modern threats, we need an ever-evolving system that addresses all the vulnerabilities, technical and otherwise.

Third, the threat to our infrastructure from cyber attack is very, very serious and growing.

Two years ago, the Internet Security Alliance reported to this committee that the main protocols that the Internet is based on were over 30 years old and had multiple well-known security flaws. Since then, the massive growth in Internet use based on these same protocols has increased our vulnerability at a massive rate. Moreover, the Internet attacks are no longer based on publicity but now are designed to generate money or, more insidiously, power and destruction.

Especially worrisome are cyber attacks that would hijack systems with false information in order to discredit systems and do lasting physical damage. At a corporate level, attacks on this kind have the potential to create liabilities and losses large enough to bankrupt large companies. At a national level, attacks directed at our critical infrastructure industries could cause hundreds of billions of dollars worth of damage and thousands of lives.

But, fortunately, we know a good deal about how to protect ourselves. The best evidence of this is that the Internet has been under attack constantly thousands of times a day and has yet to go down. The largest study ever done of best practices found that organizations that follow the approved best practices for information security have shown a remarkable ability to fend off attacks, recover from attacks, and even deter attacks. The problem is, we need more entities to embrace these practices while also working with us to develop new ones.

The best mechanism to effectively establish a sustainable defense system is to inject market incentives to motivate the adoption of best practices.

Unlike some of the conversation at the first panel, markets do not emerge spontaneously. They must be created and managed. That is what we need to do with cybersecurity.

In this regard, the Internet Security Alliance has come to the committee with a specific and concrete proposal. This proposal is detailed more fully in our written testimony, but it offers a market-based incentive program to bridge the gap between the purely voluntary program as outlined in the national strategy to secure cyber space, and a regulatory model which, A, won't work and, B, would probably be counterproductive.

The core elements of the Cyber Safety Act would be for government to use its market power instead of its regulatory power to promote security primarily through the procurement practice. Congress can lead by example, as Ms. Katzen pointed out. Congress can tie incentives such as civil liabilities safe harbors such as those that are currently provided in the SAFETY Act. Congress can stimulate the stunted cyber insurance market, and I would be delighted to discuss the specifics with this further with the committee. And, Congress can create government industry consortiums similar to what we did with the Sema-Tech to solve our computer chip problem in the 1980s. And, government can create awards programs.

There are other market-based programs such as the use of model contracts that we can use to expand the perimeter of cybersecurity. But I urge the committee to consider acting, but acting in a novel and creative fashion. The old system won't work. A new system must be created. Thank you.

[The statement of Mr. Clinton follows:]

PREPARED STATEMENT OF LARRY CLINTON

Good Morning, I am Larry Clinton, President & CEO of the Internet Security Alliance (ISAlliance). I also am a member of the DHS's Communications Sector Coordinating Council, the Critical Infrastructure Partnership Advisory Council and serve as an Officer on the IT Sector Coordinating Council.

ISAlliance is a cross-sector trade association focused exclusively on information security. We were created in 2001 as collaboration with the Carnegie Mellon University. We now have roughly 1,000 member companies. We provide our members with a range of services, including technical, business operational and public policy. ISAlliance provides its members with an integrated series of security services addressing the technical, legal, business and public policy concerns simultaneously.

I want to thank the Chairman for inviting me to participate.

ISAlliance continues to believe that the threat to our economy, our nation, and our citizenry from cyber attacks is real and growing.

We also believe that government and industry must work much more aggressively to address these threats. We are past the time for simple education about the cyber threat. Now is the time for action.

However, for industry and government to create a sustainable and effective system of cyber defense we need a fundamental re-thinking of how we go about addressing these issues.

This rethinking must include at least three critical realizations.

First, the Internet is a technology unlike anything we have dealt with before and hence will require a solution unlike what we have traditionally used to address technology and business.

We need to change the way government, perhaps including Congress, thinks about and conceptualizes its role in assuring Internet security. In its June 2006 report, "Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan," the GAO got it right. It listed as the number one challenge we face the "innate characteristics of the Internet."

How then is the Internet different?

- It transmits phone calls but it is not a phone line.
- It makes copies but it is not a Xerox machine.
- It houses books but it is not a library.
- It broadcasts images but it is not a TV station.
- It is critical to our national defense, but it is not a military installation.
- It is all these things and much, much more.

The Internet is international, interactive, constantly changing, constantly under attack, then changes and changes again.

It is not even really an "It." It is actually lots of "Its" all knitted together—some public, some private—all transmitting information across corporate and national borders without stopping to pay tolls or check regional sensitivities.

We can not simply "cut and paste" previous governance systems from old technologies or business models and realistically expect that we will be able to manage this system effectively.

The regulatory model we have traditionally used to govern business has not changed much since we created it to deal with the breakthrough technology of 2 centuries ago—the railroad.

To manage the railroad, Congress decided to create an expert agency, the ICC, to pass specific regulations. The ICC begat the rest of the alphabet soup: the FCC, the SEC, the FTC. And, that system has worked arguably well in most instances.

But that system will not work with Internet security. Even if Congress were to enact an enlightened statute, it would not have reach beyond our national borders and hence would not be comprehensive enough. Even if some agency wrote a brilliant regulation, it would likely be out-dated before it got through the process, a process that can be further delayed with court challenges.

And that assumes, unrealistically, that the political process inherent in a government regulation system doesn't "dumb-down" the eventual regulations so that we wind up with a campaign-finance-style standard where everyone can attest that they met the federal regulations, but everyone knows the system is really not working.

That may work in politics, but, frankly, we can't afford that when it comes to Internet security.

Regrettably not enough is being done, either by government or industry, to secure cyber space. We have attempted to manage the risk of 21st century technology solely using regulatory models designed two centuries ago. While regulation has its place, a new, more creative, model built on market incentives must be developed.

Yet, we can't stand idly by either. We must, together, develop a mechanism to assure an effective and sustainable system of security that will accommodate the global breadth of the Internet and still result in a dynamic and constantly improving system of mutual security.

Second, information security is not a static technical problem. Even within the past couple of years the threats have become not just more sophisticated, but more subtle.

For example, we now know that threats to the net have morphed from broad and often relatively benign, if well publicized, attacks like Love Bug and Blaster, to designer malware constructed to target specific systems where it can reside undetected by traditional methods for an indeterminate period of time while causing serious damage.

As a result, traditional AV software and firewall solutions are becoming inadequate. However, a new generation of security products has been, and continues to be, developed to address the continually evolving threats.

To adequately address information security concerns we need to address the full organizational system which relies on information infrastructure.

Our members now look to us to provide a comprehensive risk management approach that encompasses the full-system approach necessary to address the problem. An example is our Enterprise Integration Program which addresses discrete cyber security issues ranging from preventing and handling breaches of personal information to securing the IT supply chain in the era of globalization.

We address these issues by looking at their technical, business operational, human resource, legal and public policy aspects simultaneously and developing an integrated solution. We would commend this fully integrated model to our government partners to consider.

Third, the threat to this nation's and the world's economic infrastructure from the risk of cyber-attack is real.

Two years ago ISA reported to this Committee that the main protocol used to protect this data is over 30 years old and has multiple well-know security flaws.

Since then the massive growth in Internet use based on these same protocols has increased the vulnerability of the Internet at a massive rate.

In addition there are now far more attackers and they have become increasingly more sophisticated. Whereas only a few years ago "hackers" created cutely named attacks like the "love bug" and "slammer" largely to get attention, the current generation use stealth and designer malware that is difficult to detect and in some cases virtually impossible to eradicate.

Even worse, the motivation for Internet attacks is no longer publicity, but money, and more insidiously power and destruction.

Especially worrisome are the cyber-attacks that would hijack systems with false information in order to discredit the systems or do lasting physical damage. At a corporate level, attacks of this kind have the potential to create liabilities and losses large enough to bankrupt most companies. At a national level, attacks of this kind, directed at critical infrastructure industries, have the potential to cause hundreds of billions of dollars worth of damage and to cause thousands of deaths.

Some of the attack scenarios that would produce the most devastating consequences are now being outlined on hacker websites and at hacker conventions. The overall patterns of cyber intrusion campaigns suggest that a number of potentially hostile groups and nation states are actively acquiring the capability to carry out such attacks. Meanwhile, the many ways in which criminal organizations could reap huge profits from highly destructive attacks are also now being widely discussed. Forth, there is some good news: We actually know a good deal about how to protect the Internet.

The best evidence of this is that although the Internet is under attack constantly—thousands of times a day—it has yet to fail. The owners and operators of the Internet, primarily the major private sector players are doing a terrific job managing the defense.

Major independent surveys, such as the PricewaterhouseCoopers "Global State of Information Security"—the largest study of its kind—have indicated that those entities that follow approved best practices of information security show a remarkable ability to fend off attacks, recover from attacks and even deter attacks.

The problem is that as the Internet continues to grow we need more entities to embrace these practices and technologies while also working with us to develop new ones.

The critical question is: how precisely can we create such a system, if the models we have used for previous technologies are inadequate?

The best mechanism to assure an adequate and sustainable defense system is to inject market incentives to motivate the adoption of best practices.

That has been the mantra of the Internet Security Alliance, and The National Infrastructure Protection Plan officially embraced the need for a government supported market based incentive program stating that the "Government can. . .[create] an environment that supports incentives for companies to voluntarily adopt widely accepted sound security practices."

Fifth, there is a concrete proposal for moving forward.

The ISAlliance has long campaigned for the development of a publicly supported market based incentive program to bridge the gap between a regulatory and pure volunteer approach.

ISAlliance believes that the Federal government should advance homeland security preparedness through reliance on existing published standards *and best practices,* and defer to the private sector to continue to invest in and develop appropriate general and industry-specific standards for improved security.

Fortunately, there exist a number of paths, most with Congressional precedent, for Congressional action to provide incentives that are in the national interest. Among these paths are:

1. Congress can use its market power, instead of its regulatory power by more prominently including security, along with cost into its procurement process.
2. Congress can lead by example by fully funding federal agency needs for cyber security and integrating security compliance into personnel evaluations along with other HR criteria
3. Congress can tie incentives such as civil liability safe harbors such as those provided in the Safety Act, or provide procurement credits to companies who can demonstrate compliance with market generated best practices for cyber security;
4. Congress can stimulate the stunted cyber insurance market by temporarily sharing the risk of a massive cyber-hurricane until the market is sufficiently large to take the risk themselves.
5. The Congress can create an industry/government/university consortium to stimulate the needed research, development and adoption of security protocols,

similar to the Sema-Tech model used in the late 1980s to address the computer chip gap.

6. The Government can create awards programs similar to the "Baldrige Awards" for quality which eventually became a sought after market differentiator for corporations.

Earlier this year the Board of Directors of the Internet Security Alliance met and approved an outline for a legislative approach we offer for your considerations which we call the "Cyber-Security Safety Act of 2007." I spend the balance of my statement further detailing our thoughts on how the Saftey Act can be used as a model for improved cyber security.

We do not come to the Committee with legislative language which we are endorsing, but rather with a set of concrete policy proposals we urge the Congress to work with us on perfecting.

We believe the "Cyber Safety Act" offers a coherent approach which will create specific Federal support for a package of incentives that will affirmatively encourage private sector investment in improved security and protection of the Internet. I would like to use the remainder of my testimony to outline he specific incentive recommendations and offer a brief analysis in their support:

- Establish a mechanism which will enable companies that adopt standards-based information security programs or best practices to be qualified to receive the specified incentives ("Qualified Companies").

The availability of incentives requires some type of baseline as a criterion to be met for the incentives to be available. The ISAlliance has long advocated that private sector standards and best practices are already in place that can be adopted by DHS as a basis for incentives.

- Create, in connection with privacy reform legislation (such as uniform breach notice laws), a Federal limitation of liability for Qualifying Companies that would limit their liability for breaches that occur, notwithstanding their use of standards-based security and best practices.

Information security is closely associated with privacy protection. Many companies otherwise eligible to be Qualified Companies have large volumes of personal information requiring protection under various Federal and state laws. Those companies will not be motivated to move forward with their cyber-security investments if they still are exposed to liability when breaches occur notwithstanding good security practices. As a final piece of the litigation-related incentives, this incentive eliminates the inhibitor of continued privacy-related liability for Qualifying Companies.

- Establish Federal Acquisition Regulations (FARs) and other legal frameworks through which private sector companies do business with the United States government that:

  Require the agencies to specify published standards and best practices as required elements for any contract relating to information security, data protection or similar services.

- Qualified Companies should be able to acquire additional cyber-security insurance to cover losses arising from CINS-related catastrophic events, and limit their liability to third-parties to the amount of that insurance. The amount of the insurance acquired must be reasonable in order to qualify for the limited liability.

Many companies defer investments in improved security out of a concern that, even with improved security, they are not protected from liability for losses that occur despite the quality of their security controls. Businesses are encouraged to invest in becoming Qualified Companies when they are offered the protection that is provided by (a) assuring the availability of insurance to cover losses from CINS-related catastrophic events and (b) limited their liability to the amount of insurance that has been obtained.

The principles of limiting liability to encourage improved homeland security are similar to the structures used to incent new homeland security technologies under the SAFETY Act which was enacted as part of the Homeland Security Act of 2002.

- To support the preceding insurance market, the Federal government should create within DHS a national program for temporary, short term reinsurance, through which insurers may purchase reinsurance coverage for their exposure to CINS-related catastrophic losses under policies issued to Qualified Companies.

Insurance carriers have been reluctant to create a vigorous marketplace for cyber-security insurance. The chief reason is that the insurance companies lack sufficient experience with cyber-terrorism to effectively evaluate the overall risks in order to determine effective premium levels, particularly for CINS-related catastrophes.

The proposed establishment of a reinsurance program provides underwriting for the insurance companies. In the event losses are incurred by the purchasing insur-

ance carrier is greater than their reinsurance deductible, the insurer would be entitled to coverage under the reinsurance agreement with the Federal program. The program administrator would have the right to increase future reinsurance premiums as deemed necessary to accomplish a revenue neutral goal. Over time, the program could be sunsetted as the insurance market gains experience with cybersecurity coverage. This solution is similar to Federal legislation that enhances the airline transport industry.

- Qualified Companies with appropriate insurance will also have litigation-related incentives available, excluding liability for consequential and punitive damages and limiting their liability for non-economic losses.

  Similar to the incentive provided by a limitation on losses to the available insurance, the limitation of liability for consequential and punitive damages, and limited liability for non-economic losses removes a serious inhibitor to information security investments—i.e., the risk of losses for which responsibility is assigned notwithstanding a company's good faith investments in adequate information security. Eliminating that inhibitor encourages a more secure preparedness, company-by-company.

  On many occasions, the Federal government has employed its influence as a major purchaser from the private sector to encourage companies to develop and implement improved business practices. Establishing criteria tied to providing services to the government offers new market opportunities to Qualified Companies and, in doing so, provides strong economic incentives to improving their cyber-security.
- Establish a "Baldrige Award" for information security quality and excellence, coordinated with specific industry organizations to develop and create awareness of information security as a competitive differentiator.

  The Malcolm Baldrige Award by the US Department of Commerce has become a cherished recognition of excellence in the marketplace. A similar program, perhaps recognizing information security excellence within industry sectors, will greatly increase awareness of the value of information security and its function as a competitive differentiator, thereby encouraging new investments.
- Create and fund an industry/government/university consortium to stimulate the needed research, development and adoption of security protocols that can, in turn, stimulate improved technologies for adoption across the private sector and government computer systems.

In the late 1980's, the Federal government provided matching funding to create an industry-government cooperative consortium that collaborated in accelerating solutions to common manufacturing problems in semi-conductor production (SEMATECH). This successful model revitalized the U.S. semiconductor industry and continues to generate industry leadership and innovation long after Federal funding was voluntarily terminated by the consortium.

A similar program today will enable government, academia and industry to work together to replace today's security poor Internet protocols with security-rich protocols. Those protocols can enhance the quality and integrity of the hardware devices, switches and other components from which the Internet is constructed.

Mr. LANGEVIN. Thank you, Mr. Clinton.

Mr. LANGEVIN. And the Chair now recognizes Dr. Gordon to summarize your statement for 5 minutes. Welcome, Dr. Gordon.

**STATEMENT OF LARRY GORDON, ERNST & YOUNG, ALUMNI PROFESSOR, MANAGERIAL ACCOUNTING INFORMATION ASSURANCE, ROBERT H. SMITH SCHOOL OF BUSINESS,**

Mr. GORDON. Chairman Langevin, Chairwoman Jackson Lee. Thank you very much for inviting me here. My comments are going to focus on how to improve cybersecurity investments within the private sector. I am going to concentrate on four points which are all detailed in my testimony that I wrote up and submitted already.

But before I talk about these four points, let me just mention two things. One is that in the private sector, efficient allocation of resources is fundamental, and the reason that is fundamental is because that leads to profits, and profits leads to increasing the value

of the firm. And increasing the value of the firm is a key concern to all senior executives in the private sector.

The second point I want to make is that investments in cyber computer compete with other investments. And I think that is also fundamental to keep in mind.

With that said, let me go to my four points. The first point I want to make is that the best, the strongest incentive by far is to have the private sector recognize that it is in their best interests in terms of increasing the value of the firm to increase investments in cybersecurity.

There is a well-established process among business people for looking at efficient allocation of resources. That often is a concept that falls under the umbrella of what we sometimes call making the business case. Making the business case is the notion of using a well-established metric cost benefit analysis. There are various models of cost benefit analysis. And actually looking at alternative investments, rank ordering them, and then allocating their resources.

So my first point is that in order to get business people to invest more in cybersecurity, what you want them to do is to recognize the importance of efficient allocation of resources toward cybersecurity investments. In other words, it is an internal incentive. It is a business incentive.

Now, one of the problems in this regard is that the people who are often arguing for cybersecurity investments, the CIOs, the chief security officers, their training is primarily in technology what you might call computer security. And many of them, at least traditionally, have not been well versed in the notion of how to make the business case. So let me give you a little real world story.

About 5 years ago, I was approached by the chief security officer for a Fortune 500 company, and he came up to me and said—he met with me for lunch, and he was all upset because he met with his CFO for his company and he asked for a $10 million upgrade to the network, the security of the network for that company. And the CFO said to him: Where is your business case?

So when he came to me and we discussed it at lunch, he said: What's wrong with the CFO? Doesn't he understand the importance of security? And my immediate reaction was: If I were the CFO, when you left the room I would probably be saying, what's wrong with you? Don't you understand the importance of economics? If I give you $10 million to upgrade the security.

I am essentially taking away from something else. And the name of the game for the private sector is, generating profits so that what you can do is you can increase the value of the firm. And when you talk about cybersecurity investments, it is what we call in capital budgeting a cost savings project. And what you really want to do when you are in a private sector is not only save costs, but equally if not more important is increase revenues. In other words, there is two ways to increase profits. You can increase revenues, save costs.

And when you talk about cybersecurity investments, one of the big problems, this is my second point, is estimating the benefits which are really cost benefits here, what you are really talking about is estimating the cost savings. And the cost savings are par-

ticularly tough to estimate for two reasons. One is a big chunk of the cost savings really come from, if you have a cybersecurity breach what you have here is you lose customers and so a big chunk of those cost savings come from avoiding lost customers. And a second big chunk of those cost savings come from the notion of potential liabilities. And these are two very tough things to measure. And in order to measure them properly, you have got to take into consideration risks, the risks associated with the breach.

And there are different notions of risk. There is a well-established body of literature in economics and finance and in insurance which has all kinds of metrics for measuring risk. These metrics have not been well integrated into the cybersecurity literature. You don't have to go out and discover new metrics. They are there already. So that is my second point.

My third point is that when you talk about cybersecurity, you have got another unique kind of issue and that is you have got what we call spillover effects, or in economics we call it externalities. And these externalities really relate to the fact that a big chunk of the costs associated with cybersecurity are private costs, costs associated to a private company. But also, another large share of these costs we call social costs. And these social costs, this is where government incentives become important. These social costs are costs that are borne by other companies, not the company that is not practicing cybersecurity.

And my last point that I want to make relates to Sarbanes-Oxley Act, or affectionately known as SOX. One of the things that recent research has shown is that SOX actually has as a side effect increased the cybersecurity activities of firms. It was, seems to me, unintended. Part of SOX requires that corporations improve their internal controls systems. There is no way an internal control system can be improved if you don't have strong security. And what has happened since SOX has gone into effect, research has shown that corporations are increasing their security activities.

I would suggest that in respect to all four of these points, that this committee and the Department of Homeland Security can do several things to improve cybersecurity investments. First, my first recommendation would be to set up some kind of workshops associated with making the business case for cybersecurity investments. That is the first thing.

The second thing is that we need more research in looking at how do you actually determine the benefits associated with cybersecurity investments.

Third, we need to look at the kinds of incentive plans that governments set up related to these externalities, these social costs.

Now, lots of people talk about tax credits, and that is certainly one option. Another option, one that I probably think should be looked at more carefully, is maybe the government needs to set up tough security standards. Now, you can do this by regulation, but I would recommend something different. I might recommend setting up tough security standards, and alongside of those is basically give preferential treatment on government contracts to those companies that comply with those standards. So you are giving them an economic incentive to comply with those standards.

And the last point I want to make is I think this committee and DHS should take a close look at the relation between cybersecurity activities at firms and Sarbanes-Oxley Act. I think what you will find is that a lot of good things are coming out of that that actually relate to your concern with improving cybersecurity in the private sector.

Thank you for giving me this opportunity, and I will be glad to answer any questions you have related to my comments.

Mr. LANGEVIN. Thank you, Dr. Gordon, and I thank the panel for their testimony.

[The statement of Mr. Gordon follows:]

***Incentives for Improving Cybersecurity in the Private Sector: A Cost–Benefit Perspective***

PREPARED STATEMENT OF DR. LAWRENCE A. GORDON

(***http://www.rhsmith.umd.edu/faculty/lgordon/***)

Thank you for inviting me here today to talk about economic aspects of improving cybersecurity in the private sector. I commend the members of the Subcommittee for focusing on this critical and complicated issue.

**Introduction**

My comments today will center on ways of encouraging (i.e., providing incentives for) investments that are directed at improving cybersecurity in profit-oriented organizations operating in the private sector. However, much of what I have to say would also apply, with some modifications, to non-profit organizations (in both the private and public sector). My comments are based on an ongoing stream of research on "economic aspects of cyber/information security" that I (along with several colleagues) started in 1998. Part of this research has already been published, as indicated in the reference section at the end of this testimony.[1]

A key concern among profit-oriented organizations is efficiency. This concern is usually thought of in terms of facilitating the generation of profits (i.e., the difference between revenues and costs) for the owners of an organization, with the ultimate goal being to increase the value of the organization. **Indeed, the most powerful incentive for an organization in the private sector to invest in cybersecurity activities is the motivation to increase the organization's value to its owners.** For a publicly traded profit-oriented corporation, this value proposition is usually (or at least primarily) thought of in terms of increasing the stockholders' value.

At the heart of implementing this stockholders' value proposition is the notion of cost-benefit analysis. "*Cost-benefit analysis* compares the costs of an activity to the benefits of that activity, thereby focusing attention on the process of efficiently allocating scarce resources among competing activities. In the context of cybersecurity, the cost-benefit analysis principle means that managers need to compare the costs of an additional information security activity with the benefits derived from that activity" (Gordon and Loeb, 2006, p. 20–21). When the benefits exceed the costs, the value of the organization will increase. **Thus, in considering a decision to increase spending on cybersecurity activities, it is important that the organization believe that the benefits will exceed the costs.**

A fundamental assumption underlying the above concept of cost-benefit analysis is the fact that organizations have scarce resources that need to be allocated to competing activities, including cybersecurity activities. In other words, cybersecurity activities are competing with other organizational activities (e.g., new product development, R&D, merger and acquisition decisions, fringe benefits for employees, etc.). If an organization invests more in cybersecurity activities, that means less will be available for other initiatives (i.e., organizations have finite resources to invest in competing projects). Accordingly, it is important for profit-oriented organizations to be able to argue that cybersecurity investments represent a more efficient allocation of organizational resources (on a cost-benefit basis) than if such resources were put to an alternative use (e.g., developing a new product). In the vernacular of business, this means it is important to be able to **"make the business case"** for investing

[1] Given the limited nature of this testimony, many facets of the above noted stream of research are not directly addressed in this document (e.g., cybersecurity risk management).

VerDate Nov 24 2008 08:44 Dec 16, 2009 Jkt 000000 PO 00000 Frm 00090 Fmt 6633 Sfmt 6621 H:\DOCS\110-HRGS\110-82\48977.TXT HSEC PsN: DIANE

in the cybersecurity activities. Generally speaking, there is a well established process for making the business case for an investment, including investments in cybersecurity activities. Figure 1 provides a diagram of that process.

As indicated in Figure 1, **making the business case** starts with specifying the cybersecurity objectives for the organization. Next, various alternative investments for achieving the cybersecurity objectives need to be identified. Once the alternatives have been identified, the data associated with each alternative needs to be specified and analyzed. The next step is to conduct a cost-benefit analysis and to rank the various investment alternatives, followed by the allocation of resources to particular cybersecurity investment(s).[2] The final step in the business case framework is to conduct a post-audit of the investment decision (i.e., evaluate the effectiveness of the cybersecurity investment decision).

Unfortunately, making the business case for cybersecurity investments is often more difficult than making the business case for many other investments. There are at least three separate, albeit related, aspects to this added difficulty. First, the benefits derived from cybersecurity investments are especially difficult to assess. Second, the risks associated with cybersecurity investments are also especially difficult to assess. Third, there are *externalities* (spill-over effects) associated with cybersecurity investments. A brief discussion of each of these concerns is provided below.

In addition to the benefits, risks and externalities associated with cybersecurity investments, there are two other items that are important to any discussion of improving cybersecurity investments in the private sector. These two additional items concern the total amount to spend on cybersecurity activities and the Sarbanes-Oxley Act of 2002. A brief discussion of both of these items is also provided below.

**Benefits Derived from Cybersecurity Investments**

The first difficulty associated with cybersecurity investments has to do with identifying and estimating the benefits derived from such investments. The primary benefits associated with cybersecurity investments are the future "cost savings" derived from the prevention of losses due to cybersecurity breaches.[3] However, if breaches were prevented, the actual losses would not occur and therefore would not be observable. In fact, the better the security, the less an organization will observe the losses resulting from cybersecurity breaches. Thus, organizations need to estimate the potential losses from cybersecurity breaches in order to estimate the benefits derived from cybersecurity investments. These estimates can be based on past experiences, where such experience exists.

**A fundamental problem in coming up with estimates of the benefits derived from cybersecurity investments is that the most important potential losses are due to unobservable lost customers resulting from cyber breaches and the potential liabilities associated with cyber breaches.** In fact, as shown in the Campbell et al. (2003) study, these costs can be staggering.[4] Unfortunately, even when organizations have data upon which to estimate the explicit losses associated with detecting and correcting past breaches, they rarely have data upon which to estimate the implicit losses associated with lost customers and the potential liabilities.

One way of addressing part of the problem discussed above concerning estimates of the benefits of cybersecurity investments is to take a "wait-and-see" approach to such investments. As pointed out in the Gordon, Loeb and Lucyshyn (2003a) study, this wait-and-see approach is consistent with the "real options" (more specifically, the "deferment option") approach to capital budgeting. Of course, as the name suggests, it also means that it is often best to defer certain investments in cybersecurity due to the problems associated with estimating the potential benefits.

The fact that the benefits derived from cybersecurity investments are essentially "cost savings" raises an additional issue not discussed above. That additional issue has to do with the fact that most corporate executives would prefer to increase profits by increasing revenues rather than by decreasing costs. The reason for this preference is due to the fact that the stock market tends to reward the owners of firms for growth as well as efficiency. Thus, in competing for funds, cybersecurity investments have a built in bias against them relative to "revenue generating" projects.

---

[2] For a detailed explanation on the mathematics underlying cost-benefit analysis, based on discounted cash flows, see Chapter 2 of Gordon and Loeb (2006).

[3] It can also be argued that cybersecurity investments can create a competitive advantage for an organization, which in turn translates into potential benefits. Although this argument is correct, such benefits are generally considered to be secondary in relation to the potential cost savings from such investments.

[4] The Campbell et al. (2003) study also shows that many cybersecurity breaches are not statistically significant, in an economic sense.

**Risks Associated with Cybersecurity Investments**

The second difficulty associated with cybersecurity investments deals with the risks (or uncertainty) associated with such investments.[5] It is important to recognize at the onset that 100% security is rarely feasible in a technical sense, and certainly not cost-beneficial in an economic sense. Thus, it is important to realize that cybersecurity investments are intended to reduce the risk (i.e., probability) of cybersecurity breaches. However, determining the reduction in the probability of a particular breach taking place, let alone a string of breaches taking place, as result of a cyber investment is extremely difficult to estimate. Nevertheless, in estimating the benefits from cybersecurity investments it becomes necessary to associate those benefits with the probability of the occurrence of security breaches. In other words, the "expected" cost savings (i.e., expected benefits) from cybersecurity investments are actually derived by multiplying the potential cyber losses by the difference between the probability of the cyber security losses occurring prior to the cybersecurity investment and the probability of the cybersecurity losses occurring after the investment.

Not surprisingly, estimating the before and after probabilities associated with cyber losses is more an art than a science. Thus, many have argued that the entire process of trying to estimate the expected benefits derived from cybersecurity investments is nothing more than an academic exercise. **However, the fact that it is difficult to estimate the risk (uncertainty) associated with cybersecurity breaches should not be used as an excuse for avoiding the determination of such estimates.**

Another aspect of the risk associated with cybersecurity investments deals with the definition of the term risk. In the cybersecurity literature, risk is usually associated with the expected loss from security breaches (i.e., the sum of the product of potential losses multiplied by the probability of such losses). The goal of reducing the risk of a cybersecurity breach, according to this definition of risk, is to reduce the expected loss. However, there are other important notions of risk that should be of interest to those responsible for allocating cybersecurity investments. For example, reducing the variance (i.e., variation) of the potential losses is another valuable facet of risk when discussing cybersecurity investments.[6] Although beyond the scope of the testimony being submitted today, it should be noted that one way for an organization to reduce the risk associated with cybersecurity breaches is to invest in cybersecurity insurance (see Gordon, Loeb and Sohail, 2003).

**Externalities Associated with Cybersecurity Investments**

The third difficulty associated with cybersecurity investments relates to the externalities (i.e., spillover effects) associated with such investments. **These spillover effects are largely the result of the inherent interconnectivity associated with computer networks.** In other words, the security of a computer network—particularly the Internet—depends on the actions of all users of the network. This creates a problem in the following sense. When a firm invests in information security activities in an effort to improve its cybersecurity, it bears all the costs, but does not reap all the benefits. The larger the share of the benefits that accrue to other firms, the smaller the incentive for a firm to increase its investments in cybersecurity activities. This may result in the firm, and hence society, under-investing in information security. While the government could, in principle, counteract this tendency by creating incentives for information security investments (for example, by offering tax credits for such investments), the government currently does not know the right level of incentives to provide.

The externalities associated with the Internet have resulted in all sorts of efforts to coordinate cybersecurity activities on both a national and international level. The ISACs (Information Sharing Analysis Centers) and the US–CERT (United States Computer Emergency Response Team) are two good examples of efforts to coordinate cybersecurity activities. Both of these efforts rely heavily on information sharing related to computer security, with particular emphasis placed upon protecting the nation's critical infrastructure.

Information sharing has the potential for lowering the cost of cybersecurity for each organization involved in such a program. Unfortunately, the free-rider problem (i.e., the situation where each member of a group shares a little amount of informa-

---

[5] In the early economics literature, a distinction is sometimes made between the terms *risk* and *uncertainty* (see Gordon and Loeb, 2006, p. 96). For purposes of this testimony, no such distinction is made.

[6] The expected loss and reducing the variance of potential losses are only two of the different concepts of risk that could be considered in the context of cybersecurity investments. For a further discussion of various risk concepts applicable to cybersecurity investments, see Chapter 5 of Gordon and Loeb (2006).

tion, in the hope of learning a lot about the other members of the group), is prevalent among information sharing arrangements related to cybersecurity (see Gordon, Loeb and Lucyshyn, 2003b). Thus, unless economic incentives are devised to offset the free-rider problem, much of the potential benefit from information sharing organizations will not be realized.

**How much in Total should be Invested in Cybersecurity Activities?**

The cost-benefit framework discussed above provides a straightforward way of assessing the benefits and costs associated with incremental investments in cybersecurity activities. If we assume that an organization already has in place some initial level of cybersecurity spending, then the total spending on cybersecurity activities would be this initial spending plus the sum of incremental investments. A more sophisticated approach to deriving the right amount to invest in cybersecurity activities is to assume a zero-base starting position for such investments. In its most rigorous form, a mathematical model can be developed to derive the optimal amount an organization should spend on cybersecurity activities. Although cost-benefit analysis would be embedded within such a model, an optimization approach would be a far more sophisticated (in terms of the mathematics) approach to deriving the right amount to invest in cybersecurity. This model should involve specifying security breach functions, the potential losses associated with security breaches, the probability of such losses, and the productivity of cybersecurity investments.

One model for deriving the optimal amount to invest in cybersecurity activities, which has gained wide acceptance among academicians and many practitioners, is referred to as the **Gordon-Loeb Model.** This model is described in the paper by Gordon and Loeb (2002). It must be emphasized, however, that the Gordon-Loeb Model is best viewed as a "framework" for examining the optimal level of spending on cybersecurity, rather than as an absolute solution to the cybersecurity investment dilemma. Indeed, in the final analysis, determining the right amount to spend on cybersecurity activities requires sound business judgment (based on experience and knowledge related to a particular firm and industry), as well as the application of sound economic principles. In other words, in the final analysis, there is no silver bullet for deriving the right amount to spend on cybersecurity.

Since cybersecurity investment decisions are made based on expectations of the future, the likelihood of getting the optimal solution to the investment problem is close to zero. However, it is important to realize that on average an organization would be better off by utilizing sound economic principles in making cybersecurity investment decisions than ignoring such principles.

**Sarbanes-Oxley Act has Created an Incentive to Increase Cybersecurity Activities**

The accounting scandals of the late 1990s resulted in the Sarbanes–Oxley Act (SOX) of 2002. A key aspect of this legislation deals with the internal control requirements of SOX under Section 404. In essence, SOX requires firms registered with the U.S. Securities and Exchange Commission to develop sound internal control procedures associated with financial reporting. Given the computer-based nature of modern organizations, it is generally agreed that sound internal controls implies sound information security. Thus, as shown by Gordon, Loeb, Lucyshyn and Sohail (2006), an indirect result of SOX has been to create an incentive for firms to increase their information security activities (and by implication, investments) by firms. **In essence, research suggests that SOX has created a strong incentive for organizations to increase their cybersecurity investments.** Although the above claim has not been directly tested, the findings by Gordon, Loeb, Luchyshyn and Sohail (2006) clearly point to the validity of this claim.

**Summary and Recommendations**

The above discussion highlights several key aspects of investments directed at improving cybersecurity within profit-oriented organizations operating within the private sector. These aspects can be summarized in terms of the following five points.

**1. The most powerful incentive for an organization in the private sector to invest in cybersecurity activities is the motivation to increase the organization's value to its owners.** At the heart of implementing this value proposition is the concept of cost-benefit analysis, which falls under the umbrella of **"making the business case"** for cybersecurity investments. The idea of deriving an optimal level of investment in cybersecurity activities is closely associated with this cost-benefit concept. Unfortunately, many (if not most) CIOs (Chief Information Officers) and CSOs (Chief Security Officers) are not well versed in the economic underpinnings of cost-benefit analysis. Accordingly, it is often difficult for those responsible for cybersecurity activities within a firm to make a cogent argument for increasing the firm's spending on such activities.

Remember, an increase in spending on cybersecurity activities generally means that less is available for spending on other initiatives (including revenue generating initiatives) within the organization. Thus, my recommendation is for this Subcommittee to initiate an effort to establish training sessions for CIOs and CSOs on how to apply cost-benefit analysis to cybersecurity investment decisions. The development of these sessions could fall under the auspices of the Department of Homeland Security. In my opinion, such training would go a long way toward improving the allocation of private sector resources toward cybersecurity activities.

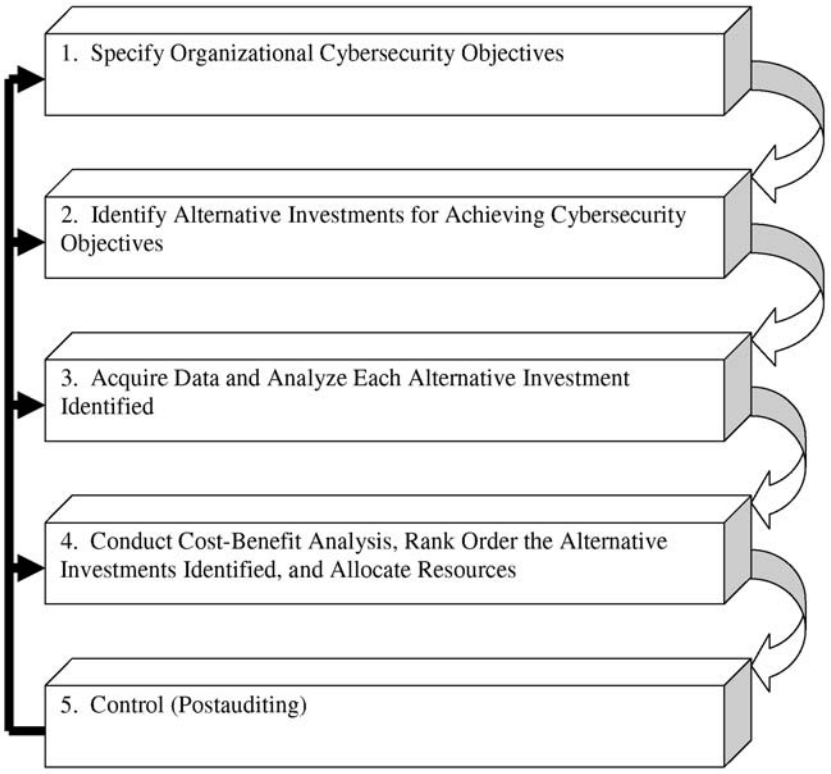
**2. A fundamental problem in coming up with estimates of the benefits from cybersecurity investments is that the most important potential losses are due to unobservable lost customers resulting from cyber breaches and potential liabilities associated with cyber breaches.** Until organizations feel more comfortable with their estimates of the benefits from cybersecurity investments, it is unlikely they will make the necessary commitment to such investments. In other words, the tendency will be to treat cybersecurity investments as a necessary evil rather than sound economic investments. Thus, my recommendation is for this Subcommittee to encourage, under the auspices of the Department of Homeland Security, additional research related to estimating the benefits of cybersecurity investments.

**3. The fact that it is difficult to estimate the risks associated with cybersecurity breaches should not be used as an excuse for avoiding the determination of such estimates.** The risks associated with cybersecurity are difficult to estimate. As a result, many view the process of deriving the "expected benefits" from cybersecurity investments as merely an academic exercise. However, there is an extensive body of existing literature on risk that has direct bearing upon cybersecurity investments. To date, this literature on risk has not been well integrated into the cybersecurity literature. Thus, my recommendation is that the cost-benefit analysis training sessions suggested in the first point above should include coverage of this literature on risk.

**4. The inherent interconnectivity associated with computer networks creates externalities (spillover effects).** These externalities revolve around issues related to welfare economics (i.e., a branch of economics associated with improving the welfare of an entire society or economic system, usually based on such principles as the efficiency of resource allocations and equitable income distribution to individuals). Since it is difficult to get organizations to incorporate these externalities into their decisions regarding cybersecurity investments, the development of exogenous government incentives may be appropriate. Thus, my recommendation is for this Subcommittee to encourage research directed at examining the appropriateness of developing incentives to address these externalities.

**5. Research suggests that the Sarbanes–Oxley Act of 2002 has created a strong incentive for organizations to increase their cybersecurity activities.** The fact that there is preliminary evidence that SOX has created a strong incentive for organizations to increase their cybersecurity activities, and by implication their spending on such activities, is worth exploring in greater depth. Indeed, assuming these preliminary findings are correct, there may be ways for the Department of Homeland Security to capitalize on this development. Thus, my recommendation is for this Subcommittee to facilitate further exploration of this SOX-cybersecurity relation.

Figure 1: The Business Case for Cybersecurity Investments




Source: Gordon and Loeb, 2006 pp. 116 and 131.

**References**

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market." Journal of Computer Security, Vol. 11, No. 3, 2003, pp. 431-448.

Gordon, L. A., and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, Vol. 5, No. 4, November 2002, pp. 438-457.

Gordon, L. A., and M. P. Loeb, *MANAGING CYBERSECURITY RESOURCES: A Cost-Benefit Analysis*, McGraw Hill, 2006.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn, "Information Security Expenditures and Real Options: A Wait and See Approach." *Computer Security Journal,* Vol. 19, No. 2, Spring, 2003a, pp. 1-7.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn, "Sharing Information on Computer Systems: An Economic Analysis," *Journal of Accounting and Public Policy*, Vol. 22, No. 6, 2003b, pp. 461-485.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and T. Sohail, "The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities," *Journal of Accounting and Public Policy*, Vol. 25, No. 5, 2006, pp. 503-530.

Gordon, L. A., M. P. Loeb and T. Sohail, "A Framework for Using Insurance for Cyber Risk Management," Communications of the ACM, Vol. 46, No. 3, March 2003, pp. 81-85.

Mr. LANGEVIN. I now recognize myself for 5 minutes. And let me begin with you briefly, Dr. Gordon, on your point that one of the primary goals of a firm is to increase the asset value of the firm. But what about protecting the asset value of the firm? And why is it that that isn't more readily apparent as a need, in a sense a primary goal of doing business, right along with increasing value at the firm?

Mr. GORDON. I think both of those actually address the issue of increasing value, but I would put it in a slightly different context. I would say that in the capital budgeting literature, we talk about generic areas of capital investments. One is revenue generating products, new product development, mergers and acquisitions. Another one would be what we call cost savings projects. Cybersecurity investments fall under that category. The third category is what we often call must-do projects.

So the way I would answer your question is to say that when you get to these cost savings projects, it is much tougher. And when you get to cybersecurity investments they are the toughest. And the reason they are the toughest, it is much tougher to actually observe the benefits. And the reason for that is if you do the job right, then you have avoided those breaches, you have avoided those catastrophes, and you don't really see what you would have incurred as a cost.

So that is why they are particularly tough. And that is why, when you talk about protecting assets in that sense, it is a different kind of project. It is not that they don't add value to the firm. They do. It is just often harder for managers to figure out how to quantify it.

I am a big believer in that you should try to—you know, what you measure is what you get. You need metrics. And after you come up with these, I look at these metrics as a framework. Once you get those, then of course you have got to bring in good business judgment, nonfinancial concerns, nonquantitative concerns. But there is a well established process for doing that. So what you have to do is go through and estimate these benefits.

Mr. LANGEVIN. You have each had the opportunity to hear each other's testimony. Let me just go down the line and ask, was there anything that you heard in the other testimony of your fellow panel members right now that struck you that you highly agree with or strongly disagree with?

Ms. KATZEN. On the basis of both the oral statements and the written testimony which I had read, I think we are in violent agreement. We all seem to believe and advocate that necessity for getting good metrics, good data, good research; that the government should not be regulating; that one size does not fit all; that it is not an IT problem, that it is an enterprise-wide problem. That there are business cases involved, and that there should be market-based incentives, with the government holding out some additional incentives to bring the companies to the table. And I don't hear very much difference among us.

Mr. CLINTON. I would have to agree with Ms. Katzen. I am struck very pleasantly by the degree of agreement with regard to what is the best way forward for Congress. And it is for Congress to act, but for Congress to act in a novel fashion.

Professor Gordon's testimony, which I think is probably pretty difficult to summarize orally, although I think he did a wonderful job with it, goes into really good detail on why it is very, very difficult for real corporations to justify the sort of extraordinary expenses that we would like to have them make for security that goes beyond their corporate borders. That is just not going to happen.

For about 6 years, we have been hearing rhetoric from DHS and others saying, well, gee, if industry would only get it and realize the value proposition is there for them to protect their own resources, then that would take care of it. That has not happened. The amount of spending has not increased dramatically. It is not going to increase dramatically unless we develop a market for this. Now, that is an unhappy solution, but I don't see how we can come to any other realistic solution. There are a range of things.

One of the things we haven't talked about here is that virtually all of the ideas, and again most of us have articulated pretty much the same ideas, use procurement better, use awards programs. You know, based on standards. You know, most of the standards are already there in the private sector. We already know a lot about how to do this. We are under attack thousands of times a day. We are preventing lots of them. We just need more people to adopt these things.

So we don't need the government to come in and provide standards. We don't need the government to come in and regulate these things. We need the government to come in and provide incentives. And the sort of incentives that I have articulated in my testimony are incentives that have already been used in agriculture, in aviation, in the environmental sphere, in ground transportation, in tax law. The government has done this stuff before, they have just not applied it to cybersecurity. And that is what I would argue, is that if we would take the precedent that we have found in other sectors of the economy and the standards that have already been proven effective in mitigating the attacks that we are having every day, that is the payoff forward for improved cybersecurity, which is in the national interest.

Mr. GORDON. In general, I would agree with what my colleagues have to say here, although—and I hate to put an end to the love fest, but I see a different focus. And let me tell you the focus.

First of all, market-based incentives, they already exist. The clearest market-based incentive is to get firms to realize it is in their best interest in terms of cost efficiency to invest more in cybersecurity investments.

And the other point I would make is, so it is not that we disagree, but I am saying the focus to me is it is already out there. We have got to get firms to understand how to use that better, and I think that is something your committee could certainly facilitate.

The other point I want to mention is that I thought the point mentioned about Enterprise Risk Management, ERM, was really a good one. And so I appreciate the fact that it was mentioned. However, having done a lot of work in that area, let me tell you the problem with ERM. ERM comes from COSO, the Committee on Sponsoring Organization from the accounting organizations. And COSO talks about ERM in four categories. They talk about operations, they talk about financial reporting, they talk about compliance and strategy.

What they don't do is give you a metric for measuring it. And if you go and read this ERM literature, what you will find is and you need, in my opinion, is if you need a metric for measuring it. In fact, I have got a Ph.D. student who just finished up a dissertation working on this very topic. And when he came to me and wanted to do something on ERM, the first thing I said to him is, you realize you are going to have to come up with a metric. What we need is some kind of a metric for measuring have we improved it.

So it is not that I would disagree. I would just say the focus has to be on developing a metric for ERM. And so I don't think we disagree. It is just a question of focus. I tend to be more focused on the quantitative metrics.

Mr. LANGEVIN. My question for Mr. Clinton is, isn't it the case, though, that firms in the private sector when, in a sense creating standards, that they tend to create substandard standards?

Mr. CLINTON. No. I am not aware of any evidence of that. In my testimony, I cite the largest study that has been done on information security which, independent study, PriceWaterhouseCoopers study. And they found that the companies, the best practices group, the group they classified as following these things, were able to

mitigate against attacks better, didn't lose money like others did, and, in fact, could deter tax.

It is, as Professor Gordon has just alluded, companies do want to protect their own cyber systems. But the Internet transcends those cyber systems. If you read the discussion of externalities that is in Professor Gordon's testimony, I think he makes a really good argument here. Basically, what we need is for corporations that go to their own corporate borders for their own self-interests, to provide security that goes to the entire system. And that is—it is important to remember, there is no private sector. There is no thing that is the private sector. The private sector is thousands and thousands of different companies, with different goals, technologies, et cetera. We have to get all these guys to cooperate. They do cooperate. They set standards all the time to make sure their systems are interoperable, so that they can generate more investment, have cooperative engagements, et cetera, et cetera.

There is plenty of reason for them to set good standards. And the research indicates that when they follow those standards and best practices, we do have demonstrable improvements in cybersecurity. I am not going to say it is 100 percent, because the threat, as I also pointed out, continually evolves. So we need to continue to work on it.

But the evidence that I am aware of, with all respect, Mr. Chairman, is the opposite. Is that rather industry set standards adequate to meet their needs, and then attempts to meet those standards.

Moreover, one last point. One of the projects that we are involved in at the Internet Security Alliance is to develop model contracts around those standards, so that the really good players like Verizon who testified on the first panel—and they are doing a great job. They are just doing as good a job as you can do, I think, from what I can see. What they want to do and what we are working with them to do is to take their system and write contracts for their vendors, their suppliers, their customers, that include in those contracts compliance with the high-level security systems that Verizon is already having, so that we are using contracts to expand the perimeter of security rather than using regulation. And those contracts are much easier to update, keep up with the technology, keep up with the evolving threat, than going through a regulatory model which takes years. And, frankly, I think it is the regulatory model. You get a bunch of lobbyists coming in, they will dumb it down for you.

Mr. LANGEVIN. My concern is that the private sector would tend to skimp or to underestimate risk. We heard testimony last week on the electric grid, where the industry ostensibly self regulates through NERC that makes recommendations to FERC about the type of regulations that should be put in place. Yet, clearly the self regulation process in that instance doesn't quite go far enough. And I believe that a model similar to the Nuclear Regulatory Commission is stronger where they have the ability to come in and direct, as opposed to just allowing industry to kind of self-advise, self-regulate.

Mr. CLINTON. If I could respond quickly to the chairman. And I apologize for taking too much time. I wouldn't classify myself as an

expert in that particular sector. I frankly don't have any members in that particular sector. We are a cross-sector organization.

My sense would be that that is the sort of thing that we could work with. I can tell you that there are standards that have been shown to work. I am unfamiliar with the standards that they have. It would seem to me that the government, particularly in a regulated sector such as the one you are describing, certainly can use that.

But let me point out something that was not pointed out in the first panel, which is when GAO did their study, they found that the number one sector that had done the best job was completely unregulated, the IT sector. The banking sector, which is heavily regulated, did among the worst jobs.

So I don't think that there is a one-to-one correspondence here with respect to regulated/unregulated in terms of doing a good job in this area. I think what we need to do is find a set of standards that we would agree on meet certain metrics. No disagreement on that. And then find ways to get more companies to do that. But you have got to do it in a way so that you can keep up with the threat.

Ms. KATZEN. If I could. What I hear, though, is almost so obvious, that this is not easy on the ERM. There are lots of ERM models, and they have to be adapted in different ways. Cost benefit analysis, I have spent the last 10 years of my professional life of doing cost benefit analysis. It is not easy. There are ways of doing it and there is literature out there and it has to work.

The problem is the diversity of the corporate models, the diversity of corporate awareness, the differences in technical capabilities. You are not dealing with the monolithic world. Someone said there is no private sector, there is lots of components of a private sector. And this decentralized nature can be very offputting or frustrating.

But if you can't fix it, flaunt it. Use it. And that means don't look for a silver bullet. Don't look for a one-size-fits-all. Don't look for the perfect thing that would work in one sector to be applied in another, but apply sort of what comes naturally to each sector.

Thank you.

Mr. LANGEVIN. Thank you. The Chair now recognizes the ranking member.

Mr. MCCAUL. Thank you, Mr. Chairman. I appreciate everybody's patience. It is getting late, and we have got an anniversary, we have trick-or-treaters tonight. We convened at 2:30. It has been 4 hours. I would like to get more input in writing, if that would be acceptable. It is just getting a little late and I have got to run on to another obligation.

But what I am hearing is, and tell me if I am wrong. It sounds like, nobody here is advocating regulatory reform, but, rather, market-based incentives. Is that correct? Is that a fair statement, from all three?

Mr. GORDON. I think there is something in between. And the something in between is you can have government incentives, which is not necessarily regulatory in nature. For example, you could go to NIST and ask NIST to set up the standards for you for security, and you can reward companies. Companies that are following those standards, you might give them preferential treat-

ment with government contracts. I don't view that as regulation, but that is not straightforward market reform.

Mr. MCCAUL. Sort of the novel, Mr. Clinton, where you are talking about the novel creative approach would be to look at this through the government contracting process, to provide incentives through that process?

Mr. CLINTON. That is one way absolutely. Yes.

Mr. MCCAUL. What are some other market-based initiatives or incentives that can be used without regulation?

Ms. KATZEN. One of the ones that we talk about, and I think Mr. Clinton does as well, is a recognition and reward program modeled on the Energy Star, which we use to increase energy efficiency; and, have a Cyber Star program where there would be recognition if you set the bar high enough and you require them to keep increasing their security.

Another of the workshops that I think we are all talking about, whether it is to educate for how to use or do a risk assessment or whether you are talking about how to use ERM, we are all talking about providing additional information. Not trying to hoard it, but to share it. And I think those kinds of incentives, whether the government picks up the cost of Federally-sponsored programs or gives tax credits for it are things that each of us have talked about in different ways, but somehow uses the Federal support for information sharing.

Those are just two ideas that I think all three of us have signed onto one way or the other.

Mr. CLINTON. Briefly, Mr. McCaul. In addition to what has been said, there are a number of things that can be done with insurance. Insurance is one of the strongest motivators that we use in health care, you know, good driving, et cetera, cetera, and there are a whole range of things that could be done with respect to insurance. As we have mentioned procurement, there are awards programs like the Baldrige Award. Make security a market differentiator, publicize that. There are creative consortiums like the Sema-Tech program that we did back in the 1980s. There are the contract systems that we use. As I said, there is at least a half dozen.

And I don't advocate tax incentives. I think the tax incentives would probably be a good idea, but IS Alliance lives in the world. We don't imagine that we are going to get tax relief for large corporations for security, even though I think it is a good idea. Politically, it probably isn't going to fly. But these other things ought to fly. We have done them, as I said, in a variety of other sectors. They passed. We really want to work with you on this.

Mr. MCCAUL. We have a Sema-Tech in Austin and that is a great model.

Just in the interest of time, because it is getting late. To the extent you can provide us additional information on what we can do at this level, what congressional action would be helpful to facilitate these incentives you are referring to; whether it be the contracting, whether it be the insurance, the information sharing? All these are great ideas that the chairman and I can look at in terms of crafting legislation that wouldn't be overburdensome in terms of regulating, but rather facilitating.

Mr. CLINTON. We have a good deal of material, Mr. McCaul, and we would be happy to share that with you and the Chairman and the rest of the committee and discuss it in greater detail at your convenience.

Mr. MCCAUL. I certainly appreciate that. Thank you.

Mr. LANGEVIN. And I agree. I look forward to seeing your recommendations as well.

The Chair now recognizes the chairwoman of the Transportation Subcommittee, Ms. Sheila Jackson Lee.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. To your ranking member, to my ranking member, and to the staying power of the witnesses, let me thank you for accepting our invitation to become fixtures in this place. But you are doing it well and we thank you very much.

Allow me to, I held up this large document that is the National Infrastructure Protection Plan. Let me just read into the record some language.

Protection includes actions to mitigate the overall risk to the critical infrastructure and key resources assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation or exploitation in the context of the National Infrastructure Protection Plan. This includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident.

And so we have our marching orders through this plan. And you are giving us sort of the wide perspective of the private sector. Can I get sort of a sentence answer from all of you, though this is cybersecurity? You heard individuals representing telecommunications and financial services on the first panel.

Do you believe that, overall, the private sector has been engaged in actions to mitigate the risk to these assets systems and networks? And do you think there have been sufficient incentives for them to do that? And as we do that, I will ask my next question of what more once I hear where you are on that question. Ms. Katzen. And welcome.

Ms. KATZEN. Thank you. It is very good to see you.

Ms. JACKSON LEE. It is good to see you. Put that on the record.

Ms. KATZEN. Thank you.

It is hard to know how much action has been taken because we have yet to develop meaningful quality metrics to measure. But one of the problems with the NIPP, the plan, is that it calls for information from the private sector, but you don't know what you are measuring against. We don't have benchmarks, we don't have metrics by which to make progress.

I think a lot of work is being done. And much of it must be productive, but I am not able to sit here and tell you that it is or it isn't as long as we have a lack of a real partnership. And this is what I was trying to say earlier. DHS has got to work in a public-private partnership, public-public partnership in a way that is respectful and exploits the trusted relationships that exist, and that provides the—and I will go back to the incentives—provides incentives for the private sector to do the right thing. Right now, I think they are more in a "do it my way" or dictate to the SSAs as or the

private sector what they should do, and I don't think that is as productive.

Ms. JACKSON LEE. Mr. Clinton.

Mr. CLINTON. Thank you, Madam Chairman. I would say, first of all, with regard to your first question, is the private sector engaged? Yes, many people in the private sector are; however, not nearly enough.

I participate on a number of these organizations. The outreach to the breadth of U.S. industry is, in my opinion, woefully inadequate. We need——

Ms. JACKSON LEE. When you say breadth, you are going beyond even the cybersecurity?

Mr. CLINTON. No, Ms. Jackson Lee. I am speaking within the context of cybersecurity. Frankly, I think that probably would be true beyond cybersecurity. We are not reaching enough people with respect to being involved in these various plans.

Ms. JACKSON LEE. DHS is not reaching enough people?

Mr. CLINTON. Yes. And with respect to do they need more incentives, I am afraid the answer is yes. Now, certainly, as Dr. Gordon has pointed out, there are incentives. Lots of people are doing a lot of good things. That best practices group I was referring to before that was found in the PriceWaterhouseCoopers found about 30 percent of corporations, many of the larger corporations. That is a lot of people, but that means 70 percent are not being reached. And when we deal with the Internet, the weakest link is the problem. So that if we have the small businesses or the commercial sectors not being engaged at all, they are intertwined with everybody else and they can help bring down the whole system. We need a much more expansive effort. And the only motivator that is going to be dynamic enough to work is the profit motive. We have to inject that in.

And you have got to remember, as somebody else pointed out before, it is not just a U.S. problem. The Internet is inherently international. So we need to reach out to the Indias and the Chinas and everybody else. We have to have some sort of system that is going to transcend that, and market incentives is the most logical one, which is why I think the three of us independently came to that conclusion.

Ms. JACKSON LEE. Mr. Gordon.

Mr. GORDON. I would say that the private sector is clearly engaged. Clear evidence of that is the growing importance of setting up a chief security officer apart from the chief information officer within a company. You have now most of your major corporations have someone in charge of security who may report to the chief information officer or may even report directly to CFO.

Are they doing enough? That is a tough one to answer, because in order to answer that one, you have got to really understand where they are and where they want to be. I can only give you my own experience, is I get contacted by at least one senior executive a week. And one of the biggest issues from a chief security officer's point of view is they want more security, okay, because not only is the company their concern but their job is their concern.

So they have the option, they have an incentive. There is an agency problem; that is what we call it in economics. They have an

incentive to overinvest. But the biggest problem they face is getting more funds out of the CFO for cybersecurity investments.

So a little side note here is if you take a look at what companies invest, all the studies tend to show that companies invest somewhere around 5 to 7 percent of their IT budget on security. And the interesting thing about that is that security is becoming one of the fastest growing concerns, and the percentage of the budget for security is not growing. So that would suggest to me that they are not getting the share they should be getting. It suggests that to me; but without having the deed on particular companies, and I am sure it varies from company to company.

Ms. JACKSON LEE. My questions are never quick, but I am going to try to offer two more quick questions recognizing your time and the lateness of the hour. But what I would ask without having that answered, I would like to get from the witnesses your list of incentives that can be utilized more effectively through DHS. And I would like that in writing. But let me try to get Mr. Clinton, and then I have a question for Ms. Katzen and Mr. Gordon.

You never were a fan in particular for the approach dealing with a regulatory scheme, if you will, I don't think. You were sort of interested in trying to, as you said, get DHS to be more enthusiastic on this best practices area. I am still looking at whether or not this should be a totally voluntary approach with incentives, or whether or not we need some regulatory structure, which I have heard my colleagues say and I too am looking at legislation along that line. I obviously have an array of infrastructure issues to look at.

But what I would like to know is what has been your association in terms of being involved with DHS to promote the best practices so that they are more broadly adopted across the IT sector through this program.

Have you been able to engage with DHS to talk about best practices? And I am just saying you in particular because you represent a component of the industry that I think is important. And, isn't this program a great way to encourage more effective cross-sector cybersecurity protection? Meaning this whole best practices. Have you been engaged in particular?

Let me ask my other question to both Ms. Katzen and Mr. Gordon. I think cybersecurity gives value to companies. And it would look like that would be one of the industry incentives that, if my investors knew that I was managing my risk, that that would make my product more valuable. Question is, does Wall Street give value to cybersecurity so that companies then are self-rewarded for what they have done? And, in essence, does the government? Have they narrowed the rewards to even that way? Cybersecurity, more valuable, protect the America's assets?

I will go to Mr. Clinton first on this whole best practices and interacting with the DHS.

Mr. CLINTON. Thank you, Ms. Jackson Lee. Yes. I, speaking as the Internet Security Alliance, am very involved.

Ms. JACKSON LEE. Is that the name of the program, so you will at least be—I will put it on the record. The Voluntary Private Sector Preparedness Certification Program.

Mr. CLINTON. Well, the Internet Security Alliance is very, very involved in developing best practices and finding incentives for our

Members to use them. We do have an insurance incentive program with the largest insurance provider of cyber insurance for our best practices. We publish best practices basically once every year. We talked earlier about the model contracts that we provide.

So we do on the private sector side a great deal with respect to developing best practices, providing incentives for best practices, et cetera. With respect to, is DHS the mode for that? I would have to tell you that we have not really found very much grounding in working with DHS in that regard.

Most of the improvements in cybersecurity that I am aware of happen by the private sector doing things through the private sector, not through DHS. Maybe that will change as DHS matures. But to this point, I would have to tell you that none of my members would say that they are doing anything to improve their security thanks to DHS. They are doing it for other reasons; some are for social, some are business, for a variety of other things.

But our view is that the infrastructure is owned and operated by the private sector. You have to work with the private sector to get it strengthened. When you strengthen that infrastructure, you are also fulfilling an important homeland security and national security function. But you do it through private sector. Going through DHS, I think you are really trying to stick a square peg in a round hole, and I think it is going to be counterproductive.

Ms. KATZEN. On the issue of both market value and Wall Street, and it is referred to in my testimony, the Ernst & Young study, which shows a very strong correlation between success in managing risks and success on Wall Street, and that investors do appreciate that. So I think there are data there that support that.

Mr. GORDON. I would agree with that. Actually, if you take a look at my written testimony, I discuss this notion of what you call value added as opposed to cost savings from cybersecurity investments. It is usually thought of as sort of a secondary effect, but in the short run firms certainly can carve out a niche for themselves, a competitive advantage of showing they have more security than another firm. In the long run, it will be hard to keep that competitive advantage. I do discuss that point in my written testimony.

Ms. JACKSON LEE. Thank you very much to all of the witnesses. And, Mr. Chairman, it has been a pleasure to be able to unveil and to pull back the covers on what has either been happening or not been happening with DHS. And I think that there are some roads not yet traveled that we can work on, in particular public-public, public-private relationships and incentives rewards.

Mr. Clinton, I don't want to leave DHS completely out and I am not convinced that they should be completely out or not, that they not be a regulatory structure. But I do believe that there should be rewards that you are aware of that are given through DHS, and apparently we have not established that structure yet.

Mr. CLINTON. I would agree with that, Ms. Jackson.

Ms. JACKSON LEE. And so, let me just thank Chairman Langevin. I look forward that we have an opportunity to work again together on this issue. And I yield back.

Thank you all for your testimony.

Mr. LANGEVIN. Thank you, Madam Chair. Let me just say how much I appreciate your participation in this joint hearing, as well

as Ranking Member Lungren. This was very productive, and some great things came out of it. I look forward to our continuing to work together.

I also, of course, want to thank the panelists for your patience, for your testimony. You have added great insight into the work that we have ahead of us and perhaps a road map of what we need to do to better coordinate this effort of cybersecurity and working together with the public and the private sector.

So I thank you for your testimony and the members for their questions.

The members of the subcommittee may have additional questions for the witnesses, and we would ask that you respond expeditiously in writing to those questions.

Hearing no further business—again, happy anniversary to you, Ms. Katzen. I hope you get home soon. And sorry for the lateness of the hour, but certainly an important issue.

Hearing no further——

Ms. JACKSON LEE. Happy anniversary.

Mr. Chairman, would you allow a moment of personal privilege?

Mr. LANGEVIN. Certainly.

Ms. JACKSON LEE. Professor Katzen goes back with my combined family.

My spouse, Dr. Elwyn Lee, he sends his greetings.

Ms. KATZEN. Thank you.

Ms. JACKSON LEE. And you allowed me a moment of reminiscing, and she is as young and vibrant. And I am apologetic. Go home for that anniversary, please. And greetings from myself and my husband. Congratulations.

I thank you for giving me a moment of personal privilege.

Mr. LANGEVIN. Certainly.

Ms. JACKSON LEE. The check is on Chairman Langevin, so do whatever you want to do tonight.

[Laughter.]

Mr. LANGEVIN. On that note, hearing no further business, the subcommittee stands adjourned. Thank you.

[Whereupon, at 6:53 p.m., the subcommittee was adjourned.]

## FOR THE RECORD

### PREPARED STATEMENT OF MICHAEL O'HANLON

Greetings. It is an honor to appear before the committee today.

My opening comments will be brief and rather broad. I am not an expert on cybersecurity, hence my contribution today will involve creating a framework within which this important aspect of homeland security can be considered and analyzed.

It is useful to think in terms of different possible strategies for homeland security. Clearly, in a society like ours, huge as it is, as open and free as it is, we could be far more diligent about protecting ourselves from terrorism than we are today.

For example, if the degree of terrorist threat here was anything approaching that in Israel, or if even a single additional major attack had been successfully carried out since 9/11, we would do things that are presently seen as politically infeasible or strategically unnecessary (such as searching baggage on most trains and buses, tightening up land borders far more, and worrying about truck bomb vulnerability at far more prominent buildings).

But we are already much more diligent than we were before 9/11, and are spending more than $50 billion a year in federal funds on the effort (whereas a decade ago we spent perhaps one fifth as much on counterterrorism, and did not even employ the term homeland security in the federal lexicon). So our current strategy might be seen as an intermediate one along a spectrum of possible approaches.

A notional list of a full spectrum of possible approaches to homeland security might look something like this, in ascending order of intensity and cost:

- Pre-9/11 Approach. The philosophy here would be to protect only against very specific threats that have manifested themselves before, or that would be especially worrisome. For example, we protected nuclear power plants from sabotage, and top officials from assassination. The annual cost to the federal government is under $10 billion for such an approach, roughly and notionally speaking.
- Post-9/11 Threat-Based Approach. This approach would follow a similar logic but expand the list of credible threats based on what we learned on September 11, 2001 and in various events around the world since then. Jeremy Shapiro of Brookings is a proponent of this approach (see opportunity08.org). Airline security is an obvious area of focus for this approach, which would emphasize prevention of what we know that al-Qa'ida and related groups CAN do, as opposed to what they might wish to do. Reducing our vulnerability to truck bombs at prominent sites is another logical area of emphasis, given known patterns of terrorist activity around the world. The annual cost is about $20 billion to $30 billion (my estimates).
- Bush Administration Approach. This goes beyond the threat-based approach to include as well attention to those types of attacks that we know al-Qa'ida would LIKE to carry out, as well as those that would be so horrible we have to worry that they might occur even if they probably will not (such as WMD attacks). Estimated annual cost $50 billion.
- Brookings Approach. This approach, reflected in two Brookings studies this decade by a team of authors, is similar in some ways to the Bush administration's concept. But it takes a slightly broader approach to defining threats and toughens up the steps taken to address them in some cases. We focus primarily on attacks that could cause major damage to our national security, our population, or our economy (catastrophic attacks). For example, we emphasize better protection of the chemical industry and the hazardous trucking industry, as well as improved use of intelligence to find patterns of possible terrorist attack before they occur (a "google function for counterterrorism") along the lines also proposed by the Markle Foundation. Estimated yearly cost $60 billion.
- "America the Vulnerable" approach. I borrow here from Stephen Flynn of the Council on Foreign Relations; former Bush administration homeland security official Clark Kent Ervin has written a somewhat similar book. The approach here is to take imagination to its logical extreme, and suppose that any serious attack al-Qa'ida might be able to carry out we should defend robustly against. It is a vulnerability-based approach, but with vulnerability defined in a broad way. Great attention is paid to inspecting cargo in international shipping by Flynn, for example, even though it could be very difficult to rework our port infrastructure to make this possible. Estimated cost $80 billion a year.
- Council on Foreign Relations task force approach. This Hart-Rudman task force of several years ago reflected the logic of Flynn, who was involved with the project as well, and also placed particular emphasis on equipping and training most of America's millions of first responders to deal with WMD attacks and other catastrophes. About $90 billion a year.
- Israel-style approach. If we had to worry about small bombs going off in most public places, a whole different level of effort would be required, with annual costs perhaps reaching $200 billion (and many inconveniences introduced to daily life).

This is a very short written testimony but I hope its succinctness will be of some use in providing a simple taxonomy for further discussion. I would be happy in particular to explain the Brookings approach, both in broad philosophy and in its specific recommendations.

I am attaching as an appendix a chapter in a recent Brookings book I coauthored in 2006. I have no reason to believe my coauthor's thinking has changed. However, given his current position, please assign responsibility for this "republishing" of material that first appeared a year and a half ago entirely to me.[1]

Appendix: Protecting Infrastructure and Providing Incentives for the Private Sector to Protect Itself

Since the attacks of September 11th, the private sector has generally not done nearly enough to improve its security against terrorist attack. For example, the Congressional Budget Office recently concluded that "there is relatively little evidence that firms have been making additional investments since September

[1] Micahel d'Arcy, Michael O'Hanlon, Peter Orszag, Jeremy Shapiro, and James Steinberg, *Protecting the Homeland 2006/2007* (Washington, D.C.: Brookings, 2007), pp. 73–95. ???

11 to improve their security and avoid losses."[2] About 85 percent of the nation's critical infrastructure is owned by the private sector, and security had typically not been sufficient before the attacks, so the failure to materially improve security measures in many key industries represents one of the most glaring and dangerous shortcomings in the nation's response to the terrorist attacks.

The key to improved security in the private sector is structuring incentives properly: Markets respond to incentives. But to date, the federal government has done little to alter firms' incentives for protecting most private sector infrastructure from terrorist attack. Apart from efforts to protect those types of infrastructure that have already been attacked, such as commercial airliners, the Administration's policy has been very restrained. Part of its reluctance to intervene may be a reflection of the admittedly daunting nature of the task—and the impossibility of knowing exactly which types of infrastructure to protect to what standards of robustness. But the Administration's laissez-faire approach also risks leaving undefended targets within the United States that could nonetheless cause catastrophic harm.

The greatest concerns apply to key pieces of private infrastructure—chemical facilities, skyscrapers, other large buildings, many hospitals, and so on. Such infrastructure is predominately owned by the private sector, but is critical to the functioning of our broader society. Protection of the public is not always consistent with private incentives in such settings. Given existing incentives, economic logic suggests that owners of key infrastructure will, from the point of view of the broader public interest, underinvest in security precautions.[3] At present, many industries see counterterrorism protection as a costly way to provide an uncertain degree of protection against an unlikely threat. There are few perceived benefits and many costs to improving security. As Frank Cilluffo, former Special Assistant to the President for Homeland Security in the Bush administration puts it: "We need to be able to spur [that] investment by providing incentives. Right now, the incentives are disincentives."[4]

Private markets by themselves do not generate sufficient incentives for homeland security, and government intervention can therefore be warranted, for several reasons. Most broadly, national security is a core constitutional responsibility of the federal government. Even if a given terrorist attack only affects private property, it can have broader ramifications for the country's sense of safety. In the terminology of economists, such an attack imposes a "0negative externality." The presence of this negative externality means that private markets will undertake less investment in security than would be socially desirable: Individuals or firms deciding how best to protect themselves against terrorism are unlikely to take the external costs of an attack fully into account, and therefore will generally provide an inefficiently low level of security against terrorism on their own.[5] Without government involvement, private markets will thus typically under-invest in anti-terrorism measures.[6]

---

[2] Congressional Budget Office, "Federal Terrorism Reinsurance: An Update," January 2005, page 13. Some industries (such as transportation, energy, utilities, and financial services) have increased spending modestly. See Benjamin Weiser and Claudia H. Deutsch, "Many Offices Holding the Line on Post-9/11 Security Outlays," New York Times, August 16, 2004; and the Conference Board, *Corporate Security Management: Organization and Spending Since 9/11* (New York: The Conference Board, 2003), p. 5.

[3] Peter R. Orszag, "Homeland Security and the Private Sector," Testimony before the National Commission on Terrorist Attacks Upon the United States, November 19, 2003.

[4] Frank Cilluffo, "The Mission of Homeland Security," *The NYU Review of Law and Security:* Are We Safer?, Issue No. 3 (Fall 2004), p. 38.

[5] It is also possible, at least in theory, for private firms to invest *too much* in anti-terrorism security. In particular, visible security measures (such as more uniformed guards) undertaken by one firm may merely displace terrorist attacks onto other firms, without significantly affecting the overall probability of an attack. In such a scenario, the total security precautions undertaken can escalate beyond the socially desirable levels—and government intervention could theoretically improve matters by placing limits on how much security firms would undertake. Unobservable security precautions (which are difficult for potential terrorists to detect), on the other hand, do not displace vulnerabilities from one firm to another and can at least theoretically reduce the overall level of terrorism activity. For an interesting application of these ideas to the Lojack automobile security system, see Ian Ayres and Steven Levitt, "Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack," *Quarterly Journal of Economics,* Vol. 108, no. 1 (February 1998). For further analysis of evaluating public policy in the presence of externalities, see Peter Orszag and Joseph Stiglitz, "Optimal Fire Departments: Evaluating Public Policy in the Face of Externalities," Brookings Institution Working Paper, January 2002.

[6] The Coase theorem shows that under very restrictive conditions, the negative externality can be corrected by voluntary private actions even if the role of government is limited to enforcing property rights. But the Coase theorem requires that all affected parties are able to negotiate at sufficiently low cost with each other. Since virtually the entire nation could be affected indi-

Second, a more specific negative externality exists with regard to *inputs* into terrorist activity. For example, loose security at a chemical facility can provide terrorists with the materials they need for an attack. Similarly, poor security at a biological laboratory can provide terrorists with access to dangerous pathogens. The costs of allowing terrorists to obtain access to such materials are generally not borne by the facilities themselves: the attacks that use the materials could occur elsewhere. Such a specific negative externality provides a compelling rationale for government intervention to protect highly explosive materials, chemicals, and biological pathogens even if they are stored in private facilities. In particular, preventing access to such materials is likely to reduce the overall risk of catastrophic terrorism, as opposed to merely displacing it from one venue to another.

Third, a related type of externality involves "contamination effects." Contamination effects arise when a catastrophic risk faced by one firm is determined in part by the behavior of others, and the behavior of these others affects the incentives of the first firm to reduce its exposure to the risk. Such interdependent security problems can arise, for example, in network settings. The problem in these settings is that the risk to any member of a network depends not only on its own security precautions but also on those taken by others. Poor security at one establishment can affect security at others. The result can often be weakened incentives for security precautions.[7] For example, once a hacker or virus reaches one computer on a network, the remaining computers can more easily be contaminated. This possibility reduces the incentive for any individual computer operator to protect against outside hackers.

Even stringent cyber-security may not be particularly helpful if a hacker has already entered the network through a "weak link."

A fourth potential motivation for government intervention involves information—in particular, the cost and difficulty of accurately evaluating security measures. For example, one reason that governments promulgate building codes is that it would be too difficult for each individual entering a building to evaluate its structural soundness. Since it would also be difficult for the individual to evaluate how well the building's air intake system could filter out potential bio-terrorist attacks, the same logic would suggest that the government should set minimum anti-terrorism standards for buildings if there were some reasonable threat of a terrorist attack on the relevant type of buildings (so that the individual would have some interest in ensuring that the building were protected against biological attack). Similarly, it would be possible, but inefficient, for each individual to conduct extensive biological anti-terrorism safety tests on the food that he or she was about to consume. The information costs associated with that type of system, however, make it much less attractive than a system of government regulation of food safety.

The fifth justification for government intervention is that corporate and individual financial exposures to the losses from a major terrorist attack are inherently limited by the bankruptcy laws. For example, assume that there are two types of possible terrorist attacks on a specific firm: A very severe attack and a somewhat more modest one. Under either type of attack, the losses imposed would exceed the firm's net assets, and the firm would declare bankruptcy—and therefore the extent of the losses beyond that which would bankrupt the firm would be irrelevant to the firm's owners. Since the outcome for the firm's owners would not depend on the severity of the attack, the firm would have little or no incentive to reduce the likelihood of the more severe version of the attack even if the required preventive steps were relatively inexpensive. From society's perspective, however, such security measures may be beneficial—and government intervention can therefore be justified to address catastrophic possibilities in the presence of the bankruptcy laws.

The sixth justification for government intervention is that the private sector may expect the government to bail it out should a terrorist attack occur. The financial assistance to the airline industry provided by the government following the September 11th attacks provides just one example of such bailouts. Such expectations create a "moral hazard" problem: private firms, expecting the government to bail them out should an attack occur, do not undertake as much security as they otherwise would. If the government cannot credibly convince the private sector that no bailouts will occur after an attack, it may have to intervene before an attack to offset the adverse incentives created by the expectation of a bailout.

---

rectly by a terrorist attack, the costs of negotiation are prohibitive, making the Coase theorem essentially irrelevant in the terrorism context.

[7] See Howard Kunreuther and Geoffrey Heal, "Interdependent Security," Journal of Risk and Uncertainty 26: 231–249 (March/May 2003), and Howard Kunreuther, Geoffrey Heal, and Peter Orszag, "Interdependent Security: Implications for Homeland Security Policy and Other Areas," Policy Brief #108, Brookings Institution, October 2002.

The final justification for government intervention involves incomplete markets. The most relevant examples involve imperfections in capital and insurance markets. For example, if insurance firms are unable to obtain reinsurance coverage for terrorism risks (that is, if primary insurers are not able to transfer some of the risk from terrorism costs to other insurance firms in the reinsurance market), some government involvement may be warranted. In addition, certain types of activities may require large-scale coordination, which may be possible but difficult to achieve without governmental intervention.

These market shortcomings provide a justification for targeted government intervention. But providing a high degree of protection for all possible targets would be prohibitively expensive and practically impossible. Focusing on high-impact attacks helps to narrow the range of private-sector settings in which government intervention is warranted.

When government intervention is needed, the best approach is to use government regulation to alter incentives for the private sector for better protecting itself. This can be done either by providing firms with certain advantages when they adopt appropriate measures (the carrot approach), or by imposing costs on those who fail to adopt such measures (the stick approach). In both cases, the goal would be the same: to introduce a difference in the cost of one activity compared to another, accomplished either by reducing the cost of the first activity (e.g., an investment in security) or by raising the cost of the second activity (e.g., business as usual).

For example, consider the case of trucking. Truck drivers can be subjected to more intensive background searches, and advanced technologies can be used to monitor trucks and ensure the security of their cargo in real time. The government could directly subsidize such steps, for example by providing tax credits to firms that adopt them. Or it could mandate insurance for trucking firms, thereby relying on insurances firms to impose costs (e.g., through higher premiums) on firms that fail to adopt appropriate security measures. The government could also combine either of these approaches with some form of regulation, such as allowing better protected cargo trucks to travel closer to population centers than less protected trucks, thereby providing time and money savings to the firms that invest in protecting their trucks.

The key distinction between the "carrot" and the "stick" approaches is who pays. Government subsidies or tax credits spread the cost of homeland security spending in a particular private market across the entire population, rather than the stakeholders (the owners of businesses, the workers, and consumers of the product) in that sector itself. The stick approach—either through regulation or insurance, or some combination thereof—instead concentrates its costs on the stakeholders in that sector. If particular sectors are inherently more dangerous than others, we as a society may want to encourage activity in other, safer sectors where we have a choice—which would be better accomplished by having stakeholders in the sector bear the full cost of protection. The reason is that imposing the cost on the stakeholders rather than the general public would raise the costs of the most dangerous activities. The market would thus discourage such activities (through higher prices), which would help to mitigate the risk of a terrorist attack in the most dangerous sectors.

Before turning to a discussion of specific industries, we first examine these generic approaches to improving security in the private sector.

SUBSIDIES

Perhaps the most obvious way of strengthening incentives for protective measures in the private sector is to provide a government subsidy. For example, some policymakers have proposed tax credits for security measures. This approach, however, is generally flawed, and not just because of the substantial budget imbalance facing the nation.

Subsidies or tax credits can encourage unnecessarily expensive investments in security measures (or "gold plating"). The problem is particularly severe in the case of investments that provide protection against terrorist attack but also have substantial other benefits to firms. Even if they don't encourage firms to undertake excessively costly investments with minimal homeland security benefits, subsidies or tax credits can provide benefits to firms that would have undertaken the investments even in the absence of the tax subsidy—raising the budget cost without providing any additional security. In other words, subsidies or tax credits "buy out the base" of what firms are already doing to protect themselves against terrorist attack. Subsidies or tax credits also do a poor job of differentiating between high-risk and lower-risk sectors, yet the degree of government intervention should clearly vary by circumstance. In other words, designing and implementing subsidies or tax credits is likely to be just as cumbersome and inefficient as designing direct regulations.

INSURANCE AS A MECHANISM FOR IMPROVING INCENTIVES

An alternative is to provide incentives for better security through the insurance system. At first glance, terrorism insurance may seem counterproductive: Firms and individuals with insurance against terrorist attack would appear to lack incentives to take appropriate precautions against an attack. However, where such insurance is available, it typically comes with provisions (such as a deductible) to ensure that the insured bear at least some of the cost of an attack, and thus have an economic incentive to avoid such attacks or minimize their consequences. More important, the insurance companies themselves have an incentive to encourage risk-reducing activities. Indeed, insurance firms are well positioned to provide incentives for mitigation efforts—for firms to take steps ahead of time to protect themselves against terrorist attack. The terrorism insurance market could thus guide protective efforts. Best practices would be encouraged through graduated rate structures for insurance that encourage individual owners to adopt prudent and cost-effective technologies and procedures for protecting their assets and the people within them.

Three critical questions arise with regard to the use of insurance in this way. The first is whether firms will voluntarily purchase the insurance. Terrorism insurance coverage among large firms has expanded noticeably: take-up rates were quite low in 2003 but nearly doubled in 2004, reaching almost half of large firms in mid2004.[8] Despite the recent increases, however, take-up of terrorism insurance remains well below 100 percent.[9] In the absence of universal take-up, at least among firms that own critical infrastructure, the incentives provided by the insurance industry would be much less likely to produce adequate risk reduction. Furthermore, voluntary insurance markets often suffer from classic problems of "adverse selection," in which firms that are riskier are the ones that are more likely to purchase insurance, creating a potential spiral of rising premiums and reduced take-up.

The shortcomings with voluntary terrorism insurance raise the question of whether insurance should be mandatory—at least for large firms or key sectors. Mandatory insurance would not only facilitate risk-mitigation efforts on a broader scale and allow the insurance industry to spread its risks more effectively, but would also reduce the likely demands on government following any attack in the future.[10]

In France, terrorism insurance is mandatory.[11] Former Deputy Homeland Security Adviser Richard Falkenrath has suggested that Congress mandate that terrorism insurance be included in all commercial insurance policies.[12] In our view, terrorism insurance should indeed be required on all commercial policies, perhaps above some minimum threshold of several million dollars to avoid unnecessary administrative costs in settings unlikely to cause high-impact terrorist damage.

The second question is whether the insurance industry will be able to develop the tools for evaluating terrorism risk. Models of terrorism risk at the level of zip codes or specific locations are now available from firms such as Risk Management Systems, EQECAT, and Applied Insurance Research Worldwide.[13] These models represent significant advances; they are, however, inherently limited not only by the paucity of historical data on terrorist attacks but also by the difficulties in predicting how terrorist behavior will evolve over time. For example, one model assumes that risk is mostly concentrated in high visibility targets; another assumes that attacks at low visibility targets could be employed to sow confusion and broad fears.[14] The key issue is not whether the models are fully reliable; they clearly are

---

[8] Congressional Budget Office, "Federal Terrorism Reinsurance: An Update," January 2005, page 6; and Erwann Michel-Kerjan and Burkhard Pedell, "Terrorism Risk Coverage in the post-9/11 Era: A Comparison of Public-Private Partnerships in France, Germany, and the U.S," Risk Management and Decision Processes Center, Wharton School, University of Pennsylvania, Working Paper 2004029, October 2004, page 22.

[9] Some economists argue that many firms *should* not insure themselves against terrorist attack, since the owners of the firm can mostly if not entirely diversify that risk. Kent Smetters, "Insuring Against Terrorism: The Policy Challenge," NBER Working Paper 11038, January 2005.

[10] Howard Kunreuther and Erwann Michel-Kerjan, "Policy Watch: Challenges for Terrorism Risk Insurance in the United States," Journal of Economic Perspectives, Volume 18, Number 4, Fall 2004, page 211.

[11] Erwann Michel-Kerjan and Burkhard Pedell, "Terrorism Risk Coverage in the post-9/11 Era: A Comparison of Public-Private Partnerships in France, Germany, and the U.S," Risk Management and Decision Processes Center, Wharton School, University of Pennsylvania, Working Paper 2004029, October 2004.

[12] Statement of Richard A. Falkenrath before the United States Senate Committee on Homeland Security and Governmental Affairs, January 26, 2005.

[13] Congressional Budget Office, "Federal Terrorism Reinsurance: An Update," January 2005, page 4.

[14] Congressional Budget Office, "Federal Terrorism Reinsurance: An Update," January 2005, page 4.

not.[15] Instead, the fundamental question is whether the models could become good enough to provide the basis for an insurance-oriented approach to protective efforts. From this perspective, especially compared to an alternative of failing to provide incentives for private efforts or relying exclusively on government regulation, the models seem relatively insightful. And it should be possible for them to be informed by government risk analyses as well. Homeland Security Presidential Directive 7 (HSPD 7) requires the Secretary of Homeland Security to coordinate national protection efforts in infrastructure sectors such as information technology, telecommunications, transportation, and the chemical industry, and requires the government as a whole to prioritize protection activities.[16]

A final question is whether the insurance industry requires a government backstop to play the role envisioned for it here. Some economists argue that the risks can be spread across private financial markets without government intervention.[17] Other economists and market observers, however, argue that capital market imperfections impede the ability of insurers to provide coverage against catastrophic risks, such as those involved in terrorist activities. In such a case, a government backstop may be required. Alan Greenspan, for example, has testified that he has "yet to be convinced" that the terrorism insurance market could operate effectively without a government backstop.[18]

The most pressing issue involves the Terrorism Risk Insurance Act (TRIA), enacted in November 2002. TRIA is scheduled to expire on December 31, 2005, and policymakers are debating whether it should be extended. Under TRIA, insurance firms are required to offer terrorism coverage, and the government agrees to pay a specified share of the insured losses in the event of a terrorist attack.[19] Although some form of federal backstop should be extended past 2005, significant changes in the existing program are warranted.[20] A substantial flaw with the current program is that no fee is imposed by the government for the backstop. (The government would recover a certain amount of its losses after the fact, but through a surcharge on all commercial policies, rather than only on those with terrorism insurance components. As a result, the government program effectively subsidizes terrorism insurance, with all commercial policyholders potentially liable to pay for part of the subsidy.) A better approach would have the government charge a premium based on how much protection the insurance firm itself wants; the government should continue, though, only to provide coverage against extreme losses.[21] Losses below the catastrophic level should be covered entirely by private markets.

## A MIXED SYSTEM WITH INSURANCE AND REGULATIONS

An insurance-based system could be combined with a larger policy of regulatory standards and third-party inspections. A mixed regulatory-insurance system is already applied in many other areas, such as owning a home or driving a car. Local building codes specify minimum standards that homes must meet. But mortgages generally require that homes also carry home insurance, and insurance companies provide incentives for improvements beyond the building code level—for example, by providing a reduction in the premiums they charge if the homeowner installs a security system. Similarly, governments specify minimum standards that drivers must meet in order to operate a motor vehicle. But they also require drivers to carry liability insurance for accidents arising out of the operation of their vehicles. Meanwhile, insurance companies provide incentives for safer driving by charging higher premiums to those with poorer driving records.[22]

---

[15] The insurance industry operates in many areas in which models are nowhere close to fully reliable, including tort cases. See Kent Smetters, "Insuring Against Terrorism: The Policy Challenge," NBER Working Paper 11038, January 2005.

[16] President George W. Bush, "Homeland Security Presidential Directive/HSPD 7: Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, available at *www.whitehouse.gov/news/releases/2003/12/print/20031217–5.htlm.*

[17] Kent Smetters, "Insuring Against Terrorism: The Policy Challenge," NBER Working Paper 11038, January 2005. See also Appendix B in Congressional Budget Office, "Federal Terrorism Reinsurance: An Update," January 2005.

[18] "Senators Trying Again To Extend Terrorism Insurance Plan," CongressDaily, February 18, 2005.

[19] For a description, see Congressional Budget Office, "Federal Terrorism Reinsurance: An Update," January 2005.

[20] See also Swiss Re, "Terrorism Risks in Property Insurance and Their Insurability After September 11, 2001" (2003).

[21] For one explanation of how various layers of insurance could be provided, including a government layer for catastrophic losses, see Howard Kunreuther and Erwann Michel-Kerjan, "Policy Watch: Challenges for Terrorism Risk Insurance in the United States," Journal of Economic Perspectives, Volume 18, Number 4, Fall 2004.

[22] To be sure, crucial differences exist between the terrorist case and these other examples. For example, stable actuarial data exist for home and auto accidents, but not for terrorist at-

A mixed system of minimum standards coupled with an insurance mandate not only can encourage actors to act safely, but also can provide incentives for innovation to reduce the costs of achieving any given level of safety. The presence of minimum regulatory standards also helps to attenuate the moral hazard effect from insurance: Moral hazard arises when firms, knowing that they are insured against terrorist losses, take less care in protecting against attack. Minimum standards could also provide guidance to courts in determining negligence under liability laws.[23]

A mixed system also has the advantage of being flexible, a key virtue in an arena where new threats will be "discovered" on an ongoing basis. In situations in which insurance firms are particularly unlikely to provide proper incentives to the private sector for efficient risk reduction (for example, because insurers lack experience in these areas), regulation can play a larger role.

Third-party inspections can be coupled with insurance protection to encourage companies to reduce the risk of accidents and disasters. Under such schemes, insurance corporations would hire third-party inspectors to evaluate the safety and security of plants seeking insurance cover. Passing the inspection would indicate to the community and government that a firm complies with safety and security regulations. The firm would also benefit from reduced insurance premiums, since the insurer would have more confidence in the safety and security of the firm.

This system takes advantage of two potent market mechanisms to make firms safer, while freeing government resources to focus on the largest risks. Insurance firms have a strong incentive to make sure that the inspections are rigorous and that the inspected firms are safe, since they bear the costs of an accident or terrorist attack. Private sector inspections also reduce the number of audits the regulatory agency itself must undertake, allowing the government to focus its resources more effectively on those companies that it perceives to pose the highest risks. The more firms decide to take advantage of private third-party inspections, the greater the chances that high-risk firms will be audited by the regulatory agency.

Studies have shown how such a program could be implemented in practice. In Delaware and Pennsylvania, the State Departments of Environmental Protection have worked closely with the insurance industry and chemical plants to test this approach for chemical facility safety.[24]

REQUIRED STEPS IN SPECIFIC INDUSTRIES AND SECTORS

The steps required to improve security vary across industries. In keeping with the principles we set forth in chapter one, it is important to find ways to maximize protection, particularly against catastrophic attack, in cost-effective ways and where possible in a manner that provides additional benefits outside the homeland security realm. But applying these principles to specific industries and sectors requires considerable detailed technical analysis on a case by case basis.

One common theme in much of the below, however, is that appropriate safeguards are often expensive to implement immediately but relatively painless to build into new systems. For example, given that al-Qa'ida appears to have considerable interest in biological agent attacks, and given the continued difficulty of treating the symptoms of biological attacks quickly and effectively (especially on a large scale), it behooves the United States to adopt defensive measures where cost-effective.[25] Air intakes on buildings can be put well above street level and beyond the reach of anyone without access to restricted areas.[26] Filters might be built into air circulation systems, to impede the distribution of any chemical or biological agent introduced into a building (and a slight overpressure maintained within buildings to re-

---

tacks. Nonetheless, it may be possible for insurers to distinguish risks of loss based on differences in damage exposures, given a terrorist incident. Some financial firms are already trying to devise basic frameworks for evaluating such risks. See, for example, Moody's Investors Service, "Moody's Approach to Terrorism Insurance for U.S. Commercial Real Estate," March 1, 2002.

[23] For a discussion of the potential benefits of a mixed system of building code regulations and mandatory catastrophic risk insurance in the context of natural disasters, see Peter Diamond, "Comment on Catastrophic Risk Management," in Kenneth Froot, ed., *The Financing of Catastrophe Risk* (University of Chicago Press: Chicago, 1999), pages 85–88.

[24] For further information, see Howard Kunreuther, Patrick McNulty, and Yong Kang, "Improving Environmental Safety Through Third Party Inspection," *Risk Analysis.* 22: 309–18, 2002.

[25] Judith Miller, "U.S. Has New Concerns About Anthrax Readiness," *New York Times,* December 28, 2003, p. A20; and Philip Shenon, "Terrorism Drills Showed Lack of Preparedness, Report Says," *New York Times,* December 19, 2003.

[26] Gregory Wright, "Is Your Building's HVAC Safe Against Terrorism?" *HVACR News,* vol. 24, no. 2 (May 2004).

duce the risk that agents will infiltrate from the outside).[27] Addition of filters may sometimes only be practical when entire heating, ventilation, and air conditioning systems are being replaced.[28] Still, over time, considerable progress is quite feasible. Many modern heating and air circulation systems have the kinds of sensors, adaptable flows, and other features that could help protect against the effects of terrorist attack as well as optimize a building's functioning and the quality of its air in normal times.[29] This shows how measures taken in part to promote homeland security can have other benefits.

Protecting key buildings against attacks involving explosives is difficult, but sometimes warranted when high casualties or other severe damage to society could result from a given attack (and when any attack is probably preventable through reasonably inexpensive measures). Sometimes it is a matter of adopting simple steps of limited but useful impact. For example, elevators might be built so as to descend to the nearest floor in the event of a power outage—a wise investment against the possibility of electricity overloading as well. (In the public sector, relatedly, street lights could be given low-energy diode emitters powered by batteries as backups to main power systems.[30])

Truck bombs will remain a threat in the future; they have been the weapon of choice of al-Qa'ida in most attacks since 9/11. Defending against them can involve constructing new, prominent buildings a certain distance back from streets—as has occurred with a number of new U.S. embassies in recent years. Further desirable measures, at least for the highest-profile buildings, can involve using shatterproof glass or comparable coatings in the lower floors of such buildings, and closing or at least inspecting entrants into underground parking garages. Relatedly, one might worry about large bombs being assembled piece by piece through the use of individual bags to carry explosives into buildings. This threat may argue for controlling access to symbolically important buildings in particular. At present, outside of New York, very few major buildings have any checks or controls on entry.[31]

*The Chemical and Nuclear Industries*

The U.S. chemical industry remains quite vulnerable to possible terrorist strikes.[32] As Richard Falkenrath recently testified, "To date, the federal government has made no material reduction in the inherent vulnerability of hazardous chemical targets inside the Untied States. Doing so should be the highest critical infrastructure protection priority for the Department of Homeland Security in the next two years."[33] A DHS study that ranked a terrorist act releasing chlorine, along with nuclear and anthrax attacks, as among the most deadly plausible scenarios for the United States to worry about in the future gives further credence to Falkenrath's view.[34] As we argue in chapter one, it is precisely such types of vulnerabilities that demand the most urgent attention.

Voluntary measures have been adopted by some chemical plants, notably those of the American Chemistry Council, but these represent a minority of the nation's total such facilities. Hardening plants against sophisticated attacks by well-trained bands of terrorists, and other such robust safeguards, could be uneconomical and in many cases unnecessary. There are thousands of chemicals produced in the United States, but only some 300 that are very dangerous and about half that number that are most extreme in the threats they pose. There are tens of thousands of chemical plants but only 4,000 to 8,000 where the improper release of agent could kill 1,000 or more individuals.[35] But a more systematic approach that at least requires peri-

---

[27] U.S. Army Corps of Engineers, "Protecting Buildings and Their Occupants from Airborne Hazards," draft, October 2001; Energy Information Administration, Department of Energy, "Building Characteristics: Buildings Use Tables," table 12, available at *www.eia.doe.gov/emeu/consumption; Letter from Michael C. Janus, Battelle Corporation, December 1, 2001, to Michael O'Hanlon; and Ann Gerhart, "Tom Ridge, on High Alert," Washington Post,* November 12, 2001, p. C1.

[28] Department of Health and Human Services, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks (May 2002);*

[29] Jon C. Lund, "Smart Buildings," *IEEE Spectrum* (August 2003), pp. 18–23.

[30] Peter Fairley, "The Unruly Power Grid," *IEEE Spectrum* (August 2004), pp. 22–27.

[31] Terry Pristin, "Different Cities, Different Security for Buildings," *New York Times,* July 9, 2003, p. C6.

[32] For further discussion of homeland security and the chemical industry, see Congressional Budget Office, "Homeland Security and the Private Sector," Chapter 3 (Chemicals and Hazardous Materials), December 2004.

[33] Statement of Richard A. Falkenrath before the United States Senate Committee on Homeland Security and Governmental Affairs, January 26, 2005.

[34] Eric Lipton, "U.S. Report Lists Possibilities for Terrorist Attacks and Likely Toll," *New York Times,* March 16, 2005, p. 1.

[35] Richard D. Farmer, *Homeland Security and the Private Sector* (Washington, D.C.: Congressional Budget Office, December 2004), pp. 21—28.

odic assessments of vulnerabilities and common-sense solutions is imperative.[36] Senator Corzine introduced a bill to do just that but it has not been passed by the Congress.[37]

There are also situations where less dangerous chemicals can be used in place of highly toxic ones. Reducing dependence on chlorine for drinking water purification is the most notable example. In these cases, the good sense of chemical plant owners combined with the guiding hand of the insurance market are the ideal mechanisms for improving safety.[38]

Another key challenge is securing nuclear materials.[39] Power plants are now protected fairly well. But the cooling ponds used for storage of spent fuel may not be protected against certain types of attacks (such as from airplanes).[40] Nor are many areas where low-medium-grade waste is stored. These latter materials can be used in "dirty bombs." While such weapons might not kill large numbers, they could cause enormous economic costs (due to cleanup) and disruption (if a city center or other important area could not be used while being cleaned). Here the most practical defense is much improved security for sites where such materials are found, at home and abroad.[41] In this type of case, where the optimal safety features are not obvious, regulation may be less desirable than reliance on insurance market incentives.

*Passenger Trains, Buses, and Boats*

On March 11, 2004, a simple terrorist strike against trains in Madrid killed some 200 people and injured another 1,500. The July 7, 2005 London attacks, killing more than 50 themselves, underscored that Madrid was not a fluke. This worry applies not only to trains, but in similar ways to buses, ferries, and cruise ships. Yet not nearly as much attention has been given to this issue as, for example, to airplane security.[42]

Several experimental efforts have been made to monitor passengers and cargo entering American trains. However, such efforts tend to rely heavily on labor-intensive methods such dogs to detect explosives. The challenge is the speed at which people must move through such stations, and the number of passengers involved, particularly for heavily traveled local train services and subways.[43] For example, the New York subway system carries nearly 4 million passengers a day (getting on and off at 468 stations); all America's airports handle just 1.5 million people a day between them.[44]

Some additional safeguards are desirable for trains and buses. Emergency communications systems can be improved, stations protected by perimeter fencing and guards and monitoring, relevant tunnels hardened, and spot checking made more common. Further federal funding is appropriate here; insurance markets are un-

---

[36] Government Accountability Office, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown,* GAO–03–439 (March 2003), summary page.

[37] Office of Senator Jon S. Corzine, "Fact Sheet on Senator Corzine's Chemical Security Legislation," November 17, 2003, available at *www.corzine.senate.gov/priorities/chem _*sec.html; and Rick Hind and David Halperin, "Lots of Chemicals, Little Reaction," *New York Times,* September 22, 2004, p. A31.

[38] A related topic concerns the safeguards applied to the sales of certain lethal chemicals. Not enough has yet been done to ensure proper oversight in this regard. For example, a full decade after the Oklahoma City tragedy, only three states have notable regulations on the sale of ammonium nitrate fertilizer. Oklahoma joined South Carolina and Nevada in requiring requiring presentation of identification from anyone wishing such fertilizer and tracking sales of such materials to allow for investigation of any problems that may result. Others should follow this lead. In such cases where simple, common-sense, minimal-cost regulations can be devised, they are hardly inconsistent with the general approach advocated here of using market incentives where possible but mixed approaches including some regulation when sensible. See Associated Press, "National Briefing—Oklahoma: Rules to Regulate Selling of Fertilizer," *New York Times,* February 18, 2005, p. A17.

[39] See Congressional Budget Office, "Homeland Security and the Private Sector," Chapter 2 (Civilian Nuclear Power), December 2004.

[40] Shankar Vedantam, "Storage of Nuclear Spent Fuel Criticized," *Washington Post,* March 28, 2005, p. 1.

[41] Peter D. Zimmerman and Cheryl Loeb, "Dirty Bombs: The Threat Revisited," Defense Horizons, no. 38 (Washington, D.C.: National Defense University, January 2004); and Joby Warrick, "Smugglers Targeting Dirty Bombs for Profit," *Washington Post,* November 30, 2003, p. 1.

[42] Arnold M. Howitt and Jonathan Makler, "On the Ground: Protecting America's Roads and Transit Against Terrorism," (Washington, D.C.: Brookings, 2005).

[43] Baronet Media Ltd., "Washington Tests High Security System for Trains," Vigilo Risk, issue #1, June 9, 2004, p. 7.

[44] Gregg Easterbrook, "In an Age of Terror, Safety Is Relative," New York Times, June 27, 2004, p. 1.

likely to be of much help since much train infrastructure is publicly owned.[45] The American Public Transportation Association has called for over $7 billion in added funding for mass transit systems including trains over the next three years—thirty times the expenditures of the last three years combined.[46] Indeed, there is a strong case for substantial funding increases.[47]

But the $7 billion added amount strikes us as too much. More logical is a gradual, incremental increase that continually evaluates the benefits of new and experimental measures as they are introduced. The fact of the matter is that, almost independent of expenditure levels, security will not be perfect on trains and buses. Controlling access of all passengers at all times seems unrealistic.

Tightened security measures can be used for special events or in the case of intelligence alerts suggesting particular cause for concern. For example, police officers were put on every subway train in New York the day after the July 7, 2005 London bombings.[48] But alas this vulnerability is one of those so difficult to address that it underscores the need for preventive homeland security activities-border patrols, prevention efforts by police departments and the FBI, and so forth—as well as continued intelligence operations and offensive action abroad.

A Democratic attempt to add $1.7 billion to the 2006 budget for rail security failed in the Congress.[49] The Democratic idea was sound but the amount was, for the reasons noted above, probably too much. That said, an increase in the range of hundreds of millions of dollars would have been appropriate, and should be pursued for the 2007 budget.

The situation is similar for passenger ships and ferries. Some improvements in security are warranted, but that said, vulnerability is a fact of life.[50] Given that most such attacks, however tragic they might be, would not be catastrophic in the terms we use in chapter one, a cost-benefit analysis—and the state of available technology and procedures for security—suggest that only limited investments of the type already underway are warranted at this time.[51]

*Cargo Trains, Trucks, and Barges Carrying Hazardous Materials*

Trucks, trains, and barges are the chief methods for the transport of hazardous materials in the United States today. On the issue of trucks, at present there are few restrictions on who can drive the trucks and where those trucks can go—except of course that as a matter of public safety, tunnels and certain other very specific sections of road are sometimes deemed off limits to certain classes of highly toxic or flammable materials. Background checks have been begun for drivers of especially dangerous classes of chemicals and other substances. But efforts to authenticate their identities using identification with biometric indicators remain in the pilot, testing stage.[52] Moreover, Mexican and Canadian drivers on American roads are not being checked in the same way.[53] Some municipalities have similarly decided to find substitutes for the most lethal sorts of chemicals often carried by trucks (such as chlorine) when possible. Some companies train their employees in security precautions and monitor key facilities such as fuel depots. But these efforts are at present scattershot.[54]

---

[45] Baronet Media Ltd., "House Committee Seeks $1 Billion for U.S. Rail Security," *Vigilo Risk,* issue #2, June 23, 2004, p. 7.

[46] David Randall Peterman, "Passenger Rail Security: Overview of Issues," *CRS Report for Congress* (Washington, D.C.: Congressional Research Service, July 29, 2005), pp. 2—3.

[47] Nicole Gaouette, "Senate is Split on Spending Bill for Domestic Security," *Los Angeles Times,* July 12, 2005.

[48] Sewell Chan, "In Added Security Measure, Officers are Riding the Rails," *New York Times,* July 8, 2005.

[49] David Rogers, "Homeland Budget Accord Is Reached," *Wall Street Journal,* September 30, 2005, p. 2.

[50] In addition to the threat of explosives being placed in cars, or planted directly on ferries and other ships, there is a risk of scuba divers attacking ships. See Jim Gomez, "Terror Plots May Reach New Depths," Chicago Tribune, March 18, 2005. Sometimes certain risky ports or waterways can be avoided overseas, but clearly this is not a protection method of complete reliability. See David Wood, "Terrorism Fears Divert Navy Supply Ships from Suez Canal," Newhouse.com, January 13, 2005.

[51] Eric Lipton, "Trying to Keep the Nation's Ferries Safe from Terrorists," *New York Times,* March 19, 2005, p. 18.

[52] William H. Robinson, Jennifer E. Lake, and Lisa M. Seghetti, "Border and Transportation Security: Possible New Directions and Policy Options," *CRS Report for Congress* (Washington, D.C.: Congressional Research Service, March 29, 2005), pp. 9—10.

[53] Transportation Security Administration, information at *www.tsa.gov/public/display?content=09000519800d3fd3&print=yes, accessed January 6, 2005.*

[54] See David Johnston and Andrew C. Revkin, "Officials Say Their Focus Is on Car and Truck Bombs," *New York Times,* August 2, 2004, p. A13.

This situation is highly imprudent. Leaving aside the issue of truck bombs, many trucks carry potentially lethal materials that could kill thousands if dissipated in densely congested parts of cities. To reduce the risks, several steps can be taken. First, for those drivers transporting anything from gasoline to chlorine, background checks must be done comprehensively and quickly. Names and fingerprints must be compared to entries on terror watchlists. Second, truck storage yards must meet minimal safety standards limiting access and monitoring perimeters. Third, safety features should be used on the doors of relevant trucks—reducing the odds that dangerous materials would be stolen for subsequent use in a terrorist attack. Given the danger of the materials involved, not just to the drivers of the trucks and others directly involved but to society on the whole, minimal safety standards are important enough to be done by regulation rather than relying entirely on the insurance markets.

As an additional precaution, trucks carrying certain highly toxic substances should be banned from the most central parts of cities—unless escorted by security and outfitted with tracking technology as well as automatic braking technology.[55] Economic incentives would thus come into play, with firms measuring the costs of protective technology against the economic benefits of being granted greater access to densely populated regions.

The chlorine gas tragedy in South Carolina in January of 2005 underscored the need for upgrades to security in this realm as well. Several types of improvements are needed. As the South Carolina accident underscored, both would have benefits for general public health beyond the subject of counterterrorism, reducing the risks of routine accidents. Since it is a dual-benefit program, it serves one of main goals we suggest in chapter one for guiding future homeland security efforts.

When substitution of dangerous chemicals by safer chemicals cannot happen, specific trains should be rerouted away from the centers of cities when necessary and practical. In early 2005, the District of Columbia prohibited shipments of hazardous materials through parts of the nation's capital. A more systematic national effort is appropriate as well.[56] (The most lethal substances should be banned outright from city centers; others could be permitted, as noted above, when companies adopt best practices on safety such as automatic tracking and braking technology on their trucks.)

Finally, safety standards should be enforced. For example, it should not be tolerated that half of the nation's 60,000 train cars frequently carrying poisonous gases are obsolete or otherwise in poor shape.[57] This recommendation complements the first, since it is easier to improve safety on a smaller number of trains.[58]

*The Food and Water Industries*

Other areas where not enough has been done to prevent attacks are the food industry and the country's water infrastructure.

In regard to food, the case for doing more can be debated. There are no known cases of al-Qa'ida or affiliates attacking the food supply, but that hardly means that an organization that has already proved itself innovative will not attack it in the future. And certain types of attacks, such as a small amount of botulism toxin poured into a milk truck leaving a farm could literally cause tens if not hundreds of thousands of deaths.[59] Thus, if simple and economical measures that bring other benefits beyond the counterterrorism domain can be identified, they should be seriously considered.

As he left the Bush administration, former Secretary of Health and Human Services Tommy Thompson said the worries "every single night" about large-scale food poisoning.[60] But infrastructure for monitoring food supplies and quickly detecting any signs of contamination is insufficient. Some additional funding has been added for food safety investigators and laboratories to check for deliberate contamination. But no demands have been placed on the nation's 50,000+ food processing sites to improve site security. Some voluntary measures have been adopted by the industry—and FDA and USDA have preferred to keep them voluntary to avoid collecting

---

[55] Flynn, America the Vulnerable, pp. 118—122.

[56] Eric M. Weiss and Spencer S. Hsu. "90-Day Hazmat Ban Is Passed; Measure Will bar Shipments in DC." *Washington Post*, February 2, 2005, p. B1.

[57] Walt Bogdanich and Christopher Drew, "Deadly Leak Underscores Concerns About Rail Safety." *New York Times*, January 9, 2005, p. 1.

[58] Sara Kehaulani Goo, "Accidents Spur New Focus on Securing U.S. Raily System," *Washington Post.* Janaury 29, 2005.

[59] Rick Weiss, "Report Warns of Threat to Milk Supply," *Washington Post,* June 29, 2005, p. A8.

[60] Mike Allen, "Rumsfeld to Remain at Pentagon; Thompson Quits at HHS, Warns of Vulnerabilities," *Washington Post,* December 4, 2004, p. A1.

data that could later be made available due to Freedom of Information Act requests. But these have been spotty.[61]

Requiring sites such as food processing centers to carry terrorism insurance (against any liability for poisoning that occurs on their premises) may provide the simplest and soundest means of addressing this vulnerability in a cost-effective way. At a minimum, it could lead to more uniform adaptation of commonsense protective measures such as more systematic patrolling and monitoring of the perimeters of facilities.

As suggested by the Democratic members of the House Select Committee on Homeland Security, each state or region should also have the ability to quickly test foods for a wide range of possible contaminants. This can allow spot checking of food under normal circumstances, and prompt efforts to contain the consequences of any attack should one occur.

As for water, it is extremely difficult to contaminate large water systems because of the amount of material needed for lethal doses. That means that protecting drinking water reservoirs, for example, need not extend to the level of providing complete assurance that no person on foot is ever near a reservoir at any time. Protective systems that keep trucks away from such reservoirs, and monitor foot traffic well enough to ensure that substantial numbers of people are not able to gain entry to a reservoir, would generally suffice. And as for the chemical treatment facilities, these can be viewed largely as any other chemical plant—with risk, and appropriate security measures, determined by the nature of the chemicals in use. To the extent chlorine is employed, that implies a reasonably high level of protection, but nothing beyond the scale of what would be properly applied to many other facilities in the chemical industry.[62]

A second problem with water concerns the potential for attacks on dams to flood metropolitan areas and create conditions not unlike those produced by Hurricane Katrina—though this time without the warning. Risk assessments have been completed for the nation's major dams.[63] The amount of high explosive needed to destroy most of them, together with improved site security near most, limit the likely danger associated with this type of terrorist scenario. But they do not eliminate the risk entirely by any means. At a minimum, this worry is further reason for the nation to digest fully the lessons of Katrina—and figure out how to mount large-scale responses to such catastrophes within hours rather than days. This observation has implications for many agencies, including NORTHCOM. The military should not be the lead responder to the vast majority of natural disasters or terrorist strikes, in terms of leading any effort. But leaving aside such issues, as well as the question of whether posse comitatus should be modified, the U.S. armed forces have physical capacities rivaled by no other national institution and at a minimum need to be better prepared to organize and deploy them fast in future crises.

*Energy Infrastructure*

It will not always be possible to know what infrastructure to protect and what not to protect—until after the fact. Take for example the Alyeska Pipeline in Alaska (or any other oil pipeline). It is possible to use a rifle to disrupt the flow of oil, and in fact that has happened before (though in an act closer to vandalism or hooliganism than terrorism). Pipelines are of course attacked in Colombia, Iraq, and elsewhere so this threat is hardly implausible. That said, taking steps to try to prevent such attacks would clearly be very difficult in some places, short of setting up dense security perimeters (or burying the pipelines). Moreover, attacks on oil pipelines would be unlikely to cause the loss of any human life. This is the type of threat that should be in a second or even third tier of importance.[64] Some measures such as protecting choke points, ensuring capacity for quick shutdown of damaged pipes, and protecting the pumping stations (and key electronics) of pipeline systems are warranted, but comprehensive protection is not.[65]

---

[61] General Accounting Office, *Food-Processing Security,* GAO–03–342 (February 2003), pp. 1—7.

[62] Government Accountability Office, *Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security,* GAO–05–33 (January 2005), pp. 84—93.

[63] Claudia Copeland and Betsy Cody, "Terrorism and Security Issues Facing the Water Infrastructure Sector," in Russell Howard, James Forest, and Joanne Moore, eds., *Homeland Security and Terrorism* (New York: McGraw Hill, 2006), p. 200.

[64] See for example, Andrea R. Mihailescu, "Alaska's Vulnerable Oil Pipeline," *Jane's Terrorism and Security Monitor,* September 1, 2004.

[65] One area where it behooves the United States to establish improved vigilance is in the vulnerability of power, communications, transportation, and water infrastructure to electromagnetic pulse from a high-altitude nuclear detonation. Terrorists are unlikely to carry out such an attack, but a nation-state could, and the nature of the preparation against such an attack is akin

To take another energy example, of greater concern given the potential loss of life involved in any attack, Boston is the only major city in the United States to have a liquid natural gas terminal nearby. (Explosions of such tankers could cause structural damage to buildings a third of a mile away and burn the skin of people a mile away.[66]) Tankers were not allowed to come into Boston harbor to service this terminal during the 2004 Democratic convention, suggesting that there is a real basis to worry about a possible attack. But has the danger really passed now that the convention is over? This question suggests that it would be prudent to move the terminal—if not immediately, then at least when a major renovation would be needed on the existing infrastructure.[67]

*Skyscrapers, Major Buildings and Other Structures*

In the United States, most large buildings, famous public facilities, sports stadiums, concert halls, and shopping malls are open to the public—and thus to terrorists armed with explosives, chemicals, or biological pathogens. Most such structures lack the types of filters that could clean up contamination that gets inside. Few buildings have the types of air circulation systems that reduce the danger of such contamination in the first place. And few have common-sense protections against the kinds of car and truck bombs that al-Qa'ida continues to employ with frequency and effectiveness around the world even in the post-9/11 era.

The degree of appropriate protection depends clearly on the nature of the potential target. For the nation's 500 skyscrapers, 250 largest arenas and stadiums, large train stations and airports, and any other locations where many thousands of people gather in confined spaces, special efforts are required when practical. New buildings might even be built a certain distance back from streets (as is the case with many U.S. embassies today), tougher structural building codes employed, and parking garages kept physically separate from buildings. But these sorts of sweeping measures are clearly not practical for all cases.[68]

Existing structures can be equipped with shatterproof glass in lower floors. Vehicles entering their parking garages can be searched and in some cases restricted in their movements. When air circulation systems are renovated, their intakes should be moved above street level and monitored. Reverse pressure air systems and good filters are among the other options. Again, insurance markets can help incentivize owners to adopt such measures.[69]

---

to homeland security activities so worthy of brief mention here. Protecting all electronics from such an attack is impractical (and modern electronic systems, with their low power requirements and low voltage tolerances, are inherently more vulnerable to such attacks than were vacuum tubes). But the country's infrastructure should not be allowed to fail catastrophically after such an attack; the period of recovery could last many months, during which time the country would have function like a premodern society. Devising protections to key nodes of major infrastructure is estimated to cost about one to three percent of total system cost, if done when a system is first being built. But retrofitting protections onto existing equipment might be an order of magnitude more expensive, implying costs reaching well into the tens of billions of dollars. This suggests a two-track approach to protection, redressing glaring vulnerabilities where feasible in the short term (that is, hardening key electronics used by major infrastructure, or purchasing backup systems), while planning to gradually eliminate other vulnerabilities as infrastructure is modernized in the coming years. See 65 Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack,* Volume I: Executive Report (2004), available at *www.iwar.org.uk/iwar/resources/emp/04–0722emp.pdf*, accessed February 17, 2005; and Testimony of Frank Gaffney before the House Committee on the Budget, U.S. Congress, February 16, 2005.

[66] Justin Blum, "Report Assesses Risks of Attack on Tankers," *Washington Post,* December 22, 2004, p. E1.

[67] Associated Press, "Collins Suicide Attack Warning," Lloyd's List, July 5, 2004, p. 12.

[68] See *Protecting the American Homeland,* pp. 54—56.

[69] See Eric Lipton and James Glanz, "New Rules Proposed to Help High-Rises Withstand Attacks," *New York Times,* March 6, 2002, p. A1; Letter from Michael C. Janus, Battelle Corporation, December 1, 2001, to Michael O'Hanlon; Ann Gerhart, "Tom Ridge, on High Alert," *Washington Post,* November 12, 2001, p. C1; and Statement of Arden Bement, Director, National Institute of Standards and Technology, Hearing before the Committee on Science, U.S. House of Representatives, 107 Cong. 2 sess. (March 6, 2002).

CONCLUSION

The number of sites that might be targeted in the United States is daunting, and a rigorous means of protecting the country comprehensively is unaffordable (if even conceivable). But the United States has a more limited number of sites of particular interest—where thousands of individuals routinely congregate, where the economy has important choke points or centers of activity, where the symbolic and political effect of any attack could be hugely significant. Most such sites are in the private sector, which holds 85 percent of the nation's infrastructure, though an important number are clearly public too. By focusing on this category of key locations (and establishing different tiers of necessary protection within that category), and by using insurance makrets and related mechanisms to give private owners incentives to adopt best practices at reasonable cost, the country's vulnerability to truly catastrophic terrorism can be substantially mitigated. Since 9/11, we have moved towards this objective. But we have a great distance still to go.

---

United States Government Accountability Office

GAO

Testimony
Before Congressional Subcommittees
Committee on Homeland Security
U.S. House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, October 31, 2007

# CRITICAL INFRASTRUCTURE PROTECTION

## Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies

Statement of David A. Powner
Director, Information Technology Management Issues


GAO-08-64T

GAO
Accountability · Integrity · Reliability

# Highlights

Highlights of GAO-08-64T, a testimony before congressional subcommittees, Committee on Homeland Security, U.S. House of Representatives

## Why GAO Did This Study

The nation's critical infrastructure sectors—such as banking and finance, information technology, and public health—rely on computerized information and systems to provide services to the public. To fulfill the requirement for a comprehensive plan, including cyber aspects, the Department of Homeland Security (DHS) issued a national plan in June 2006 for the sectors to use as a road map to enhance the protection of critical infrastructure. Lead federal agencies, referred to as sector-specific agencies, are responsible for coordinating critical infrastructure protection efforts such as the development of plans that are specific to each sector. GAO was asked to summarize a report being released today that identifies the extent to which the sector plans addressed key aspects of cyber security, including cyber assets, key vulnerabilities, vulnerability reduction efforts, and recovery plans. In the report, GAO analyzed each sector-specific plan against criteria that were developed on the basis of DHS guidance.

## What GAO Recommends

In its report, GAO recommends that the Secretary of Homeland Security request that, by September 2008, the sector-specific agencies develop plans that fully address all of the cyber-related criteria. In written comments on a draft of the report, DHS concurred with GAO's recommendation.

To view the full product, including the scope and methodology, click on GAO-08-64T. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.

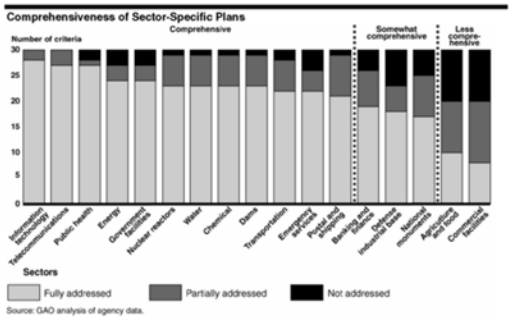
October 31, 2007

CRITICAL INFRASTRUCTURE PROTECTION

# Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies

## What GAO Found

The extent to which the sectors addressed aspects of cyber security in their sector-specific plans varied; none of the plans fully addressed all 30 cyber security-related criteria. Several sector plans—including the information technology and telecommunications sectors—fully addressed many of the criteria, while others—such as agriculture and food and commercial facilities—were less comprehensive. The following figure summarizes the extent to which each plan addressed the 30 criteria.




Source: GAO analysis of agency data.

In addition to the variations in the extent to which the plans covered aspects of cyber security, there was also variance among the plans in the extent to which certain criteria were addressed. For example, all plans fully addressed identifying a sector governance structure for research and development, but fewer than half of the plans fully addressed describing any incentives used to encourage voluntary performance of risk assessments. The varying degrees to which each plan addressed the cyber security-related criteria can be attributed in part to the varying levels of maturity in the different sectors.

DHS acknowledges the shortcomings in the plans. DHS officials stated that the sector-specific plans represent only the early efforts by the sectors to develop their respective plans. Nevertheless, until the plans fully address key cyber elements, certain sectors may not be prepared to respond to a cyber attack against our nation's critical infrastructure. As the plans are updated, it will be important that DHS work with the sector representatives to ensure that the areas not sufficiently addressed are covered. Otherwise, the plans will remain incomplete and sector efforts will not be sufficient to enhance the protection of their computer-reliant assets.

Mr. Chairman, Madame Chairwoman, and Members of the Subcommittees:

Thank you for the opportunity to join in today's hearing to discuss transitioning critical infrastructure protection sector-specific plans into action. Because the nation's critical infrastructure relies extensively on computerized information systems and electronic data to maintain the nation's security, economy, and public health and safety, the security of those systems and information is essential. To help address critical infrastructure protection, federal policy has established a framework for public- and private-sector partnerships.[1] It has also identified 17 critical infrastructure sectors that are largely owned and operated by the private sector, including banking and finance, information technology, telecommunications, energy, and public health and healthcare.

Federal policy requires the development of a national plan by the Department of Homeland Security (DHS) to outline national goals, objectives, milestones, and key initiatives as well as the development of individual critical infrastructure sector plans—referred to as sector-specific plans—to outline how a sector's public and private stakeholders will implement the national plan. Lead federal agencies, referred to as sector-specific agencies (including DHS, Department of the Treasury, and the Department of Health and Human Services), are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors.

DHS issued a National Infrastructure Protection Plan (NIPP) in June 2006 to be used as a road map for how DHS and other relevant stakeholders are to use risk management principles to prioritize protection activities within and across the sectors in an integrated, coordinated fashion. NIPP requires each of the lead federal agencies associated with the 17 critical infrastructure sectors to develop sector-specific plans to address how the sectors' stakeholders would implement the national plan and how they would improve the security of their assets, systems, networks, and functions. These plans are to, among other things, describe how the sector will identify and prioritize its critical assets, including cyber assets, and define approaches the sector will take to assess risks and develop

[1]The White House, *Homeland Security Presidential Directive 7* (Washington, D.C.: Dec. 17, 2003). Department of Homeland Security, *National Infrastructure Protection Plan*, (Washington, D.C.: June 2006).

programs to protect those assets. DHS announced the release of the 17 sector plans on May 21, 2007.

As requested, our testimony today will summarize our report being released today on the cyber security aspects of the critical infrastructure protection sector-specific plans.[2] In the report, we analyzed each sector-specific plan against 30 criteria that we developed based on DHS guidance. The 30 criteria are shown in appendix I. The report contains a detailed overview of the scope and methodology we used. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

## Results in Brief

The extent to which the sectors addressed key aspects of cyber security in their sector-specific plans varied; none of the plans fully addressed all 30 cyber security-related criteria. Several plans—including those from the information technology and telecommunications sectors—fully addressed many of the criteria, while others—such as those from the agriculture and food and commercial facilities sectors—were not as comprehensive. In addition to the varying degrees with which the sector-specific plans covered aspects of cyber security, the plans as a whole addressed certain criteria more comprehensively than they did others. For example, all 17 plans fully addressed the criterion to identify a sector governance structure for research and development, while only 7 plans fully addressed the process for identifying the consequences of cyber attacks. Further, only 3 plans fully addressed the criterion to describe incentives used to encourage voluntary performance of risk assessments.

The varying degrees to which each plan addressed the cyber security-related criteria can be attributed in part to the varying levels of maturity of the different sectors: that is, sectors where stakeholders had more experience working together on critical infrastructure issues generally had more comprehensive and complete plans than those in which their stakeholders had less prior experience working together. Without comprehensive plans, certain sectors may not be effectively identifying, prioritizing, and protecting the cyber aspects of their critical infrastructure protection efforts. For example, with most sectors lacking a process for identifying the consequences of cyber attacks against their assets, our

[2]GAO, *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-113 (Washington, D.C.: Oct. 31, 2007).

nation's sectors could be ill-prepared to respond properly to a cyber attack.

To assist the sectors in securing their cyber infrastructure, we made a recommendation in our report to the Secretary of Homeland Security to request that by September 2008, the sector-specific agencies' plans address the cyber-related criteria that have not been fully addressed. In written comments on a draft of the report, DHS concurred with our recommendation.

## Background

Our nation's critical infrastructures—such as banking and finance, information technology, telecommunications, energy, and public health and healthcare—rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data, referred to as cyber critical infrastructure protection, is essential to preventing disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Due in part to the importance of and increasing reliance on these electronic systems, we designated cyber critical infrastructure protection, in conjunction with protecting the federal government's information systems, as a high risk area in 2003. In January 2005 and 2007, we identified cyber critical infrastructure protection as a high-risk area because of the continuing concern about risks to information systems from escalating and emerging threats; the ease of obtaining and using hacking tools; the steady advance in the sophistication of attack technology; and the emergence of new and more destructive attacks.

As the focal point for critical infrastructure protection, DHS has many cyber security-related roles and responsibilities that are called for in law and policy. In May 2005, we identified 13 key cyber security responsibilities (see table 1).[3] These responsibilities are described in more detail in appendix II.

[3]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

**Table 1: DHS Key Cyber Security Responsibilities**

| | |
|---|---|
| 1. | Develop a comprehensive national plan for critical infrastructure protection, including cyber security. |
| 2. | Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector. |
| 3. | Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities. |
| 4. | Develop and enhance national cyber analysis and warning capabilities. |
| 5. | Provide and coordinate incident response and recovery planning efforts. |
| 6. | Identify and assess cyber threats and vulnerabilities. |
| 7. | Support efforts to reduce cyber threats and vulnerabilities. |
| 8. | Promote and support research and development efforts to strengthen cyber space security. |
| 9. | Promote awareness and outreach. |
| 10. | Foster training and certification. |
| 11. | Enhance federal, state, and local government cyber security. |
| 12. | Strengthen international cyber space security. |
| 13. | Integrate cyber security with national security. |

Source: GAO analysis of the Homeland Security Act of 2002, the Homeland Security Presidential Directive-7, and the National Strategy to Secure Cyberspace.

In May 2005, we reported that while DHS had initiated multiple efforts to fulfill its responsibilities, it had not fully addressed any of the 13 responsibilities.[4] For example, the department established the United States Computer Emergency Readiness Team as a public/private partnership to make cyber security a coordinated national effort and it established forums to build greater trust and information sharing among federal officials who have information security responsibilities and law enforcement entities. However, DHS had not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cyber security. In September 2006, we testified that DHS had made progress on its responsibilities, but that none had been completely addressed.[5]

One of DHS's key cyber security responsibilities is the development of a comprehensive national plan for securing both the physical and cyber

[4]GAO-05-434.

[5]GAO, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity*, GAO-06-1087T (Washington, D.C.: Sep. 13, 2006).

aspects of the key resources and critical infrastructure of the United States. The plan is to outline national strategies, activities, and milestones for protecting critical infrastructures. To fulfill this responsibility, in June 2006, DHS issued the National Infrastructure Protection Plan (NIPP) to guide how DHS and other relevant stakeholders are to use risk management principles to prioritize protection activities within and across the sectors in an integrated, coordinated fashion. NIPP requires each of the lead federal agencies associated with the 17 critical infrastructure sectors to develop sector-specific plans to address how the sectors' stakeholders would implement the national plan and how they would improve the security of their assets, systems, networks, and functions. As part of these efforts, DHS provided guidance to the sectors for developing their sector-specific plans, including guidance on cyber aspects.

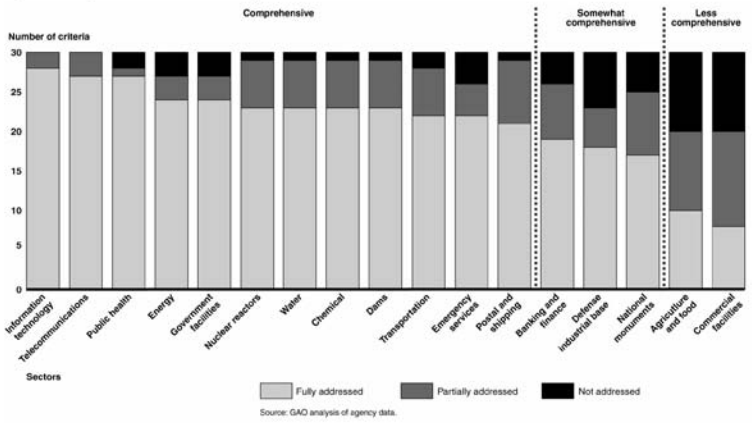
To strengthen DHS's ability to implement its cyber security responsibilities and to resolve underlying challenges, we have made about 25 recommendations over the last several years. These recommendations focus on the need to (1) conduct threat and vulnerability assessments, (2) develop a strategic analysis and warning capability for identifying potential cyber attacks, (3) protect infrastructure control systems, (4) enhance public/private information sharing, and (5) facilitate recovery planning, including recovery of the Internet in case of a major disruption. For example, in May 2005, we recommended, among other things, that DHS prioritize key cyber security responsibilities, including: performing a national cyber threat assessment and facilitating sector cyber vulnerability assessments. DHS has made varying levels of progress on many of these recommendations; however, additional efforts are needed to fully address them. Regarding the protection of infrastructure control systems, we issued a report on September 10, 2007, and testified on October 17, 2007, before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, House Committee on Homeland Security. In the report, we made a recommendation that DHS develop a strategy for coordinating control systems security efforts and enhance information sharing with control systems stakeholders.[6] Collectively, our recommendations provide a high-level road map for the agency to use in improving our nation's cyber security posture.

[6]GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but More Remains to Be Done*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007) and *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-08-119T, (Washington, D.C.: Oct. 17, 2007).

## Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies

In May 2007, DHS announced the release of 17 sector-specific plans to fulfill the NIPP requirement for individual sector plans. The extent to which the sectors addressed aspects of cyber security in their plans varied; none of the plans fully addressed all 30 cyber security-related criteria. Several plans—including those from the information technology and telecommunications sectors—fully addressed many of the criteria, while others—such as agriculture and food and commercial facilities—were less comprehensive. Figure 1 summarizes the extent to which each plan addressed the 30 criteria.

**Figure 1: Comprehensiveness of Sector-Specific Plans**




Source: GAO analysis of agency data.

In addition to the variations in the extent to which the plans covered aspects of cyber security, there was also variance among the plans in the extent to which certain criteria were addressed. For example, all plans fully addressed (1) identifying a sector governance structure for research and development, (2) describing how the sector-specific agency intends to manage its NIPP responsibilities; and (3) describing the sector's

coordinating mechanisms and structures. Also, at least 15 of the plans fully addressed (1) characterizing the sector's infrastructure, including the cyber reliance, (2) identifying stakeholder relationships for securing cyber assets, (3) describing a process for updating, reporting, budgeting, and training, and (4) describing a process for cyber-related information sharing. However, fewer than half of the plans fully addressed: (1) describing a process to identify potential consequences of cyber attacks, (2) describing any incentives used to encourage voluntary performance of risk assessments, (3) developing and using cyber metrics to measure progress, and (4) identifying existing cyber-related projects that support goals and identify gaps.

The varying degrees to which each plan addressed the cyber security-related criteria can be attributed in part to the varying levels of maturity of the different sectors. According to DHS officials, the sectors that have been working together longer on critical infrastructure issues generally have developed more comprehensive and complete plans than the sectors with stakeholders that had not previously worked together. For example, the plan for the energy sector was among those categorized as most comprehensive: the chemical sector had worked with DHS to improve the cyber component in its plans and it included most of the key information required for each plan element. Furthermore, the limited amount of time to complete the plans—6 months—was a factor for those sectors that had not previously been working together on critical infrastructure issues and were thus less mature.

DHS acknowledges the shortcomings we identified in the plans. Officials stated that the sector-specific plans represent only the early efforts by the sectors to develop their respective plans and anticipate that the plans will improve over time. Nevertheless, until the plans fully address key cyber elements, certain sectors may not be prepared to respond to a cyber attack against our critical infrastructure. As the plans are updated, it will be important that DHS work with the sector representatives to ensure that the areas not sufficiently addressed are covered. Otherwise, the plans will remain incomplete and sector efforts will not be sufficient to enhance the protection of their computer-reliant assets.

To assist the sectors in securing their cyber infrastructure, we recommended in our report that the Secretary of Homeland Security direct the Assistant Secretary for Infrastructure Protection and the Assistant Secretary for Cybersecurity and Communications to request that by September 2008, the sector-specific agencies' plans address the cyber-related criteria that were not fully addressed. In written comments on a

draft of the report, DHS's Director, Departmental GAO/OIG Liaison, concurred with our recommendation. In addition, he stated that DHS is currently working on an action plan to assist sectors in addressing cyber security issues not adequately addressed in the initial sector-specific plans.

In summary, without comprehensive plans, certain sectors may not be effectively identifying, prioritizing, and protecting the cyber aspects of their critical infrastructure. For example, with most sectors lacking a process for identifying the consequences of cyber attacks against their assets, our nation's sectors could be ill-prepared to respond properly to a cyber attack. In addition, without comprehensive plans, DHS cannot adequately identify where it and the rest of the federal government can most effectively assist in enhancing the security of the nation's critical infrastructures that are largely owned and operated by the private sector.

Ultimately, our nation needs to move beyond the planning stages of securing our critical infrastructures and public and private sector owners and operators of our nation's critical infrastructure need to effectively implement these plans. Implementation of these plans is more likely if DHS can successfully fulfill its role as a focal point for critical infrastructure protection. To accomplish this, DHS needs to address its 13 key responsibilities and our previous recommendations. For example, if DHS enhanced national cyber analysis and warning capabilities and provided assessments of cyber threats and vulnerabilities, it would be viewed as providing a valuable service to critical infrastructure owners, thus improving our nation's ability to prepare for, respond to, and prevent major cyber attacks from occurring.

Mr. Chairman and Madame Chairwoman, this concludes my statement. I would be happy to answer any questions at this time.

If you have any questions on matters discussed in this testimony, please contact me at (202) 512-9286 or by e-mail at pownerd@gao.gov. Other key contributors to this testimony include Scott Borre, Michael Gilmore, Nancy Glover, Barbarol James, and Eric Winter.

# Appendixes

## Appendix I: Cyber Security Criteria

| | |
|---|---|
| **Section 1: Sector Profile and Goals** | **Section 6: Measure Progress** |
| • Characterizes cyber aspects | • Ensures that integration of cyber metrics is part of measurement process |
| • Identifies stakeholder relationships for securing cyber assets | • Describes how cyber metrics will be reported to DHS |
| **Section 2: Identify Assets, Systems, Networks, and Functions** | • Includes developing and using cyber metrics to measure progress |
| • Describes process to identify cyber assets, functions, or elements | • Describes how to use metrics to guide future cyber projects |
| • Describes process to identify cyber dependencies/independences | **Section 7: Critical Infrastructure Protection Research and Development** |
| **Section 3: Assess Risks** | • Describes how technology developments are related to the sector's cyber goals |
| • Describes how the risk assessment process addresses cyber elements | • Describes process to identify cyber security technology requirements |
| • Describes a screening process for cyber aspects | • Describes process to solicit information on ongoing cyber research and development initiatives |
| • Describes methodology to identify potential consequences of cyber attacks | • Identifies existing cyber-related projects that support goals and identifies gaps |
| • Describes methodology for vulnerability assessments of cyber aspects | • Identifies research and development governance structure |
| • Describes methodology for threat analyses of cyber aspects | **Section 8: Managing Sector-Specific Agency Responsibilities** |
| • Describes incentives to encourage voluntary vulnerability assessments | • Describes sector-specific agency's management of NIPP responsibilities |
| **Section 4: Prioritizing Infrastructure** | • Describes process for updating, reporting, budgeting, and training |
| • Identifies entity responsible for prioritization of cyber aspects | • Describes sector's coordination structure |
| • Describes criteria and basis for prioritization of cyber aspects | • Describes process for investment priorities |
| **Section 5: Develop and Implement Protective Programs** | • Describes process for cyber-related information sharing |
| • Describes process to develop long-term protective plans for cyber aspects | |
| • Describes process to identify specific cyber-related program needs | |
| • Identifies programs to deter, respond, and recover from cyber attack | |
| • Addresses implementation and maintenance of protective programs | |

Source: GAO analysis based on DHS guidance.

# Appendix II: Thirteen DHS Cyber Security Responsibilities

| Critical infrastructure protection responsibilities with a cyber element | DHS responsibilities |
|---|---|
| 1. Develop a national plan for critical infrastructure protection that includes cyber security | Develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including information technology and telecommunications systems (including satellites) and the physical and technological assets that support such systems. This plan is to outline national strategies, activities, and milestones for protecting critical infrastructures. |
| 2. Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector | Foster and develop public/private partnerships with and among other federal agencies, state and local governments, the private sector, and others. DHS is to serve as the focal point for the security of cyber space. |
| 3. Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities | Improve and enhance information sharing with and among other federal agencies, state and local governments, the private sector, and others through improved partnerships and collaboration, including encouraging information sharing and analysis mechanisms. DHS is to improve sharing of information on cyber attacks, threats, and vulnerabilities. |
| **Responsibilities related to the cyber space strategy's five priorities** | |
| 4. Develop and enhance national cyber analysis and warning capabilities | Provide cyber analysis and warnings, enhance analytical capabilities, and develop a national indications and warnings architecture to identify precursors to attacks. |
| 5. Provide and coordinate incident response and recovery planning efforts | Provide crisis management in response to threats to or attacks on critical information systems. This entails coordinating efforts for incident response, recovery planning, exercising cyber security continuity plans for federal systems, planning for recovery of Internet functions, and assisting infrastructure stakeholders with cyber-related emergency recovery plans. |
| 6. Identify and assess cyber threats and vulnerabilities | Lead efforts by the public and private sectors to conduct a national cyber threat assessment, to conduct or facilitate vulnerability assessments of sectors, and to identify cross-sector interdependencies. |
| 7. Support efforts to reduce cyber threats and vulnerabilities | Lead and support efforts by the public and private sectors to reduce threats and vulnerabilities. Threat reduction involves working with the law enforcement community to investigate and prosecute cyberspace threats. Vulnerability reduction involves identifying and remediating vulnerabilities in existing software and systems. |
| 8. Promote and support research and development efforts to strengthen cyber space security | Collaborate and coordinate with members of academia, industry, and government to optimize cyber security-related research and development efforts to reduce vulnerabilities through the adoption of more secure technologies. |
| 9. Promote awareness and outreach | Establish a comprehensive national awareness program to promote efforts to strengthen cyber security throughout government and the private sector, including the home user. |
| 10. Foster training and certification | Improve cyber security-related education, training, and certification opportunities. |
| 11. Enhance federal, state, and local government cyber security | Partner with federal, state, and local governments in efforts to strengthen the cyber security of the nation's critical information infrastructure to assist in the deterrence, prevention, preemption of, and response to terrorist attacks against the United States. |
| 12. Strengthen international cyberspace security | Work in conjunction with other federal agencies, international organizations, and industry in efforts to promote strengthened cyber security on a global basis. |
| 13. Integrate cyber security with national security | Coordinate and integrate applicable national preparedness goals with the National Infrastructure Protection Plan. |

Source: GAO analysis of the Homeland Security Act of 2002, the Homeland Security Presidential Directive-7, and the National Strategy to Secure Cyberspace.