IMPLICATIONS OF POWER BLACKOUTS FOR THE NATION'S CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

JOINT HEARING

OF THE

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

AND THE

SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY

OF THE

SELECT COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 4, 2003 and SEPTEMBER 23, 2003

Serial No. 108–23

Printed for the use of the Select Committee on Homeland Security

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

99–793 PDF WASHINGTON : 2005

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

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
W.J. (BILLY) TAUZIN, Louisiana
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ-BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, Jr., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, *Ranking Member*
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
CHARLES GONZALEZ, Texas
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

JOHN GANNON, *Chief of Staff*
UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY

DAVE CAMP, Michigan, *Chairman*

KAY GRANGER, Texas, *Vice Chairwoman*
JENNIFER DUNN, Washington
DON YOUNG, Alaska
DUNCAN HUNTER, California
LAMAR SMITH, Texas
LINCOLN DIAZ-BALART, Florida
ROBERT W. GOODLATTE, Virginia
ERNEST ISTOOK, Oklahoma
JOHN SHADEGG, Arizona
MARK SOUDER, Indiana
JOHN SWEENEY, New York
CHRISTOPHER COX, California, *ex officio*
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
CHARLES GONZALEZ, Texas
JIM TURNER, Texas, *ex officio*

Subcommittee on Cybersecurity, Science, and Research and Development

MAC THORNBERRY, Texas, *Chairman*

PETE SESSIONS, Texas, *Vice Chairman*
SHERWOOD BOEHLERT, New York
LAMAR SMITH, Texas
CURT WELDON, Pennsylvania
DAVE CAMP, Michigan
ROBERT W. GOODLATTE, Virginia
PETER KING, New York
JOHN LINDER, Georgia
MARK SOUDER, Indiana
JIM GIBBONS, Nevada
KAY GRANGER, Texas
CHRISTOPHER COX, California, *ex officio*
ZOE LOFGREN, California
LORETTA SANCHEZ, California
ROBERT E. ANDREWS, New Jersey
SHEILA JACKSON-LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
KEN LUCAS, KENTUCKY
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
CHARLES GONZALEZ, Texas
JIM TURNER, TEXAS, *ex officio*

CONTENTS

WITNESSES

SEPTEMBER 4, 2003

SEPTEMBER 17, 2003

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD

THE ELECTRIC GRID, CRITICAL INTERDEPENDENCIES, VULNERABILITIES, AND READINESS

THURSDAY, SEPTEMBER 4, 2003

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE,
AND RESEARCH AND DEVELOPMENT,
AND
SUBCOMMITTEE ON INFRASTRUCTURE
AND BORDER SECURITY,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, DC

The subcommittees met, pursuant to call, at 1:00 p.m., in Room 2237, Rayburn House Office Building, Hon. Dave Camp, [chairman of the Subcommittee on Infrastructure and Border Security] presiding.

Present for the Subcommittee on Infrastructure and Border Security: Representatives Camp, Dunn, Smith, Shadegg, Gibbons, Sanchez, Markey, Dicks, Cardin, Slaughter, DeFazio, Jackson-Lee, and Pascrell.

Present for the Subcommittee on Cybersecurity, Science and Research and Development Subcommittee: Representatives Thornberry, Smith, Weldon, Camp, Linder, Lofgren, Sanchez, Andrews, Jackson-Lee, Christensen and Etheridge.

Also present: Representatives Cox and Turner.

Mr. CAMP. The joint hearing of the Subcommittee on Infrastructure and Border Security and Subcommittee on Cybersecurity, Science and Research and Development of the Select Committee on Homeland Security will come to order. The title of today's hearing is Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities and Readiness.

Good afternoon. Chairman Thornberry and I would like to welcome and thank you for attending today's hearing on infrastructure interdependencies.

The two subcommittees will hear from a panel of experts representing academia, industry and the national security community. We have the Honorable J. Cofer Black, Coordinator of the Office of the Coordinator for Counterterrorism, Department of State; Larry Mefford, Executive Assistant Director of Counterterrorism and Counterintelligence, Federal Bureau of Investigation.

Later, we will have Paul Gilbert, Former Panel Chair of Energy Facilities, Cities and Fixed Infrastructure from the National Research Council; Peter Orszag, Senior Fellow of the Brookings Institution; John McCarthy, Executive Director of the Critical Infra-

structure Protection Project, George Mason University; Karl Rauscher, Founder and President, Wireless Emergency Response Team; and Ken Watson, President and Chair, Partnership for Critical Infrastructure Security.

Thank you all for your participation. Your experience in critical infrastructure security and interdependencies make your testimony very valuable as the Homeland Security Committee continues to look at ways to strengthen America's critical infrastructure.

The Chair would like to inform members that several witnesses have precise departure times, particularly those from across the country who have flights to catch; and considering the expertise of our two panels and the importance of having sufficient time to hear their statements and ask questions, the Chair requests that members agree to a unanimous consent request to waive opening statements.

Seeing no objection, we will proceed.

Today's hearing will examine our Nation's complex critical infrastructure and the computers and networks that operate and sustain them. There has never been a more compelling time for our Nation to be educated on the threats and vulnerabilities that terrorists pose to the Nation through attacks on our critical infrastructure.

I would again like to thank our witnesses for being here. We will hear testimony from our government panel first, and we will begin with Ambassador Black. We have received your written testimony and ask that you briefly summarize in 5 minutes your statement. Thank you. You may begin.

STATEMENT OF THE HONORABLE J. COFER BLACK, COORDINATOR, OFFICE OF THE COORDINATOR FOR COUNTERTERRORISM, DEPARTMENT OF STATE

Mr. BLACK. Mr. Chairman, committee members, thank you for giving me the opportunity to speak here today. I look forward to discussing some of the key challenges we face in our global war on terrorism and how protecting critical infrastructure fits into the broader scope of our efforts in this area.

I have a longer formal statement which, with your permission, I would like to submit for the record.

Mr. CAMP. Without objection.

Mr. BLACK. Mr. Chairman, the phrase "critical infrastructure" covers many elements of the modern world. To cite a few examples: the computers we use to transfer financial information from New York to Hong Kong and other cities, the air traffic control systems for international and domestic flights and, of course, the electric grid systems.

The global critical infrastructure is both a contributor to, and a result of, the interdependence that exists among nations today. Critical infrastructure essentially means all the physical and virtual ties that bind us together, not only as a society but as a world. Terrorists know this, and they see attacking the very bonds that hold us together as one more way to drive us apart.

We have made significant progress in the war on terrorism, but the recent blackouts in this country serve as an urgent reminder of vulnerabilities that terrorists can possibly exploit. We continue

to believe that these blackouts were not the result of terrorist attacks. We know, however, that terrorists have plotted more devastating ways to bring massive disruption to our society.

My role in international cooperation: responsibility for protecting critical infrastructure has been assigned to the Secretary for Homeland Security. In my role as a coordinator for counterterrorism, I am responsible for managing the international effort to counter the terrorist threat through effective integration and coordination of the efforts of our allies and partners with our own.

The State Department plays an essential role in coordinating our government's response to matters surrounding critical infrastructure as those issues arise abroad. We are working closely on this with regional and global sorganizations including APEC, the OAS and the OECD and will convene a Southeast Europe cybersecurity conference next week in Sofia, Bulgaria, to raise awareness of this issue in that region. In addition, we have made this topic a priority of our global agenda by drafting three U.N. general Assembly resolutions on these issues. All these resolutions were adopted unanimously. The U.N.-sponsored World Summit on the Information Society will provide yet another forum where we can advance our goals on cybersecurity.

Antiterrorism assistance training. Bilaterally, the State Department is also working with countries across the globe. We are working with 16 nations on issues of critical infrastructure protection, countries ranging from Canada to India and Australia. Through the State Department's Antiterrorism Assistance Program, known as ATA, we offer three separate courses on cyberterrorism that address varying but equally important facets of the problem.

Additionally, ATA offers vital installation security courses to foreign law enforcement and security organizations. Sixteen countries on four continents have received the ATA vital installations course in the past two years and at least four more are planned for fiscal year 2004. Our recently developed cybersecurity course already has been provided to three countries. We plan to engage two more in fiscal year 2004.

Budget requests. Our planned courses for fiscal year 2004 reflect the administration's requested level of ATA funding. The Senate foreign operations appropriations bill provides the requested level, but the House mark is short by $16 million from the administration's $106 million request. These reductions could result in cutting at least several cybersecurity and vital installation courses during fiscal year 2004.

I must also add that funding was cut from our Terrorist Interdiction Program (TIP) that helps countries better control their borders and from our senior policy workshop program. I hope the distinguished members of this committee will encourage their colleagues on appropriations committees to support the full funding of these critical counterterrorist programs when the fiscal year 04 foreign operations appropriation bill goes to conference.

Mr. Chairman, the State Department also plays a role in helping to develop technology to counter threats to the critical infrastructure. My office co-chairs, with the Department of Defense, the Technical Support Working Group which conducts the national, interagency combatting terrorism technology research and develop-

ment program. Within the TSWG, an interagency working group on infrastructure protection, chaired by the Department of Defense with the FBI, focuses on meeting interagency requirements for technology development in the areas of cybersecurity, information analysis and physical protection.

The TSWG's cybersecurity projects focus on preventing or mitigating threats to computer networks vital to defense, transportation and critical infrastructure. Our projects are aimed at enhancing detection, prevention, response and alert capabilities to counter cyberattacks and harden computer systems.

For fiscal year 2004 the TSWG program has allotted approximately $10 million to fund rapid prototyping and development work on 25 projects in the infrastructure protection area based on requirements identified by the interagency community.

In other areas of activity, the Department also has provided some 18 key counterterrorist partner countries overseas with an intensive senior policy workshop. This helps them develop plans and procedures to mitigate any use by terrorists of weapons of mass destruction. We are also providing a series of workshops to improve energy security in the Caspian Basin, focusing on Kazakhstan.

I would like to put the issue of critical infrastructure into the context of our global efforts in the war on terrorism by discussing another type of critical infrastructure: the alliances, partnerships and friendships that we have worked so hard to build. These networks of diplomatic exchange and communication serve as the foundation on which our national security often rests.

I just returned this morning from a week in Colombia and Barbados where I worked to strengthen our partnerships on counterterrorism. In Colombia, kidnapping and drugs are primary sources of terrorist funding in that country. While in Colombia, I inaugurated a new $25 million anti-kidnapping initiative funded by the State Department that will provide training and equipment for Colombia's special police and military anti-kidnapping units.

In Barbados, I met with prime ministers from across the Eastern Caribbean. Important progress is being made in that region. Several Caribbean states are developing national and regional immigration alert systems so that they can better track and capture terrorists who cross their borders and are drafting counterterrorist legislation.

We have also built new relationships with the countries in the tri-border region—Brazil, Argentina and Paraguay. We have also initiated new counterterrorism partnerships with China, Russia and the central Asian republics.

Our success in this struggle depends heavily on those nations around the world that are working with us to defeat terrorism within their own borders. Pakistan has taken more than 500 terrorist suspects into custody. Morocco has arrested al Qaeda operatives planning attacks against our shipping. Many other nations around the world are helping us to uncover terrorist networks.

Since 9/11, the United States and its partners have detained more than 3,000 terrorists in over 100 countries. Also since 9/11, more than 30 nations have signed on to all 12 of the international antiterrorism conventions and protocols, and many more have be-

come parties to them. There has been an upsurge in the number of laws, both domestic and international, that deal with terrorism-related issues.

Regarding counterterrorism funding, a key part of our counterterrorism effort is the designation of terrorists and foreign terrorist organizations. The State Department, together with the Departments of Justice, Treasury and Homeland Security and the Intelligence Community, has been developing legal cases for the designation of terrorists and terrorist organizations so that we can block funding.

Since 9/11, over 170 countries and jurisdictions have issued orders to freeze terrorist assets. So far, we have frozen more than $136 million in terrorist funding and designated more than 290 terrorist groups and individuals, working hard to help other countries become more effective in stopping terrorists from raising and moving funds.

It is essential that we continue to work relentlessly to ensure that terrorists, whatever their ideology, religion or ethnicity, do not receive safe haven, funding or any other kind of support, both inside and outside our own borders. But with each of these victories, new challenges emerge. As the chains of commands in these organizations are stressed and broken, it becomes more difficult for terrorists to confer with their leaders and coordinate large-scale attacks. That is why we are seeing an increasing number of small-scale operations against softer targets.

One of the lessons our Nation learned a new on that tragic morning nearly 2 years ago was that the fates of all nations are linked. This lesson takes on new meaning when considered in the context of protecting our national and international critical infrastructures because, in the last analysis, it is precisely those global systems, structures and networks that serve as the foundation for all our efforts to bring freedom, prosperity and security to people around the world.

I thank you, Mr. Chairman; and I would be happy to take your questions when you so choose.

Mr. CAMP. Thank you, Ambassador.

[The statement of Mr. Black follows:]

PREPARED STATEMENT OF THE HON. COFER BLACK

Mr. Chairman, Committee Members:

Thank you for giving me the opportunity to speak here today. I look forward to discussing some of the key challenges we face in our global war on terrorism. It is a privilege to speak to you on the crucial issue of counterterrorism, and how protecting critical infrastructure fits into the broader scope of our efforts in this area.

Critical infrastructure means many different things. It means the computers we use to transfer financial data from New York to Hong Kong. It means the production facilities that distribute our food across the country and the sanitation systems that make our water safe to drink. It means the electronic signals that keep our planes in the air and our trains on proper course. At the most fundamental level, it means the very interconnectedness on which our society so heavily depends. But it also means something more.

We must remain mindful that global critical infrastructure is both a contributor to—and a result of—the interdependence that exists among nations today. It is because our ties to Europe and Asia are so strong that an attack on the banking systems in either of those places would have a powerful impact on our country. It is because we rely so much on our extensive trade relationships with nations around the globe that we must ensure that those products reaching our shores are safe to sell in this country. It is because we depend on global partnerships for our power

that a blackout in one country can trigger a blackout in another. Critical infrastructure essentially means all the physical and virtual ties that bind us together—not only as a society, but as a world. Terrorists know this, and they see attacking the very bonds that hold us together as one more way to drive us apart.

We have made significant progress in the war on terrorism, but the recent blackouts in this country serve as an urgent reminder that there remain vulnerabilities for terrorists to exploit. We continue to believe that these blackouts were not the result of terrorist acts. We know that terrorists have plotted more devastating ways to bring massive disruption to our society.

We know, for example, that terrorists have assessed the possibility of attacking our nuclear plants and our transportation systems. But, in the end, it does not matter to terrorists whether the target is an Embassy or a nightclub, a power grid, a hotel, or an unguarded building. The targets terrorists attack will no doubt vary widely, but the goal toward which they strive remains the same: to undermine the security and stability that Americans seek for themselves, their country, and the world.

STATE'S ROLE, INTERNATIONAL COOPERATION

In the United States, the responsibility for protecting critical infrastructure has been assigned to the Secretary for Homeland Security. In my role as the State Department's Coordinator for Counter-Terrorism, I am responsible for managing the international effort to counter the terrorist threat through the effective integration and coordination of the efforts of our allies and partners with our own.

The State Department plays an essential role in coordinating our government's response to issues surrounding critical infrastructure, as those issues arise abroad. We are working closely with regional and global organizations from APEC, the OAS, and the OECD, and will convene a Southeast Europe cyber security conference next week in Sofia, Bulgaria, to raise awareness of this issue in that region. In addition, we have made this topic a priority on our global agenda by drafting three UN General Assembly resolutions on issues related to information technology and cyber security—and all these resolutions were adopted unanimously. The UN-sponsored World Summit on the Information Society, which will be held in Geneva in December, will provide yet another forum where we can advance our goals on cyber security.

ATA TRAINING

The State Department is also engaged bilaterally on this issue with countries across the globe. We are working with sixteen nations on the issue of critical infrastructure protection—countries ranging from Canada to India and Australia. And through the State Department's Antiterrorism Assistance program (ATA), we offer three separate courses on Cyber Terrorism that address varying but equally important facets of the problem; preventive measures, techniques in responding to and investigating cyber attacks, and familiarizing senior level officials on dealing with the problems of a cyber incident.

Additionally, ATA offers Vital Installations Security courses to foreign law enforcement and security organizations. Sixteen countries on four continents have received the ATA Vital Installations course in the past two years and at least four more are planned for Fiscal Year 2004. Our recently developed Cyber Security course already has been provided to three countries, and we plan to engage two more in FY 2004.

Our planned courses for FY 2004 reflect the Administration's requested level of ATA funding. The Senate Foreign Operations Appropriation bill provides the requested level, but the House mark is short by $16 million from the Administration's $106 million request.

These reductions, if not restored in the Senate-House conference committee, would result in cutting at least several Cyber Security and Vital Installations courses during FY 2004. I might also add that funding was cut from our Terrorist Interdiction Program, which helps countries better control their borders, and from our Senior Policy Workshop program.

I hope the distinguished members of this Committee will encourage their colleagues on the Appropriations Committee to support the full funding of these critical counterterrorism programs when the FY 2004 foreign operations appropriations bill goes to the conference committee in the near future.

RESEARCH AND DEVELOPMENT

Mr. Chairman, the State Department plays a role in helping to develop technology to counter threats to the critical infrastructure. My office co-chairs, with the Department of Defense, the Technical Support Working Group (TSWG) which conducts the national, interagency combating terrorism technology research and development program. Within the TSWG, an interagency working group on Infrastructure Protection, chaired by DOD and the FBI, focuses on meeting interagency requirements for technology development in the areas of Cyber Security, Information Analysis, and Physical Protection. Other Departments and Agencies represented on the Infrastructure Protection Subgroup include the Departments of Homeland Security, Energy, Defense, Justice, Agriculture, Commerce, Treasury, and Transportation, as well as the Federal Emergency Management Agency, the Environmental Protection Agency, and the Nuclear Regulatory Commission.

The TSWG's Cyber Security projects focus on preventing/mitigating threats to computer networks vital to defense, transportation, and critical infrastructure. Our projects are aimed at enhancing detection, prevention, response, and alert capabilities to counter cyber attacks and harden computer systems. Our Information Analysis projects focus on enabling analysis and understanding of the information space. Specifically, we are working on technologies to enhance information storage, protection, and analysis. The TSWG's Physical Protection projects seek to develop standardized methodologies and decision aids for vulnerability analysis and enhanced protection of critical elements of the nation's infrastructure with particular emphasis on meeting the needs of Supervisory Control and Data Acquisition (SCADA) users and systems.

For FY 2004, the TSWG Program has allotted approximately $10M to fund rapid prototyping and development work on 25 projects in the Infrastructure Protection area based on requirements identified by the interagency community. A number of the Departments and Agencies included in the Infrastructure Protection Subgroup are contributing funds to support the work of the TSWG in this vital area.

In another area of activity, the Department also has provided some 18 key counterterrorist partners with an intensive Senior Policy Workshop to help them develop plans and procedures to mitigate any use by terrorists of weapons of mass destruction. We are also providing a series of workshops to improve energy security in the Caspian Basin, focusing on Kazakhstan. These are all part of the important effort to strengthen the ability of countries worldwide to counter the variety of terrorist threats that face us today.

GLOBAL CONTEXT

I would like to use my remaining time to put the issue of critical infrastructure into the context of our global efforts in the war on terrorism—by talking with you about another type of critical infrastructure: the alliances, partnerships, and friendships that we have worked so hard to build. Like other types of critical infrastructure, these networks of diplomatic exchange and communication serve as the foundation on which our national security often rests.

I just returned from a week of travel to Colombia and Barbados, where I worked to strengthen our partnerships on counterterrorism. In Colombia, I saw firsthand the powerful impact of our cooperation against kidnapping and drugs—both primary sources of terrorist funding in that country. While in Colombia, I had the pleasure of inaugurating a new $25 million Anti-kidnapping initiative—funded by the State Department—that will provide training and equipment for Colombia's special police and military anti-kidnapping units to enhance their ability to deal with the estimated 3,000 kidnapping incidents each year.

In Barbados, I met with Prime Ministers from across the Eastern Caribbean, and I am pleased to report that important progress is being made throughout that region. Several Caribbean states are developing national and regional immigration alert systems so that they can better track and capture terrorists who cross their borders. Some Caribbean countries are also making strides against money laundering and drug trafficking—and some are working to develop common laws to achieve common goals in the campaign against terrorism. I was pleased to see—in both Colombia and Barbados—that our partnerships are aimed at combating terrorism in a number of different ways.

In the fight against terrorism—triumph will not come solely, or even primarily, through military might. Rather, it will come through success on a variety of different fronts with a variety of different tools. We need better regional and global methods of collecting and exchanging intelligence and information, and better military coordination. We need more vigorous cooperation to sever the sources of terrorist funding. Our actions must help to win the trust not only of governments, but

of the people they represent. And success on each of these requires effective diplomacy.

DIPLOMACY

Diplomacy is the backbone of our campaign—for one simple reason: terrorism has no citizenship. The list of passports that terrorists—and their victims—carry is long indeed. Those 19 extremists who hijacked our planes on September 11, killed the innocent sons and daughters of more than 90 countries that day. Those men and women of the United Nations whom terrorists attacked in Baghdad last month, had come together from across the globe. Terrorism affects all corners of the world and we must be united, as a world, in fighting it.

Secretary of State Colin Powell has worked hard to forge new friendships and strengthen existing ones. Through our Smart Border Accords with Canada, we held the TOPOFF II exercises last May. This five-day, full-scale exercise involved top officials and response personnel and gave us a clearer picture of how our country would respond to attacks with weapons of mass destruction on major metropolitan areas. This exercise is just one example of the success old partnerships can produce in facing the new challenges that lie ahead.

On a global and regional level, we continue to work closely with organizations, ranging from NATO, the G–7, and the United Nations, to ASEAN, the OAS, and the OSCE. We have built new relationships on counterterrorism with countries like Brazil, Argentina, and Paraguay through the young "3+1" Counterterrorism Dialogue. We have also initiated new counterterrorism partnerships with China, Russia, and the Central Asian Republics. And many more nations hold promise for deepened engagement in the future.

Our success in this struggle largely rests with those nations around the world who are working with us to defeat terrorism within their own borders. Pakistan has taken more than 500 terrorist suspects into custody, including Ramzi bin al Shibh and Khalid Sheikh Mohammed. With Jordan's help, two individuals were arrested, both of whom we believe are responsible for the murder of USAID employee Laurence Foley in October, 2002. Morocco has arrested Al Qaida operatives planning attacks against our shipping interests. And Saudi Arabia has helped in many ways to capture terrorists and disrupt their activities. Many other nations around the world are helping us to uncover the extent of terrorist networks; chart the movements of their members; and master the means of their demise.

Just a few weeks ago, we accomplished a key goal in the war by capturing Hambali, the mastermind behind Bali bombing in October, 2002. Working together with the governments of Thailand and the Philippines, we added Hambali to the list of nearly two-thirds of the top Al Qaida leaders, key facilitators and operational managers whom we have either killed or captured in the past two years. And since 9/11, the United States and its partners and allies have detained more than 3,000 terrorists in over 100 countries.

And we are making measurable progress on many other fronts, as well.

COUNTERING TERRORISM FUNDING

Since 9/11, over 170 countries and jurisdictions have issued orders to freeze terrorists' assets—and so far, the international community has frozen more than $136 million in terrorist funding and designated over 290 terrorist groups and individuals. We are working hard to build capacity in those states that are on the front lines of the war on terrorism, so that they can better stop terrorists from raising and moving funds. Thanks to UN Security Council Resolution 1373, we now have specific criteria by which to measure national progress in blocking terrorist fundraising. And we are developing international standards and best practices, through both the Security Council's Counterterrorism Committee and the Financial Action Task Force.

Since 9/11, more than 30 nations have signed onto all 12 of the international antiterrorism conventions and protocols, and many more have become parties to them. There has been an upsurge in the number of laws—both domestic and international—that deal with terrorism-related issues. There are now more laws limiting terrorists' actions in more countries than ever before, and more governments are willing to enforce those laws. Our country has been involved in helping other nations strengthen their counterterrorism legislation and then, enforce it.

But with each of these victories, new challenges emerge. As the chains of command in these organizations are stressed and broken, as they were when we captured Hambali, it becomes more difficult for terrorists to confer with their leaders and coordinate large-scale attacks. That is why we are seeing an increasing number of small-scale operations against softer targets.

The more successful we are, the more likely it is that terrorists will act independently against unguarded targets. As a result, we will need to exercise heightened vigilance even as we continue making measurable progress on many fronts.

Another key part of our counterterrorism effort is the designation of terrorists and terrorist organizations. The State Department—together with the Departments of Justice, Treasury, and Homeland Security, and the Intelligence Community—has been developing legal cases for designating terrorists and terrorist organizations so that we can freeze funds and prevent attacks.

To do this, we rely primarily on two legal authorities. The first is the Antiterrorism and Effective Death Penalty Act of 1996 which amended the Immigration and Nationality Act, to authorize the Secretary of State to formally designate foreign terrorist organizations. The second one is the Executive Order on Terrorist Financing, which the President signed on September 23, 2001. These authorities block the property of designated terrorists and make it illegal to provide financing and other forms of material support to designated groups. Designating terrorists and their organizations is an important tool in the war on terrorism because it helps us curb their funding and invoke other sanctions. It is essential that we continue to work relentlessly to ensure that terrorists—whatever their ideology, religion, or ethnicity—do not receive safe haven, funding, or any other kind of support both inside and outside our own borders.

One of the lessons our nation learned anew on that tragic morning nearly two years ago was that the fates of all nations are linked—and that we deny this at our own peril. This lesson takes on new meaning when considered in the context of protecting our national and international critical infrastructures. Because, in the last analysis, it is precisely those global systems, structures, and networks that serve as the foundation for all our efforts to bring freedom, prosperity, and security to people around the world.

Thank you. I would be happy to take your questions

Mr. CAMP. Mr. Mefford.

STATEMENT OF LARRY A. MEFFORD, EXECUTIVE ASSISTANT DIRECTOR, COUNTERRORISM AND COUNTERINTELLIGENCE, FEDERAL BUREAU OF INVESTIGATION

Mr. MEFFORD. Mr. Chairman, members of the committee, thank you very much for the opportunity to speak about this very important topic.

The FBI, in cooperation with the Department of Energy, Department of Homeland Security, the North American Electrical Reliability Council and Canadian authorities, has aggressively investigated the August 14 power outages. To date, we have not discovered any evidence indicating that the outages were the result of activity by international or domestic terrorists or other criminal activity. The FBI Cyber Division, working with DHS, meanwhile has found no indication that the blackout was the result of a malicious computer-related intrusion.

This is a preliminary assessment only, and our investigative efforts continue today. The FBI has received no specific, credible threats to electronic power grids in the United States in the recent past; and the claim of the Abu Hafs al-Masri Brigade to have caused the blackout appears to be no more than wishful thinking at this stage. We have no information confirming the actual existence of this group, which has also claimed on the Internet responsibility for the August 5 bombing of the Marriott Hotel in Jakarta and the July 19 crash of an airplane in Kenya.

We remain very alert, however, to the possibility terrorists may target the electrical power grid and other infrastructure facilities of our country. They are clearly aware of the importance of electrical power to the national economy and livelihood.

For instance, al Qaeda and other terrorist groups are known to have considered energy facilities and other infrastructure facilities as possible targets.

Guerrillas and extremist groups around the world have attacked power lines—.

Mr. CAMP. You may continue.

Mr. MEFFORD. —as standard targets in the past.

Domestic terrorists have also targeted energy facilities in the United States. In 1986, the FBI disrupted a plan by a radical splinter group connected to an environmental organization to attack power plants in Arizona, California and Colorado.

The FBI has developed a multilayered approach to investigating potential threats to infrastructure facilities that brings together the strengths of law enforcement, the Intelligence Community, DHS, Department of Energy and private industry. This approach incorporates many new changes the FBI implemented since September 11 of 2001. They include:

The formation of a Counterterrorism Watch, which is a 24/7 operation center based at FBI headquarters which is responsible for collecting and coordinating all FBI threat-related activities in the United States, including all terrorist threats to the electric power grid of the country.

The creation of the National Joint Terrorism Task Force at FBI headquarters. This entity today incorporates over 35 Federal agencies and acts as a fusion point for the FBI and allows us to share information and coordinate activities quickly and efficiently. We have expanded the Joint Terrorism Task Forces in the country from 35 prior to September 11 of 2001 to almost 84 today. These task forces are now located in every major metropolitan area of the country and include major law enforcement agencies at the local, State and Federal level. All of these task forces have opened lines of communications with the electric power industry to share information and enhance preventive efforts.

The U.S. intelligence Community is also a key component of these task forces.

We have also enhanced our capabilities in the FBI's Counterterrorism Division by significantly increasing personnel, including about a five-fold increase in personnel, which includes a major increase in analytical personnel as well as FBI special agents.

We have formed the FBI Cyber Division to improve the FBI's ability to address Internet crime and computer intrusions and threats to our computer networks. This includes potential terrorist threats to our utility computer networks and power grids.

We have formed the Office of Intelligence to rapidly improve our ability to manage our databases effectively and to analyze threats and other related intelligence data.

We have also joined forces with many different agencies, including DHS in establishing and operating the Foreign Terrorism Tracking Task Force, the Terrorism Threat Integration Center and the Terrorism Financing Operations Section. All of these entities are designed to improve information exchange, enhance coordination and help us do a better job of preventing terrorism in the United States, which is our number one priority in the FBI.

In close coordination with DHS, the FBI works with the Information Sharing and Analysis Centers, the ISACs, that have been established around the country and members of the FBI's InfraGard program. Both the ISACs and InfraGard were established to facilitate information sharing between industry and law enforcement and to alert industry to potential threats and capitalize on private industry knowledge to assess threat information. Today, the FBI's InfraGard program consists of over 8,000 companies located in all 50 States and serves as an important link between the FBI and the private sector. This link is used by the FBI to exchange information to help us defend against terrorist attacks and is a vital part of the FBI's national strategy to prevent and disrupt terrorist activities in the U.S. .

In summary, we have developed a comprehensive and robust mechanism to deter and disrupt potential terrorist attacks, including attacks on the electrical power grids of the country; and we are working on a 24/7 basis with our partners in law enforcement and the Intelligence Community to constantly improve our preventive capabilities. Understanding that the number of critical infrastructure targets is so vast and facilities spread so widely that no system can be perfect, the structure of private and government entities acting in coordination will also provide an effective response in the unfortunate event of an attack.

I thank you, and I look forward to questions.

[The statement of Mr. Mefford follows:]

PREPARED STATEMENT OF LARRY A. MEFFORD

The FBI, in cooperation with the Department of Energy (DOE), the Department of Homeland Security (DHS), the North American Electrical Reliability Council (NERC), and Canadian authorities aggressively investigated the 14 August 2003 power outages. To date, we have not discovered any evidence indicating that the outages were the result of activity by international or domestic terrorists or other criminal activity. The FBI Cyber Division, working with DHS, meanwhile, has found no indication to date that the blackout was the result of a malicious computer-related intrusion, or any sort of computer worm or virus attack.

The FBI has received no specific, credible threats to electronic power grids in the United States in the recent past, and the claim of the Abu Hafs al-Masri Brigade to have caused the blackout appears to be no more than wishful thinking. We have no information confirming the actual existence of this group, which has also claimed on the Internet responsibility for the 5 August bombing of the Marriott Hotel in Jakarta and the 19 July crash of an airplane in Kenya.

We remain very alert, however, to the possibility terrorists may target the electrical power grid and other infrastructure facilities. They are clearly aware of the importance of electrical power to the national economy and livelihood.

- Al-Qa'ida and other terrorist groups are known to have considered energy facilities—and other infrastructure facilities—as possible targets.
- Guerillas and extremist groups around the world have attacked power lines as standard targets.
- Domestic extremists have also targeted energy facilities. In 1986, the FBI disrupted a plan by a radical splinter element of an environmental group to attack power plants in Arizona, California, and Colorado.

Terrorists could choose a variety of means to attack the electrical power grids if they choose to do so, ranging from blowing up power wire pylons to major attacks against conventional or nuclear power plants. We defer to DHS, however, for an assessment of the vulnerabilities of the electrical power system and the necessary responses to damage to various types of power facilities.

The FBI has developed a multilayered approach to investigating potential threats to infrastructure facilities that brings together the strengths of law enforcement, the Intelligence Community, DHS, DOE, and Industry.

• CT Watch is the FBI's 24/7 "threat central" for counterterrorism threat information. CT Watch is located within the Strategic Information and Operations Center (SIOC) at FBI Headquarters, and is the primary point of notification for all potential terrorism threats. Upon notification of a potential threat, CT Watch immediately passes the threat information to the DHS Homeland Security Operations Center (HSOC) through DHS representatives detailed to CT Watch. CT Watch then notifies each FBI field office Joint Terrorism Task Force (JTTF) that may be affected by the threat. CT Watch also notifies the National Joint Terrorism Task Force (NJTTF) and the appropriate FBI counterterrorism operational sections. This interagency coordination not only ensures that relevant government agencies are notified of the threats, but also that involved JTTFs take timely action and appropriate remedial action. This is especially noteworthy given that the 84 JTTFs in existence today incorporate all major law enforcement agencies in the country.

• The NJTTF is comprised of representatives from 35 government agencies, representing the intelligence, law enforcement, diplomatic, defense, public safety and homeland security communities, co-located at SIOC. The NJTTF acts as a point of fusion for terrorism threat information and manages the FBI's national JTTF program. The NJTTF coordinates closely with CT Watch, the JTTFs, DHS representatives assigned to the CT Watch and NJTTF, and the appropriate FBI sections to ensure threat information has been received by all appropriate entities across federal, state and local levels, as well as other JTTFs. The NJTTF accomplishes this by distributing threat information vertically to the JTTFs, and horizontally to other government agencies that are members of the NJTTF.

• Working with the state departments of homeland security and watch centers, the JTTFs across the country combine local law enforcement, Intelligence Community, and DHS representatives to fuse threat information and coordinate the local response to threats.

• Information from the JTTFs also flows up to the NJTTF, which ensures that it is received by all entities across the federal and pertinent local governments, as well as other JTTFs.

• In close coordination with DHS, the FBI works with the Information Sharing and Analysis Centers (ISACs) and members of the FBI's InfraGard program. Both the ISACs and InfraGard were established to facilitate information sharing between industry and law enforcement and to alert industry to potential threats and capitalize on private industry knowledge to assess threat information. Today, the InfraGard Program consists of over 8,000 companies located in all 50 states, and serves as an important link between the FBI and the private sector. This link is used by the FBI to exchange information to help us defend against terrorist attacks, including cyber threats from home and abroad. It is a vital part of the FBI's national strategy to prevent and disrupt terrorist activities in the US.

• The FBI Cyber Division investigates malicious computer intrusions and attacks on computers and networks, including attacks on networks that help control critical infrastructure. We are working with DHS and the electrical power ISAC to preserve and analyze computer logs from electrical companies in connection with the recent blackout.

The expansion of the FBI's Counterterrorism Division has significantly enhanced our ability to uncover threats to infrastructure facilities. In addition to CT WATCH, the FBI has established new sections to analyze terrorist communications and financial transactions for threat-related information, and we have more than quadrupled the number of analysts working on terrorism since September 11, 2001.

The increase in the FBI's resources devoted to terrorism, combined with the partnerships with other federal agencies, state and local law enforcement, and industry, provides a defense in depth that brings together the strengths of law enforcement and intelligence to respond efficiently and quickly to threats. Since September 11, 2001, the FBI has investigated more than 4,000 terrorist threats to the U.S. and the number of active FBI investigations into potential terrorist activity has quadrupled since 9/11.

No threat or investigative lead goes unanswered today. At Headquarters, in our field offices, and through our offices overseas, we run every lead to ground until we either find evidence of terrorist activity, which we pursue, or determine that the information is not substantiated. While we have disrupted terrorist plots since 9/11, we remain constantly vigilant as a result of the ongoing nature of the threat.

The Patriot Act is another change enhancing our ability to disrupt terrorist plots. The provisions of the Patriot Act allowing the freer flow of information between in-

telligence and law enforcement are essential to uncovering and foiling terrorist plots, and have allowed the FBI to fuse our law enforcement and intelligence missions so as to enhance our preventive capabilities. These improved capabilities are conducted pursuant to constitutional standards and relevant guidelines, and, in my view, have made the country safer for all. For example, the ability to share intelligence and law enforcement information was essential to the success of the recent indictment of a suspected member of the Palestinian Islamic Jihad for conspiracy.

- Given the potential to disrupt critical infrastructure via computer intrusion, the provision of the Act that allows law enforcement, with the permission of the system owner, to monitor computer trespassers is of particular note. This provision puts cyber intruders on the same footing as physical intruders, and means that hacking victims can seek law enforcement assistance in much the same way as burglary victims can invite police officers into their homes to monitor and catch burglars.
- The Patriot Act also bolsters the ban on providing material support to terrorists by clearly making it a crime to provide terrorists with "expert advice or assistance" and clarifies that material support includes all forms of money. These provisions have made possible the arrest and prosecution of extremists across the country and have enabled the US Government to cut terrorist organizations off at the source.

In summary, we have developed a comprehensive and robust mechanism to deter and disrupt potential terrorist attacks, including attacks on the electrical power grids of the country, and we are working on a 24/7 basis with our partners in law enforcement and the Intelligence Community to improve our preventive capabilities. Understanding that the number of critical infrastructure targets is so vast and facilities spread so widely that no system can be perfect, the structure of private and government entities acting in coordination will also provide an effective response in the unfortunate event an attack occurs.

Mr. THORNBERRY. [Presiding.] The Chair thanks both witnesses for their testimony.

I might mention to members that Mr. Camp and I intend to keep the testimony going and trade off going back and forth to vote. We are going to try to do the best we can as far as calling on members generally in the order they came to the hearing but also asking your patience as we try to figure it out as people come and go during this series of procedural votes.

I am going to submit any questions I have for this panel for the record and will not ask any questions at this time.

[The information follows:]

PREPARED STATEMENT OF THE HONORABLE CHRISTOPHER COX, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRMAN, SELECT COMMITTEE ON HOMELAND SECURITY,

Good afternoon. I would like to thank the subcommittee chairmen and ranking members for taking the lead on this important examination of the lessons learned as a result of the recent power outages, and the effects the blackout had to related critical infrastructure around the country.

I am especially pleased to welcome Ambassador Cofer Black, and FBI Executive Assistant Director Larry Mefford. Many of us know them as friends, colleagues, and dedicated public servants. I am particularly eager to hear from all of our witnesses their thoughts on the state of affairs for the protection of our national critical infrastructure. This is not the first hearing on these matters, and I am certain we will continue to explore the subject for years to come. The recent power outages on August 14, however, have given us a timely opportunity to revisit those things we already know, to ask ourselves if we are as prepared as we can be for similar events, and to further examine what we would do in the event that something worse occurred.

Initial review of the blackout tells us that it was not a terrorist event. Still, the Department of Energy and the North American Electric Reliability Council (NERC) have not completed their analysis of exactly what went wrong, and why. In our second part of this hearing on Sept. 17, hopefully the Department of Energy will have an answer for us. Until then, we can assume that our enemies took notice of the massive social and economic disruption the blackout caused. The blackout shutdown over 100 power plants, including 22 nuclear reactors, cutoff power for 50 million

people in eight states and Canada, including much of the Northeast corridor and the core of the American financial network, and showed just how vulnerable our tightly knit network of generators, transmission lines, and other critical infrastructure is.

Today, we seek to learn as much as possible about the interrelated nature of our critical infrastructure, the potential risks of physical as well as cyber-attacks on the infrastructure, and, quite literally, what happens when the lights go out. We are especially interested in the capabilities of our enemies to do us harm whether it be by blowing up a transformer station or by using the internet to disable our power grids.

Cyber attacks are a real and growing threat. The problem of cyber-security is unique in its complexity and in its rapidly evolving character. Cyber attacks are different from physical attacks since they can be launched from anywhere in the world and be routed through numerous intermediate computers. Cyber attacks require a different skill set to detect and counter, and are not limited to the risks posed from al-Quaida. They include threats posed by those criminals and hackers who are already attacking our infrastructure for their own amusement or using it to steal information and money. As the most information technology-dependent country in history, we remain uniquely vulnerable to cyber attacks that can disrupt our economy or undermine our national security.

The dependence of major infrastructural systems on the continued supply of electrical energy, and of oil and gas, is well recognized. Telecommunications, information technology, and the Internet, as well as food and water supplies, homes and worksites, are dependent on electricity; numerous commercial and transportation facilities are also dependant on natural gas and refined oil products. Physical or cyber attacks can amplify the impact of physical attacks on this critical infrastructure, and diminish the effectiveness of emergency responses.

We have all heard the reports that the 911 emergency systems in New York and Detroit failed during the blackout. New York City's computer-aided dispatch system for its fire department and rescue squad crashed. Reportedly, the New York City Fire Department had to monitor its 12,000 plus fire fighters, EMTs, and fire marshals manually because its computer tracking system couldn't boot up. Harlem's sewage treatment plant shut down without power for its pump. Water systems in Cleveland and Detroit could not handle the drop in power. Ohio Governor Bob Taft declared a state of emergency in Cleveland after all four pumping stations that lift water out of Lake Erie went out and residents were ordered to boil their water for days. The beaches were off limits for swimming after a sewage discharge into Lake Erie and the Cuyahoga River sent bacteria levels soaring.

As a group, the critical infrastructure sectors are backbone services for our nation's economic engine and produced approximately 31% of the Gross Domestic Product (GDP) in the year 2000. The blackout rippled through the economy. Nearly all manufacturers in southeast Michigan ground to a halt with the blackout. More than 50 assembly and other plants operated by General Motors Corp., Ford Motor Co., DaimlerChrysler, and Honda Motor Co. were idled by the cascading blackout. NOVA Chemicals shutdown plants in Pennsylvania, Ohio, and Ontario, Canada. Wallmart closed 200 stores in Canada and the United States. Marriott International saw 175 of its hotels in the Northeast lose power at the height of the blackout, and seven oil refineries in the U.S. and Canada temporarily shut down, worsening an already tight gasoline supply situation.

Hundreds of airline flights were cancelled. For many airports throughout the U.S. and Canada, the power failure has exposed the risk of fuel supply interruptions from electricity outages, since most hubs in North America are fed by pipeline systems. Many airports were not closed because of air traffic problems but due to inoperable systems on the ground. Tightened security measures established after 9–11 could not be maintained as power was not available for baggage screening machines. Refueling of aircraft stopped as hydrant systems and fuel farms lacked power.

The examples are endless, and experience shows us that the blackout is not alone in its capacity to disrupt the economy. The information super highway of the Internet has become a fast lane for computer viruses. A computer virus launched one morning can infect computers around the world in one day. The Slammer virus, launched in January of this year, reportedly infected 100,000 computers in its first ten minutes alone. Because of the SoBig computer virus, some rail routes of CSX were recently shut down on August 20, until a manual backup system started the trains running again. Without railroads to deliver coal, the nation loses 60 percent of the fuel used to generate electricity. Without electricity, fueling stations cannot pump fuel. Without diesel, the railroads will eventually stop running. When the railroads stopped running after 9/11 in order to guard hazardous materials, it only took

the city of Los Angeles two days to demand chlorine or face the threat of no drinking water—the railroads began operating again on the third day.

We know that terrorists have assessed the possibility of attacking our nuclear power plants and our transportation system. Al-Qaida computers seized in Afghanistan in 2001 had logged on to sites offering that offer software and programming instructions for the distributed control systems (DCS) and Supervisory-control and Data-acquisition (SCADA) systems that run power, water, transport and communications grids. All critical infrastructure industries are becoming increasingly dependent on information management and internal telecommunications systems to control and maintain their operations. The U.S. Dept. of Commerce's National Telecommunications & Information Administration (NTIA) published a study in January 2002 that detailed the myriad of uses the internal wireless communications systems to meet essential operational, management and control functions including two-way emergency restoration and field communications, monitoring power transmission lines and oil and natural gas pipeline functions to instantaneously respond to downed transmission lines or changes in pipeline pressure; sending commands to various remote control switches; inspecting 230,000 miles of rail track; managing wastewater, processing drinking water, and protective relaying.

SCADA systems could be attacked simply by overloading a system that, upon failure, causes other systems operations to malfunction as well. While there is some debate about the ability of a terrorist to successfully launch a cyber attack against a SCADA system, there are several examples of people or groups who have tried.

In March 2000 a disgruntled former municipal employee used the Internet, a wireless radio and stolen control software to release up to 1 million liters of sewage into the river and coastal waters of Queensland, Australia.

Similarly, NERC reports that over the past two years, there have been a number of "cyber incidents that have or could have directly impacted the reliable operation of the bulk electric system," including:

- In January 2003, When the SQL/Slammer worm caused an electric utility company to lose control of their SCADA system for several hours, forcing the company operations staff to resort to manual operation of their transmission and generation assets until control could be restored.
- In September 2001, the Nimda worm compromised the SCADA system of an electric utility, and then propagated itself to the internal project network of a major SCADA vendor via the vendor's support communications circuit, devastating the vendor's internal network and launching further attacks against the SCADA networks of the vendor's other customers.

More telling, perhaps, is a report issued in May 2002 by the Defense Department's Critical Infrastructure Assurance Program (CIAP) claiming that there was evidence of a coordinated cyber reconnaissance effort directed against the critical assets of at least two electric utilities participating in the Defense Department sponsored program. The report revealed that the probing appeared to come from the People's Republic of China, Hong Kong, and South Korea, with each probe building upon information previously garnered.

The blackout is yet another wake-up call to our nation. It demonstrated the fragility of our electric transmission system, and reminds us of the interdependent nature of our infrastructure. Clearly, we need to encourage private industry and government to raise the standards of cyber security, and to further enhance our infrastructure security against attack.

We can take heart, however, from the system's durability and our society's resilience. The blackout caused major disruption and much inconvenience, but it did not cause terror. Our training and preparations since 9–11 are beginning to show positive results. Keep in mind that power was restored within 48 hours to most of the effected areas.

It is too soon to identify specific equipment, measures, and procedures that did or did not work as intended on August 14, but it is important to note that large parts of the Eastern Interconnection power grid did not suffer the blackout. Protective relays within the distressed area operated to remove transmission lines, transformers, and generating units from service before they suffered physical damage, as designed. It was the action of those individual relays, operating to protect individual pieces of equipment, which eventually isolated the portion of the grid that collapsed from the remainder of the Eastern Interconnection. The fact that the equipment did not suffer physical damage is what made it possible to restore the system and service to customers as quickly as happened.

Another factor in the successful restoration of power was the restoration plans themselves. Restoring a system from a blackout requires a very careful choreography of re-energizing transmission lines from generators that were still on line in-

side the blacked-out area as well as from systems from outside the blacked-out area, restoring station power to the off-line generating units so that they can be restarted, synchronizing those generators to the interconnection, and then constantly balancing generation and demand as additional generating units and additional customer demands are restored to service. Many may not realize it takes days to bring nuclear and coal fired power plants back on-line. With those plants down, gas-fired plants normally used for peak periods were being used to cover baseload needs. The diversity of our energy systems proved invaluable.

Can we do better? Of course we can. We must. It is the job of this Committee to help ensure that we do.

I thank all our witnesses for being with us and look forward to your testimony.

PREPARED STATEMENT OF THE HONORABLE JAMES LANGEVIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF RHODE ISLAND

Thank you, Mr. Chairman.

I would like to welcome our witnesses, and express my appreciation for your willingness to come here for what I hope will be a very enlightening and productive hearing. I look forward to hearing from these distinguished experts on our infrastructure and how we regard it.

Mr. Chairman, it was with great expectation that we created the Department of Homeland Security and charged it with protecting us from terrorist threats and responding to emergencies here at home. This means not just controlling the border or patrolling airports, but making sure that the infrastructure that is vital to the daily operation of the United States is protected. Our early fears focused on our water supplies, but as we have seen in the last two weeks, weaknesses in our electrical grid and our communications systems may hold even greater potential for terrorist exploitation.

My concern is that we have not seen meaningful plans or progress from DHS in identifying critical infrastructure and existing risks. That step is critical before we can talk about how to protect it. This is a task DHS needs to be working on closely with local and state governments, though several states have decided to identify their critical infrastructure even without DHS support. I would like to hear from our panel what they believe the first steps should be for our national effort of infrastructure identification and protection and how they see DHS either leading or supporting the endeavor.

Again, I greatly appreciate all of our guests taking time to be here to discuss this vital issue.

PREPARED STATEMENT OF THE HONORABLE JIM TURNER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Thank you, Mr. Chairman.

The August 14, 2003, blackout left nearly 50 million people from the Midwest to the Northeast without power. Our relief that the massive blackout of 2003 does not appear to have been the work of terrorists should not divert our attention from the core question raised by the blackout: Have we done enough since September 11th, 2001 to protect our nation's critical infrastructures from potential terrorist attack?

Although there is no evidence that the blackout was caused by terrorism, this incident demonstrated that there are literally hundreds of thousands of potential targets that terrorists could choose to strike. These include power systems, chemical and nuclear plants, commercial transportation and mass transit, skyscrapers, and sports and concert venues. In addition to physical assets, we also need to protect cyber assets. Recent computer disruptions have had unexpected consequences on nuclear plants and other utilities.

Eighty-five percent of our critical infrastructure assets are privately owned. We must, therefore, work in partnership with the private sector to improve our national security. But we can not rely too heavily on voluntary private action. Companies seeking to maximize profits simply are unlikely to have the economic incentives to voluntarily make the investments necessary to raise security levels to where they need to be.

While there are many potential targets for terrorists, is there enough protection? Are our policies and initiatives equal to the urgency and gravity of the threats we face? I note that, with the two-year anniversary of September 11th approaching, we have not yet produced a comprehensive national threat and vulnerability assessment for our nation's critical infrastructure, which is the starting point for a serious effort to improve homeland security.

In the absence of sufficient action by critical infrastructure owners, we have a duty to take the initiative to protect the American people. The federal government

need not do so through the heavy hand of direct regulation. We must fully explore all the tools at our disposal. These can include targeted incentives or other assistance to owners of vulnerable critical infrastructure; higher standards for accountability when it comes to protecting assets that are at risk; faster timelines for implementing better security measures; and only when it is absolutely necessary, mandates and regulation.

Displaying stronger federal leadership to better protect critical infrastructure should not be viewed as undue interference, but rather the exercise of our constitutional duty to provide for the common defense of our nation.

Today, we face many threats to our country and our way of life. Our reaction to the blackout cannot be limited to seeking improvements in our electricity grid. This episode should be a wake-up call that we remain extremely vulnerable as a nation and that our governments at all levels, together with the private sector, must do more to increase the security of our critical infrastructures against potential terrorist attacks.

I want to thank the distinguished panel for appearing before us today. I look forward to your testimony as we seek to understand what progress we have made—and need to make—in increasing the security of all of our critical infrastructures.

Mr. THORNBERRY. I would yield to the gentlelady from California, ranking member of the Border Subcommittee, if she has any questions for this panel.

Ms. SANCHEZ. Thank you, Mr. Chairman.

I actually just had one question of Mr. Black, and that is the whole issue—one of the reasons we have called this with respect to the power blackouts that we had obviously in the metropolitan area of the Northeast. I know that you spoke broadly to us about the tri-state area and South America and other issues. In particular, have you had any particular instances where you have actually heard of terrorist groups or cells really—from the outside really taking a look at penetrating our grids here in the United States?

Mr. BLACK. We do know from intelligence collection activities of the U.S. Intelligence Community as well as great work done by law enforcement to give the FBI—these efforts have resulted in the identification of the objectives of a lot of these terrorist groups, particularly like the al Qaeda organization; and the essence of it is to attempt to stage large-scale attacks and, ideally, multiple attacks at the same time to create a lot of damage.

We do know that they look aggressively across the spectrum of potential targets to select those targets that they think they can work towards and achieve successfully as well as keep in mind that there is an active effort to identify their operatives and their operational activity.

Essentially, so far most of their effort has been to attempt to kill lots of people; and that is sort of the established modus operandi of terrorist groups, primarily using explosives, but we do know that some terrorist groups are branching out and looking at other potential target sets. This would include electrical systems of countries and potential targets.

But I am unaware at this point of a significant emphasis at this time on the electrical grid although they are always looking for vulnerabilities and they certainly will be aware if this event happened in the United States and see if there are any potential lessons learned that they can employ in potential future attack scenarios.

Ms. SANCHEZ. Because of the interest of time and because I still have to go over and vote, I have one last question. You may not

know the answer to this. I might have to go and ask somebody else. But I notice in the blackout that we had with respect to the Northwest that, in fact, Canada was included in some of those outages. I am from California. During our problems in California we were looking towards Mexico to see if we could get electricity up to our grid up from that area. The fact of the matter was that we are not connected with respect to our infrastructure grid down into Mexico. My question would be—if either one of you would be able to answer it and if not I will go look for another source—does that make us more vulnerable if in fact we are tied into an infrastructure that crosses a sovereign line?

Mr. BLACK. Well, I would be prepared fully to defer to my close FBI colleague on this. I think that question perhaps more appropriately should be addressed to the Department of Homeland Security officials and other people in the industry. It is a little technical I think at this stage, certainly for me.

Mr. MEFFORD. I would concur with that.

Ms. SANCHEZ. Okay. Thank you both, gentlemen.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank the gentlelady.

Does Chairman Cox have questions for this panel?

Mr. COX. Thank you, Mr. Chairman.

Mr. Mefford, first, thank you for being here. Mr. Black as well. Thank you very much for helping us with these difficult issues today.

In your past career, Mr. Mefford, you have been involved with setting up the FBI's cyberefforts. Let me ask both of you—and direct my question first to you because you might have come across this in your previous work—in the blackouts that we experienced in August, tripping mechanisms, at least to the extent that the system functioned as we expected, shut down generating capacity. Is it possible for those tripping mechanisms which are automated to be triggered intentionally from the outside through cyber means?

Mr. MEFFORD. That is a good question. I, unfortunately, would have to defer to the experts on that because I am not educated to the degree that I think I could give you a serious answer.

Mr. COX. Mr. Black, do you happen to know?

Mr. BLACK. Unfortunately, sir, I am unable to answer that also. I would have to refer that to an expert.

Mr. COX. Second, according to the Congressional Research Service, one of the means of protection that we have in our industrial utilities, in particular the electrical power generating industry, and transmission is, ironically, the wide variety of legacy codes that are employed, a lot of different instructions, a lot of different systems that are unfamiliar to modern day hackers. Do we run the risk inevitably when we modernize these facilities to make sure that we have the capacity that we need of updating everything for the convenience of hackers?

Mr. MEFFORD. Again, that is another excellent question; and I don't have the technical expertise personally to answer that. I mean, clearly that is a danger.

Mr. COX. Mr. Black, anything?

Mr. BLACK. Unfortunately, nor do I, sir.

Mr. COX. Well, I think that at least embedded in the problem is the potential solution, which is, if we are unwittingly the beneficiaries of a wide variety of different command instruction protocols, possibly when we update this critical infrastructure we can take care not to make it all homogenous but to make sure there is a wide variety in there that will serve as another means of foiling attacks.

Mr. Chairman, since there is a vote on the floor, I yield back.

Mr. THORNBERRY. Thank the chairman. Does the Gentleman from Texas, Ranking Member, wish to ask questions of this panel?

Mr. TURNER. Thank you, Mr. Chairman.

The main subject, of course, that you have addressed here today is the issue of the blackouts that we saw in August. To me, the main message for this committee flowing from that incident was to remind us once again how vulnerable we are; and the vulnerabilities of the power grid seems to me to be one of many potential vulnerabilities in our critical infrastructure. I don't know if, Mr. Mefford, you can answer this or not, or Mr. Black, but have either of you ever seen produced by the Department of Homeland Security or any other agency of the Federal Government a list in terms of priorities of protecting our critical infrastructure?

Mr. MEFFORD. I have not. I understand that there is something in process—in progress at this point, but I have not personally seen that.

Mr. BLACK. I have not seen it either, Congressman, but I understand that was one of the key reasons for the establishment of the Department of Homeland Security, to identify these vulnerabilities, so I am confident they are working on it. But, again, I think that question should be addressed to their representative, sir.

Mr. TURNER. Ambassador, you are correct. That is one of the principal responsibilities of the new Department of Homeland Security: to survey and assess our critical infrastructure, to determine our vulnerabilities, to assess the threats, and to match those threats, against those vulnerabilities and come up with a list of priorities for hardening our critical assets and making our country more secure and safer. In the absence of that, it seems that we will have a very difficult time knowing what our priorities should be and knowing where we should spend our limited dollars.

I know from your perspective, Ambassador, you, of course, are looking at the issue of terrorism from the international perspective. Do you feel that we are sufficiently providing information to the various agencies of the government regarding the intelligence that is available out there worldwide that we collect to allow the Department or the FBI or any other agency to really understand clearly what the current state of threats is at any given time?

Mr. BLACK. I think that is always a challenge, but I will say, Congressman, that certainly in the period since 9/11 there has been a tremendous intensification on this exact issue, with the United States playing a very key role in the constellation of nations that includes virtually every nation in the world except for a handful. And the objective is the effective and timely exchange of threat information and intelligence information. Both the American Intelligence Community and the U.S. law enforcement—I will turn to my colleague from the Bureau—are key in this.

The State Department's role would be referred to as the first among equals. It is our duty and our responsibility to facilitate this process, to enable the Intelligence Community and law enforcement, the military and the economic units in the United States to exchange information effectively with their foreign counterparts. Our job is to facilitate that process. I think we have made tremendous strides, truly. It may even be in sort of historical proportions. But I think there is a lot left to do. I think that everyone in the United States involved in this, as well as our foreign counterparts sees this as the objective, to have transparency and a timely exchange of intelligence and threat information. And I think the progress to date has been exceptionally good.

Mr. MEFFORD. I concur with that view. From the FBI's perspective we have made very significant progress in information sharing and analysis; and while it is not perfect, we are clearly headed in the right direction.

Mr. TURNER. Mr. Mefford, from your vantage point, do you have a sense for what is the most critical need for protecting critical infrastructure? We saw the failure of the power grid, as you said, not resulting from terrorism. But do you have any opinions regarding what portion of our infrastructure—in the absence of a clear delineation of vulnerabilities by the Department of Homeland Security—do you see any particular sector that, from your experience in observing the intelligence, would be most critical for us to be concerned about currently?

Mr. MEFFORD. I think if you look at the comprehensive intelligence environment, unfortunately, al Qaeda and groups such as al Qaeda have looked at and considered a variety of potential targets. We know that based on the analysis of information available to us, and it is across the board in a variety of infrastructures. So I am really not in a position to say that one is more than the other.

But, obviously, based on what we saw in 2001, the aviation and transportation industry is something of concern. We know that the Ambassador has mentioned previously in his remarks that certain terrorist groups like al Qaeda have talked about and focused on electrical power grids, for instance. But we haven't seen any specific or credible threats to date. So it is difficult for us at this point. Some of that is based on the nature of intelligence work inherently, that it is very difficult to get clear, precise pictures at various times and space. But I think we are making progress. Working with Homeland Security I think we will be able to fine-tune our efforts and improve efficiencies in the future.

Mr. TURNER. Thanks to both of you for being here with us today, and thank you for your service to our country.

Mr. BLACK. Thank you, sir.

Mr. CAMP. [Presiding.] Thank you.

Mr. Weldon, any inquiry?

Mr. WELDON. Thank you, Mr. Chairman. Thank you both for being here. Two questions.

Number one, last week, the Canadian news reported that there had been arrests of individuals with suspected terrorist ties who were flying planes and casing out a nuclear power plant in Canada; and my concern is that several months ago I shared some information with the Intelligence Community relative to an alleged threat

on a nuclear site in America with the first three letters of SEA which could be the Hanford site in Seattle or the Seabrook site in New Hampshire. These arrests troubled me greatly last week, and so I would ask the question, are we aware of any intelligence that has been brought forward indicating that perhaps a site—a nuclear site in America may in fact be the target of either al Qaeda or other terrorist networks and are you aware of the arrests in Canada?

Mr. MEFFORD. Yes, sir, we are aware of the arrests in Canada. We are working with our counterparts in Canada to address those issues. We are told, frankly, that there are no links to al Qaeda that have been uncovered to date and there are no specific threats against nuclear power plants, particularly no threats to power plants in the United States. But we continue to work with our allies north of us on a constant basis.

Mr. WELDON. Thank you.

Second line of questioning is, I happen to think, as a 17-year-member of the Armed Services Committee, now vice chairman, that the greatest threat to our Homeland Security in terms of both our energy supply and our electronics would be from a deliberate laydown of electromagnetic pulse. There wasn't much attention given to this certainly in this book. It is mentioned in one page and by people in my opinion who are responsible for protecting our infrastructure to the vulnerability of America to electromagnetic pulse. We on the Armed Services Committee put together a task force which is chaired by an ambassador that has been looking at our vulnerability to EMP.

One, have either of your agencies had any interaction and, if so, to what extent with the EMP Commission that has now been in force for about year?

And, Mr. Chairman, I would like to ask this question of every other witness before us. My feeling is that perhaps the answer will be for most of the witnesses they have had no interaction with the EMP Commission. But I will ask these two gentlemen. Have you had any direction interaction with the EMP Commission?

Mr. BLACK. I personally have not. That is not to say that others in the State Department may have. I just do not know, sir.

Mr. MEFFORD. I think my answer would be the same to that.

Mr. WELDON. Mr. Chairman, this to me is the greatest threat. Because, as you well know, all you would need would be a low-yield nuclear weapon, which we now know that North Korea has and Iran is trying to obtain, and the ability to put it up into the atmosphere, which we know that both Iran and North Korea have, a low-complexity missile; and by detonating that low-yield nuclear weapon off of the coast in the atmosphere the EMP laydown would fry all the electronic components within a given range within the U.S. In fact, our military has tested this type of capability in the past.

In testimony before the Armed Services Committee, we have not hardened our systems. Only our ICBM system is hardened, and almost the entirety of our energy complex in America would be vulnerable to any EMP laydown. I would ask each of you to comment whether or not you have had contact with the Commission. What is your assessment of the EMP threat to America and to our infrastructure?

Mr. MEFFORD. I would have to defer to the technical experts in the FBI. I don't have that knowledge personally.

Mr. BLACK. I would have to share that answer, sir.

Mr. WELDON. Mr. Chairman, I would also suggest that at some point in time we invite the board of the EMP Commission in before this committee; and I would hope that every witness before us here—because these are the utility companies, all of which would be rendered useless if any EMP laydown occurred, none of which I will tell you right now before they testify are hardened to deal with an electromagnetic pulse attack.

[The information follows:]

National Operations and Analysis Hub: NOAH

Policy Makers' Tool for Acting Against

Emerging Transnational Threats
and
Dangers to U.S. National Security

1999

Policy Makers Need Better Decision Support Tools

- Policy makers continue to work in a vacuum. Briefings and testimonies are the primary vehicles for transmitting information to leadership
- The volume of information germane to national issues is expanding so rapidly that policy makers are overwhelmed with data
- Policy makers need robust situational awareness over growing asymmetric threats to national security
- Policy makers need an overarching information and intelligence architecture that will quickly assimilate, analyze and display assessments and recommended course of action from many national agencies simultaneously
- Policy makers need tools to aid them in developing courses of action against threats to US policy, interests, or security
- Policy makers need virtual communications with one another
  - White House, Congress, Pentagon and at the agency levels should each have centers they can go to and receive, send, share, discuss, and collaborate on assessments before they act

National Level Collaboration Solution: NOAH

National Agencies

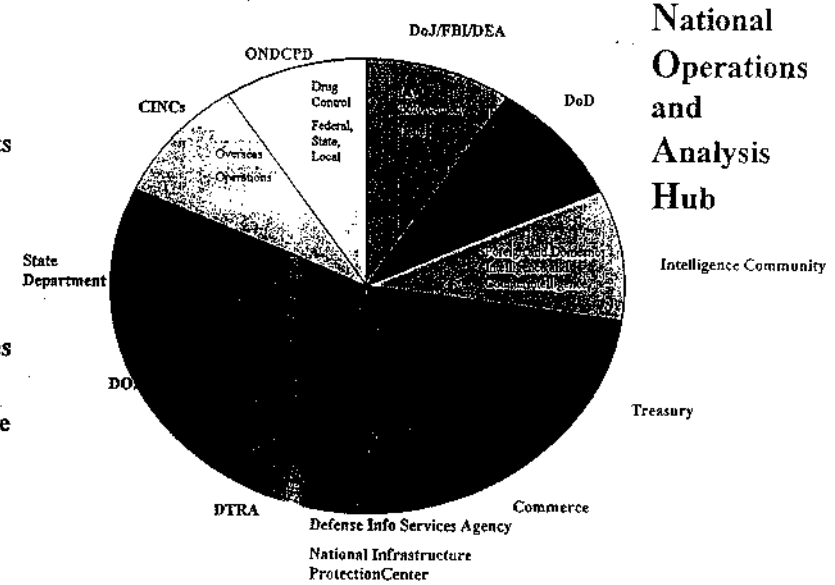
National Departments

Military Services

National Laboratories

White House

Congress



National Operations and Analysis Hub

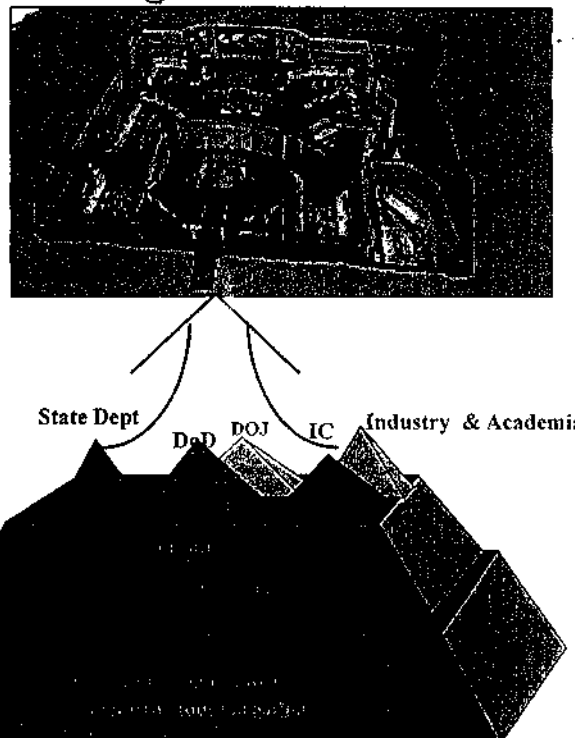
PDD 63's Info Sharing and Analysis Center

Universities

Civilian Corporations

Tasks Supported by NOAH's Overarching Collaborative Environment

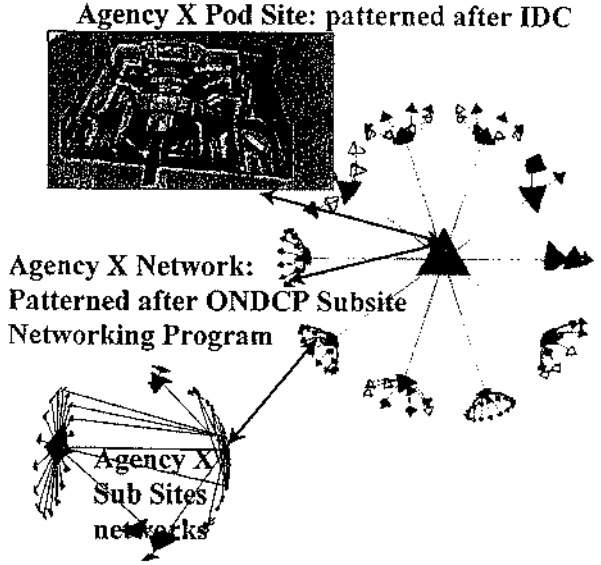
- Provide Multi Issue, Multi-agency Hybrid Picture to White House Situation Room, JCS,
- HUMINT Support
- Peacekeeping Missions
- Humanitarian Aid
- Battle Damage Assessment
- Develop and Leverage new Technologies of importance to national security
- Support Congressional Committees/Hearings



- Apply Analysis of Foreign Threat to Policy
- Provide Hybrid Situational Awareness Picture of the Threat
- Incorporate Industrial Efforts of interest to the Policy Maker
- Link academia directly to policy maker
- National Emergencies

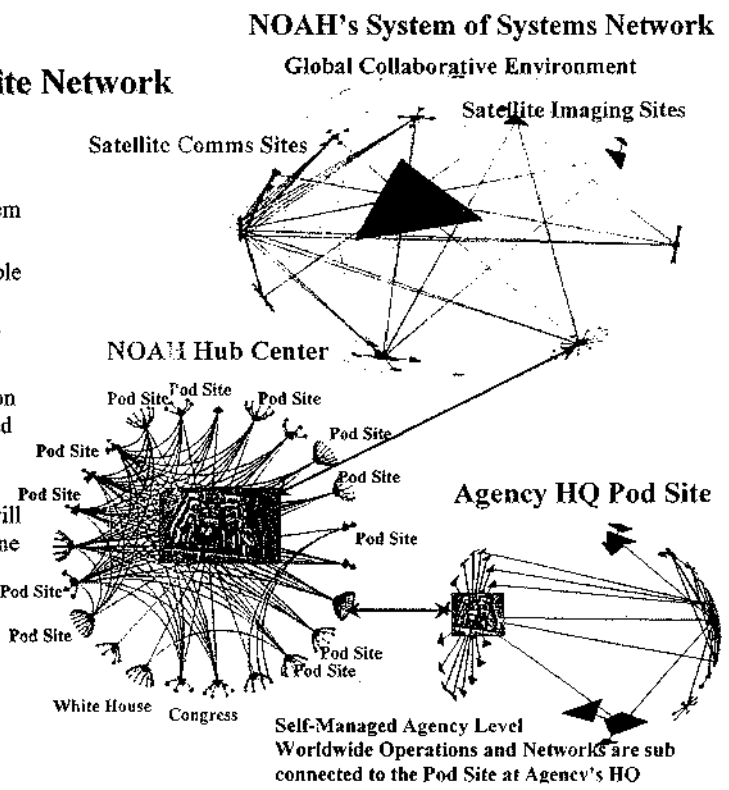
NOAH can Leverage Existing Networks to Address Diverse Issues

- NOAH's Hub Center is linked to other agency centers electronically
- Each key agency must possess a Pod Site and be connected to the NOAH network
- The Pod can consist of a large screen and appropriate connectivity for collaboration. Operations Centers can simply be converted to link into NOAH
- National Policy Makers cannot control agency Pods; agencies must post replicated data on the NOAH system so that sister groups can access data
- Support multi-level security requirements and can sanitize and "push" data to many types of users at many levels
- NOAH can address National, law enforcement and military needs. The situation will determine the mission
- Ties policy maker, military and law enforcement together
- Goal of the NOAH Hub Center is to apply agency operations, strategic analysis, tactical assessments to a course of action for the policy maker
- Optimizes groups of expertise within each organization--experts always on hand regardless of issue



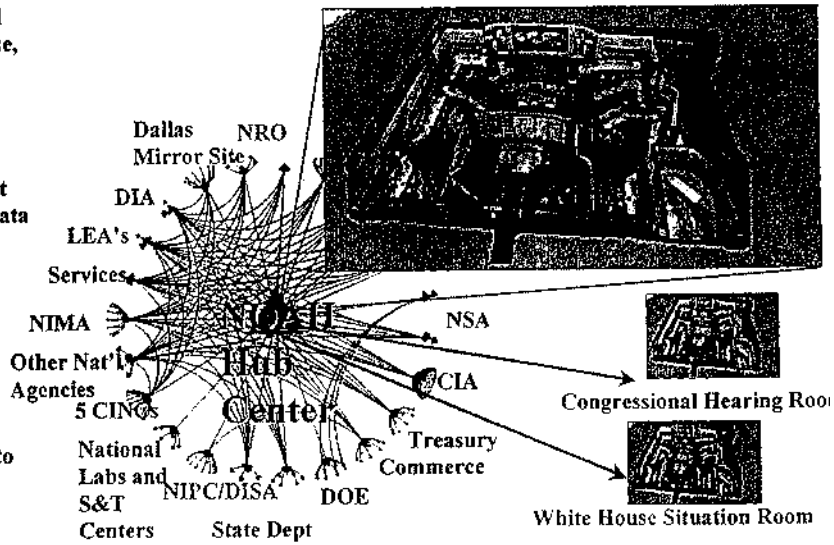
NOAH and Pod Site Network

- Part of national policy creation and execution system
- Will existing sites and connectivities where available
- Will share tools available at LIWA IDC so every agency has same tools
- All agencies will post data on NRO highway in a replicated format sensitive to classification
- NOAH's Global Network will use NRO System as backbone
- All centers connect to other centers electronically
- Mechanism for gathering, analyzing, displaying, tailoring, and disseminating all kinds of information quickly at the national level



Overview
National Operations and Analysis Hub

- Center dedicated to National Policy Makers at White House, Congress and National Agencies
- Provides System of System advanced technological communications environment to harvest, analyze, display data as needed
- Coordinate and Synchronize information among IC, S&T centers, Military Services
- Provide near real time situational awareness at the national level
- Link virtually via a pod site to every participating member agency
- Pod Sites designed to pull together Agency resources on single system of systems



NOAH's is staffed by members from participating agencies. The staff has a 24 x 7 high bandwidth, virtual connectivity to experts at agency Pod Sites. This provides decision makers with

Steps to Achieve NOAH Capability

- Establish baseline capability by building initial Hub Center and congressional virtual hearing room.Equip White House Situation Room to Collaborate with these sites.
- Staff the Hub Center with two reps from each of the 28 key participating agencies
- Link up NOAH internal and external collaborative environment
- Hook in Back up Site for redundancy and begin training on collaborative tools
- Build the 28 Key Agency Pod Sites along model of the Information Dominance Center at Fort Belvoir, VA
- Link all Pod Sites to NOAH hub center establish Protocols for Inter-agency data sharing
- Exercise live ability to retrieve, collate, analyze, display disparate data and provide policy makers course of action analysis at the NOAH Hub Center.
- Refine procedures and Protocols

Congress of the United States
House of Representatives
Washington, DC 20515–3807

July 30, 1999

e Jel re
ary ise

).C -1010

re:

ve t has come to create a central national level entity t n acquire, fuse
lispe a from many agencies in order to support the polic er in taking
thr m terrorism, proliferation, illegal technology diver espionage,
orms arfare and cyberterrorism. These challenges are be ng to overlap,
ng t tinction while posing increasing threats to our Nat

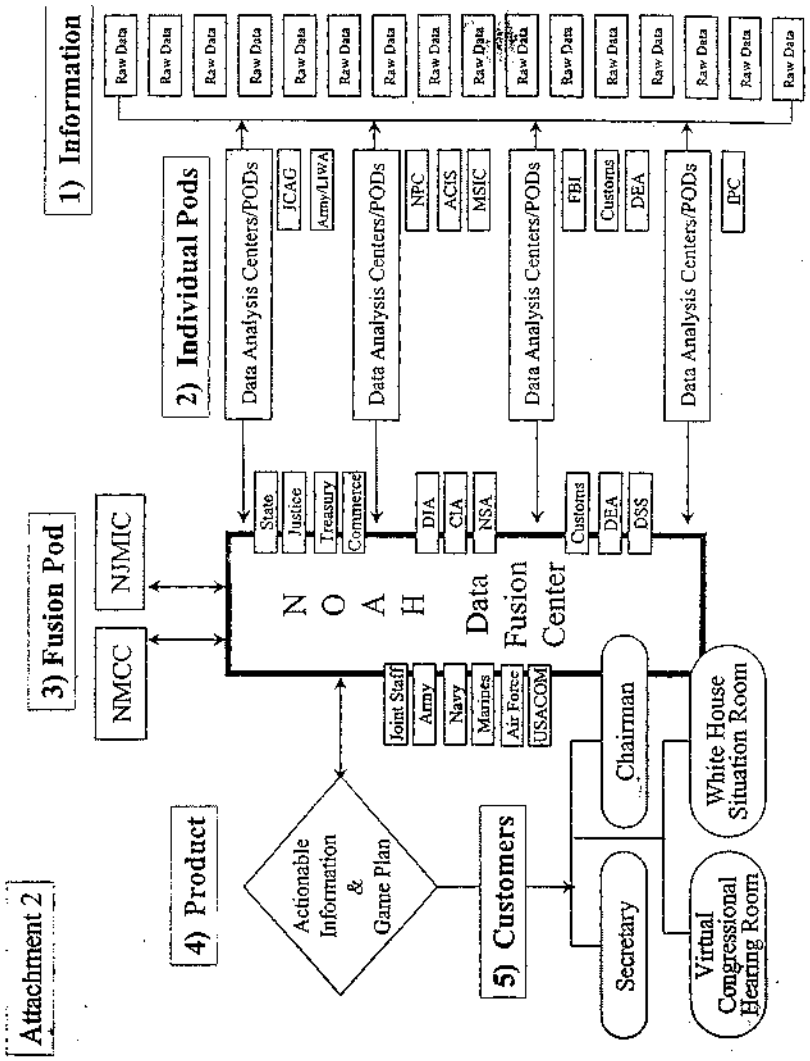
e wc tion to counter these emerging threats, we must fi lerstand their
on er, their patterns, the people and countries involve the level of
to c n. The Department of Defense has a un. opp to create a
tion r that can do this for the country. It would be patt fter the Army's
ation re Activity (LIWA) at Fort Belvoir, but would oper a much broader
ntity allow for near-time information and analysis to fi a central fusion
I w signate the National Operations Analysis Hub (NO I think this
as N will be provide a central hub built to protect our na rom the flood of

I wc e comprised of a system of agency-specified mini-c , or "pods" of participating agencies and services associated with growing national security concerns (attachment 1). NOAH would link the policymaker with action recommendations derived from fused information provided by the individual pods. NOAH would provide the automation and to all pods to talk together, share data and perspectives given situation in ne, c r-based environment.

Agencies Represented in the
National Collaborative Center

. Central Intelligence Agency.
. Defense Intelligence Agency.
. National Imagery and Mapping Agency
. National Security Agency
. National Reconnaissance Office
. Defense Threat Reduction Agency
. Joint Chiefs of Staff
. Army/LIWA
. Air Force
. Navy
. Marine Corps
. Joint Counter-Intelligence Assessment Group
. ONDCP
. FBI
. Drug Enforcement Agency
. U.S. Customs
. National Criminal Investigative Service
. National Infrastructure Protection Center
. Defense Information Systems Agency
. State Department
. Five CINCs
. Department of Energy
. Department of Commerce
. Department of the Treasury
. Justice Department
. Office of the Secretary of Defense
. National Military Command Center
. National Joint Military Intelligence Command

Elements to be connected to the national collaborative center would include the White House Situation Room, a Congressional Virtual Hearing Room and a possible redundant, or back-up site.


Attachment 2
1) Information
Raw Data
2) Individual Pods
Data Analysis Centers/PODs
JCAG
Army/LIWA
NPC
ACIS
MSIC
FBI
Customs
DEA
IPC
3) Fusion Pod
NMCC
NJMIC
NOAH Data Fusion Center
State
Justice
Treasury
Commerce
DIA
CIA
NSA
Customs
DEA
DSS
Joint Staff
Army
Navy
Marines
Air Force
USACOM
4) Product
Actionable Information & Game Plan
5) Customers
Chairman
Secretary
White House Situation Room
Virtual Congressional Hearing Room

Along with its system of connected agency pod sites, NOAH would permit the display of collaborative threat profiling and analytical assessments on a large screen. It would be a national level operations and control center with a mission to intergrate various imagery, data and analytical viewpoints for decision-makers in support of national actions. I see NOAH as going beyond the capability of the National Military Command Center (NMCC) and the National Joint Military Intelligence Command (NJMIC), providing recommended courses of action that allow us to effectively meet those emerging challenges from asymmetrical threats in near real-time. Given its mission, I believe that NOAH should reside in the Office of the Secretary of Defense (Attachment 2).

I am aware of the initiative to link counterintelligence groups throughout the community. I am also aware of the counterterrorism center at the CIA, the new National Infrastructure Protection Center at the FBI, and a new HUMINT special operations center. I have heard of an attempt to connect the Office of Drug Control Policy (ONDCP) and OSD assets with federal, state and local law enforcement agencies. I also have seen what the Army has done at LIWA, which has created a foundation for creating a higher-level architecture collaborating all of these efforts. Each of these independent efforts needs to be coordinated at the national level. I believe LIWA has created a model that should be used as a basis for creating the participating agency pod sites.

I do not expect that establishment of NOAH should exceed $10 million. Each agency involved could set up its own pod to connect with the central NOAH site or to exchange data with any of its participants. Each agency could dedicate monies to establish their own pod site, while the $50 million available in DARPA for related work could be used to establish the NOAH structure immediately.

The NOAH concept of a national collaborative environment supporting policy and decision-makers mirrors the ideas you have expressed to me in recent discussions, and it is a tangible way to confront the growing assymetrical threats to our nation. I have a number of ideas regarding staffing options and industry collaboration, and would appreciate the opportunity to discuss them with you. Thank you for your consideration. I look forward to hearing from you at your earliest convenience.

Sincerely,

Curt Weldon

CURT WELDON
Member of Congress

National Operations and Analysis Hub (NOAH)

The Challenge

- The United States continues to rely upon decades-old approaches in dealing with threats to our national security. It is time to consider new approaches beyond those developed in the 1950s if we are to successfully meet the challenges and issues facing us in the 21st century.
- This new approach supports the needs of the nation's policymakers, military commanders, and law enforcement agencies in taking action against asymmetrical threats such as terrorism, proliferation, illegal technology diversions transfers, espionage, narcotics, information warfare and cyberterrorism.
- The challenges facing policymakers, the military, and various law enforcement agencies are beginning to overlap, blurring their distinction and jurisdiction while posing an increasing threat to our nation, both domestically and internationally.

Addressing the Threat

- Numerous federal agencies continue their efforts to deal with these threats, often separate and distinct from the work of other agencies. This presents a serious problem because agencies often fail to share or bring together vital information that can assist in a timely solution.
- We don't need another analytical center. Instead, we need a national level "fusion center" that can take already analyzed data and offer courses of action for decision-making.
- On July 30, 1999 I wrote Deputy Secretary of Defense Hamre on the need for such a central national-level entity -- the National Operations Analysis Hub.
- This central national-level hub would be comprised of a system of agency-specified mini-centers, or "pods," of participating agencies and services associated with growing national security concerns. In all, some 33 such agencies would initially participate.
- Patterned after the Army's Land Information Warfare Activity center at Fort Belvoir, NOAH would display collaborative threat profiling and analytical assessments. With the aid of a variety of electronic tools, it would integrate various imagery, data, and analytical viewpoints for decisionmakers in support of national actions.

Benefits

- For national policymakers, such a national collaborative environment offers situation updates across a variety of issues and offers suggested courses of action — based on analysis — to help government officials make more informed decisions.
- For the intelligence community, a national collaborative center such as NOAH will help end stovepiping and create more robust strategic analyses as well as near-real-time support to field operations.
- For law enforcement, such a national-level center provides investigative and threat profiling support, and field station situational awareness.
- For military commanders and planners, the national-level center offers full battlefield visualization, threat profiling, robust situational awareness, as well as near real-time support to special missions such as peacekeeping, humanitarian aid, national emergencies or special operations.

Defense Information and Electronics Report

1st Place 1999
Newsletter Publishers Foundation
Exclusive News Award

an exclusive weekly newsletter on defense information and electronic warfare programs, procurement and policymaking from the publishers of Inside the Pentagon

Vol. 4, No. 45, November 12, 1999

Industry worried administration may waver
LAWMAKERS WEIGH IN AGAINST PROPOSED ENCRYPTION REGULATIONS

Concerned that the Clinton administration may be moving away from earlier pledges to liberalize encryption export policy rules, lawmakers on both sides of the aisle criticized the administration this week for seeking to narrowly write new regulations governing the foreign sale of encryption technology. House members were responding to industry groups who say White House officials have shown signs of "backsliding" during recent

continued on page 11

Pentagon intel officials mulling similar plan
WELDON: DOD NEEDS MASSIVE INTELLIGENCE NETWORK FOR SHARED THREAT INFO

Senior Pentagon officials are mulling over an idea proposed by Rep. Curt Weldon (R-PA) that would link classified and unclassified documents in a massive intelligence clearinghouse that could be accessed by 33 federal agencies — a concept similar in some ways to one floated by DOD intelligence officials but with significantly fewer players involved.

"Our problem with intelligence is that we're stove-pipped," said

continued on page 22

DISA undertakes 'aggressive action plan'
DEFENSE DEPARTMENT STRUGGLES TO KEEP UP WITH BANDWIDTH DEMANDS

A recent growth spurt in the military's Internet speed and connectivity requirements has left the Defense Information Systems Agency struggling to keep up with demands from the services while contending with local carriers backlogged with bandwidth orders — a dilemma DISA is answering through an "aggressive action plan" to protect DOD's future networking needs.

continued on page 23

RUSSIAN DELEGATION DOESN'T SHOW FOR YEAR 2000 TALKS

Russian officials this week did not show up for scheduled discussions on solutions to the Year 2000 computer problem and future information technology management issues, according to defense and congressional sources.

After Pentagon officials cleared schedules to arrange for tours, conferences and meetings, as well as hotel rooms and dinners for the small Russian delegation, defense officials were stunned when they didn't show on Nov. 8 for two days of meetings.

"We don't know why," said a DOD Y2K spokesman, adding that phone calls to the Russians were made in vain because of a national holiday in Russia. "No one knows yet."

Talks were originally scheduled to begin Oct. 11 but were pushed back several weeks due to scheduling conflicts "as a result of other Y2K cooperative efforts with the Russian Federation," according to an Oct. 6 letter from DOD's Y2K Outreach Program. Calling the proposed cooperative effort the Information Technology Management working group, DOD suggested last September to continue addressing the

continued on page 21

Virtual Virtues

Rep. Curt Weldon (R-PA), chairman of the House Armed Services research and development subcommittee, continues to push for a Capitol Hill "virtual reality" hearing room. Using workstations set aside for each lawmaker, legislators could [illegible]

... MODEL FOR INTEL NETWORK UNLIKELY . . . begins on page one

Weldon, chairman of the House Armed Services military research and development subcommittee, during a Nov. 8 interview. "Each agency has its own way of collecting data and analyzing it, but they don't share that information with other agencies. The need is to have a better system of analyzing and fusing data sets across agencies and services – certainly within the Pentagon and the military, but my opinion is that we have to go further than that."

Weldon first proposed the concept of a "National Operations Analysis Hub" to Deputy Defense Secretary John Hamre last July, although the congressman said he kept his initiative quiet until a stronger plan could be developed.

The Pentagon-funded network of agencies would be operated by DOD. According to Weldon, it would pull together large amounts of information to produce intelligence profiles of people, regions and national security threats, such as information warfare and cyber-terrorism.

"The NOAH concept of a national collaborative environment supporting policy and decision-makers mirrors the ideas you have expressed to me in recent discussions, and it is a tangible way to confront the growing asymmetrical threats to our nation," Weldon wrote in his July 30 letter to Hamre.

The NOAH concept, however, was not wholeheartedly embraced by Hamre, who met with Weldon last summer and told the congressman his suggested use of the Army's Land Information Warfare Activity at Ft. Belvoir, VA, as a model for NOAH, would never stick.

Because LIWA is already short of resources, the Army is apprehensive about taking on any new tasks, Hamre told Weldon.

Weldon, in a July 21 letter to Hamre, also urged the Pentagon to support additional future funding for LIWA, citing critical budget shortfalls that he said have kept the agency from fulfilling a barrage of requests for intelligence files from Army commanders *(Defense Information and Electronics Report*, July 30, p1).

"There's a massive amounts of data out there, and you have to be able to analyze it and create ways to focus on that data so its relevant to whatever you're interested in," he said this week about his support for LIWA. "Well, the Army has already done that."

While Weldon continues to push for NOAH to be patterned after LIWA, he sees it operating on a much larger scale. Impressed by its ability to pull together huge amounts of both unclassified and classified data, Weldon noted LIWA's Information Dominance Center can create in-depth profiles that could be useful to the CIA, FBI and the White House. Yet most federal agencies don't even know LIWA exists, he added.

"Right now the military is limited to [its] own sources of information," Weldon said. "And in the 21st century, a terrorist group is more than likely going to be involved with terrorist nations. So the boundaries are crossed all the time. We don't have any way to share that and get beyond the stove-pipping."

Meanwhile, officials within the Defense Department's intelligence community have been considering another way to amass intelligence information through a concept called the Joint Counter-intelligence Assessment Group. A DOD spokeswoman said proponents of the idea, for now, are unwilling to disclose details about it. She was also unable to say whether a formal proposal to Hamre had been made yet.

In Weldon's July 30 letter to Hamre, however, Weldon alludes to an ongoing "initiative to link counterintelligence groups throughout the community."

"I have heard of an attempt to connect the Office of Drug Control Policy (ONDCP) and [Office of the Secretary of Defense] assets with federal, state and local law enforcement agencies," Weldon wrote.

However, Weldon said in the interview he believes JCAG is simply more "stove-pipping."

"I also have seen what the Army has done at LIWA, which has created a foundation for creating a higher-level architecture collaborating all of these efforts," his July letter states.

NOAH would link together almost every federal agency with intelligence capabilities, including the National Security Agency, the National Imagery and Mapping Agency, the Energy Department, the CIA and the FBI. Both Congress and the White House would be offered a "node" for briefing capabilities, meaning intelligence agencies could detail situations on terrorist attacks or wartime scenarios.

"It's mainly for policymakers, the White House decisionmakers, the State Department, military, and military leaders," he said.

Although information-sharing among the intelligence community has yet to be formalized through NOAH or JCAG or a similar system, military officials have said they need some kind of linked access capability.

Intelligence systems need to be included within the Global Information Grid – the military's vision of a future global network that could be accessed from anywhere in the world, said Brig. Gen. Marilyn Quagliotti, vice director of the Joint Staff's command, control, communications and computers directorate, during a Nov. 5 speech on information assurance at a conference in Arlington, VA.

"We need a more integrated strategy, including help from [the Joint Staff's intelligence directorate] with intelligence reports or warnings of an attack," she said.

Quagliotti said the toughest challenge for achieving "information superiority" is the need to unite networks and network managers under one command structure with strong centralized awareness capabilities.

"[Part of the challenge] is the ever-widening amount of information, the ability to access that information, and the ability to reach back and get that information, which means that networks become more crucial to the mission[illegible]

SEC. 903. REVISED JOINT REPORT ON ESTABLISHMENT OF NATIONAL COLLABORATIVE INFORMATION ANALYSIS CAPABILITY.

(a) REVISED REPORT.—At the same time as the submission of the budget for fiscal year 2003 under section 1105 of title 31, United States Code, the Secretary of Defense and the Director of Central Intelligence shall submit to the congressional defense committees and the congressional intelligence committees a revised report assessing alternatives for the establishment of a national collaborative information analysis capability.

(b) MATTERS INCLUDED.—The revised report shall cover the same matters required to be included in the DOD/CIA report, except that the alternative architectures assessed in the revised report shall be limited to architectures that include the participation of all Federal agencies involved in the collection of intelligence. The revised report shall also include a draft of legislation sufficient to carry out the preferred architecture identified in the revised report.

(c) OFFICIALS TO BE CONSULTED.—The revised report shall be prepared after consultation with all appropriate Federal officials, including the following:

(1) The Secretary of the Treasury.

(2) The Secretary of Commerce.

(3) The Secretary of State.

(4) The Attorney General.

of an Office of Transformation within the Office of the Secretary of Defense to advise the Secretary on—

(1) development of force transformation strategies to ensure that the military of the future is prepared to dissuade potential military competitors and, if that fails, to fight and win decisively across the spectrum of future conflict;

(2) ensuring a continuous and broadly focused transformation process;

(3) service and joint acquisition and experimentation efforts, funding for experimentation efforts, promising operational concepts and technologies, and other transformation activities, as appropriate; and

(4) development of service and joint operational concepts, transformation implementation strategies, and risk management strategies.

(c) SENSE OF CONGRESS ON FUNDING.—It is the sense of Congress that the Secretary of Defense should consider providing funding adequate for sponsoring selective prototyping efforts, wargames, and studies and analyses and for appropriate staffing, as recommended by the director of an Office of Transformation as described in subsection (b).

Fusion Center Concept Takes Root As Congressional Interest Waxes

Army's Land Warfare Information Activity provides model of profiling approaches to meet new hazards.

Creation of a national operations and analysis hub is finding grudging acceptance among senior officials in the U.S. national security community. This fresh intelligence mechanism would link federal agencies to provide instant collaborative threat profiling and analytical assessments for use against asymmetrical threats. National policy makers, military commanders and law enforcement agencies would be beneficiaries of the hub's information.

Prodded by a resolute seven-term Pennsylvania congressman and reminded by recent terrorist and cyberthreat activities, the U.S. Defense Department is rethinking its earlier aversion to the idea, and resistance is beginning to crumble. Funding to establish the national operations and analysis hub (NOAH), which would link 28 federal agencies, is anticipated as a congressional add-on in the Defense Department's new budget. An initial $10 million in funding is likely in fiscal year 2001 from identified research and development accounts.

Spearheading the formation of NOAH is Rep. Curt Weldon (R-PA), chairman of the U.S. House of Representatives National Security Committee's military research and development subcommittee. He emphasizes that challenges facing U.S. leaders are beginning to overlap, blurring distinction and jurisdiction. "The increasing danger is both domestic and international."

Conceptually, NOAH would become a national-level operations and control center with a mission to integrate various imagery, data and analytical viewpoints. The intelligence products would support U.S. actions. "I see NOAH as going beyond the capability of the National Military Command Center and the National Joint Military Intelligence Command. NOAH would provide recommended courses of action that allow the U.S. to effectively meet emerging challenges in near real time," the congressman illustrates.

"This central national-level hub would be composed of a system of agency-specified mini centers, or 'pods,' of participating agencies and services associated with growing national security concerns," Weldon reports. "NOAH would link the policy maker with action recommendations derived from fused information provided by the individual pod." Automation and connectivity would allow the pods to talk to each other in a computer-based environment to share data and perspectives on a given situation.

The congressman believes that NOAH should reside within the Defense Department and is modeling the hub's concept on a U.S. Army organization he closely follows. He says the idea for NOAH comes from officials in several federal agencies. However, it is also based on his own experiences with the U.S. Army's Intelligence and Security Command's (INSCOM's) Land Warfare Information Activity (LIWA) and Information Dominance Center, Fort Belvoir, Virginia.

Patterned after LIWA (*SIGNAL*, March, page 31), NOAH would display collaborative threat profiling and analysis.

Rep. Curt Weldon (R-PA), chairman of the U.S. House of Representatives National Security Committee's military research and development subcommittee, displays a Russian laser gyroscope and an accelerometer intercepted en route to Iraq. The ballistic missile guidance package is from a Russian SS-N-19 submarine launched missile. Transferred at least three times to hide the shipment, the guidance package was sold with the knowledge of Russian officials, which is a violation of the International Missile Technology Control Regime.

With the aid of a variety of electronic tools, the hub would support national actions, Weldon discloses.

The congressman is conscious of other initiatives such as linking counterintelligence groups throughout the community. He also is aware of the Central Intelligence Agency's (CIA's) counterterrorism center, the Federal Bureau of Investigation's (FBI's) National Infrastructure Protection Center and a new human intelligence (HUMINT) special operations center. "We don't need another analytical center. Instead, we need a national-level fusion center that can take already analyzed data and offer courses of action for decision making," he insists.

Weldon's wide experience in dealing with officials from the FBI, CIA and the National Security Agency (NSA) convince him that policy makers are continuing to work in a vacuum. "Briefings and testimonies are the primary vehicles for transmitting information to leaders. The volume of information germane to national security issues is expanding so rapidly that policy makers are overwhelmed with data," he claims.

Robust situational awareness of asymmetric threats to national security is a key in assisting leaders, Weldon observes. "Policy makers need an overarching information and intelligence architecture that will quickly assimilate, analyze and display assessments and recommend courses of action for many simultaneous national emergencies," he declares. The concept of NOAH also calls for virtual communications among policy makers.

Weldon's plan is for White House, Congress, Pentagon and agency-level leaders each to have a center where they receive, send, share and collaborate on assessments before they act. He calls NOAH the policy maker's tool. In the collaborative environment, the hub would provide a multiissue, multiagency hybrid picture to the White House situation room and the Joint Chiefs of Staff.

NOAH's concept also includes support for HUMINT and peacekeeping missions along with battle damage assessment. The same system could later help brace congressional committees and hearings. The new capability would allow application of foreign threat analyses to policy, while providing a hybrid situational awareness picture of the threat, Weldon relates. Industrial efforts of interest to the policy maker could be incorporated, and academia also could be directly linked.

In meetings with high-level FBI, CIA and defense officials, Weldon stressed the need to "acquire, fuse and analyze disparate data from many agencies in order to support the policy maker's actions against threats from terrorism, [ballistic missile] proliferation, illegal technology diversions, espionage, narcotics [trafficking], information warfare and cyberterrorism." He is convinced that current collection and analysis capabilities in various intelligence agencies are stovepiped. "To some extent, this involves turf protection, but it clearly hinders policy making."

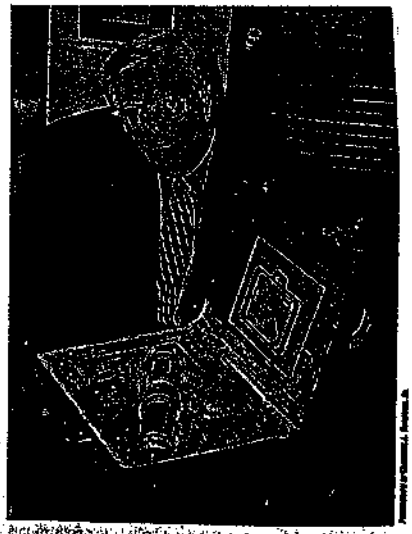
Weldon, who was a Russian studies major, offers some of his own recent experiences as examples of why there is a strong need for NOAH. He maintains close contact with a number of Russians and understands their programs and technologies. The congressman is quick to recall vignettes about Russian officials and trips to facilities in the region.

During the recent U.S. combat action involvement in Kosovo, Weldon was contacted by senior Russian officials. Clamoring for Russia to be involved in the peace pro they claimed that otherwise upcoming elections could the communists. The Russians proposed a Belgrade me with Weldon, congressional colleagues, key Serbian offi and possibly Yugoslave President Slobodan Milosevic.

After the first meeting with key officials from the de ments of State and Defense and the CIA, Weldon and members of Congress went to Vienna, Austria. The Department objected to a meeting in Belgrade, sugges instead a neutral site. Before the departure, the Russ informed Weldon that Dragomir Karic, a member of a p erful and wealthy Kosovo family, would attend the meet Karic's brother was a member of the Milosevic regime.

At the end of the Vienna meeting, the Russians and Ka told Weldon that if he would accompany them to Belgra Milosevic was prepared to meet with them and publi embrace a peace agreement concept reached during t Vienna meeting. The agreement would have direct involved Russia in the peace process. A diplomatic offic with the U.S. delegation telephoned Washington, D.C., a the State Department objected to the Belgrade trip. T congressman and his colleagues returned home.

As soon as he arrived in Washington, D.C., the FI telephoned to request a meeting with Weldon to gath details on Karic. It was clear, Weldon reports, they ha very little information on him or his family. The follow



Rep. Weldon displays a Russian-designed replica of a uranium-fueled gun nuclear device hidden in a briefcase. The entire 1- to 10-kiloton bomb package was manufactured from open source Russian Ministry of Defense and KGB specifications obtained by a former CIA agent.

...g day, the CIA telephoned the congressman and asked for a meeting "about Karic." Instead, the congressman proposed a joint meeting with CIA and FBI agents in his office. Two officials from each agency attended with a list of questions.

Weldon learned from the agents that they were seeking information on Karic to brief the State Department. When he explained that the information came from the Army and LIWA, the CIA and FBI agents had no knowledge of that organization, he confirms. Before his departure for Vienna, the congressman received a six-page LIWA profile of Karic and his family's links to Milosevic.

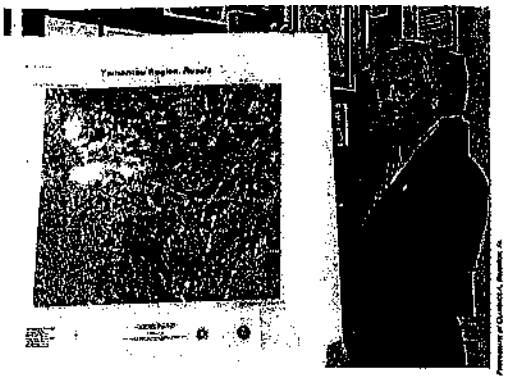
"This is an example of why an organization like NOAH is so critically necessary," Weldon contends. "LIWA's Information Dominance Center provides the best capability we have today in the federal government to assess massive amounts of data and develop profiles. LIWA uses its contacts with other agencies to obtain database information from those systems," he explains. "Some is unclassified and some classified."

Weldon cites an "extraordinary capability by a former CIA and Defense Intelligence Agency official, who is a LIWA profiler, as one of the keys in LIWA's success. She does the profiling and knows where to look and which systems to pull information from in a data mining and extrapolation process," he proclaims. "She makes the system work."

Weldon intends to use LIWA's profiling capability as a model for building NOAH. "My goal is to go beyond service intelligence agencies and integrate all intelligence collection. This must be beyond military intelligence, which is too narrow in scope, to provide a governmentwide capability. Each agency with a pod linked to NOAH would provide two staff members assigned at the hub, which would operate continuously. Data brought together in "this cluster would be used for fusion and profiling, which any agency could then request," he maintains.

NOAH would not belong to the Army, which would continue with its own intelligence capabilities as would the other services. There would only be one fusion center, which would handle input from all federal agencies and from open sources, Weldon explains. "NOAH would handle threats like information operations and examine stability in various regions of the world. We need this ability to respond immediately." The congressman adds that he recently was briefed by LIWA on very sensitive, very limited and scary profile information, which he describes as "potentially explosive." In turn, Weldon arranged briefings for the chairman of the House National Security Committee, the Speaker of the House and other key congressional leaders.

"But this kind of profiling capability is very limited now. The goal is to have it on a regular basis. The profiling could be used for sensitive technology transfer issues and information about security breaches," the congressman allows. LIWA has what he terms the fusion and profiling state-of-the-art capability in the military, "even beyond the military." Weldon is pressing the case for NOAH among the leaders in both houses of Congress. "It is essential that we create a governmentwide capability under very strict controls."



Despite economic upheaval, Russia continues to spend billions of dollars on a secret underground site in the Urals. Rep. Weldon shows a photograph of the Yamantau Mountain complex near the cities of Beloretsk 15 and 16. A large-gauge rail line runs into the mountain, which could be for strategic-directed energy weapons development and storage.

Weldon adds that establishing NOAH is not a funding issue; it is a jurisdictional issue. "Some agencies don't want to tear down their stovepipes. Yet, information on a drug lord, as an example, could be vitally important to help combat terrorism." He makes a point that too often, federal agencies overlap each other in their efforts to collect intelligence against these threats, or they fail to pool their resources and share vital information. "This redundancy of effort and confusion of jurisdiction only inhibits our nation's capabilities," he offers.

NOAH would provide high-bandwidth, virtual connectivity to experts at agency pod sites. Protocols for interagency data sharing would be established and refined in links to all pod sites. The ability to retrieve, collate, analyze and display data would be exercised to provide possible courses of action. A backup site would be established for redundancy, and training would begin on collaborative tools as soon as it is activated.

The hub system would become part of the national policy creation and execution system. The tools available at LIWA would be shared so that every agency would have the same tools. Weldon explains that all agencies would post data on the National Reconnaissance Office (NRO) highway in a replicated format sensitive to classification. NOAH's global network would use the NRO system as a backbone.

NOAH optimizes groups of expertise within each organization—experts who are always on hand regardless of the issue. This approach ties strategic analysis and tactical assessment to a course of action. "Before the U.S. can take action against emerging threats, we must first understand their relationship to one another, their patterns, the people and countries involved and the level of danger posed to our nation," Weldon says, "That is where NOAH begins." —*CAR*

Thank you.

Mr. CAMP. Thank you.

Miss Lofgren may inquire.

PREPARED STATEMENT OF THE HONORABLE ZOE LOFGREN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

• Thank you Chairman Thornberry. It is always a pleasure to work with you. It is also a pleasure to be holding this joint hearing with the Subcommittee on Infrastructure and Boarder Security. This subcommittee is led by my good friend and California colleague, Congresswoman Loretta Sanchez, and Chairman Dave Camp of Michigan.
• The blackout on August 14, 2003 left nearly 50 million people in 8 states and Canada without power. When the lights went out that afternoon, there was widespread concern that this incident might have been another major terrorist attack on the United States. The video of pedestrians streaming out of Manhattan was eerily reminiscent of the events September 11, 2001.
• Thankfully, we quickly determined that terrorism played no role in this event. The regional power grid simply was overwhelmed and broke down.
• While we can express some relief that the blackout was not a terrorist attack, this event does highlight our continuing need for better protection of our critical infrastructure.
• Too many of our nation' infrastructure assets remain extremely vulnerable to terrorist attack. Power plants, airports, bridges, water treatment facilities, and public and private sector computer networks are just not sufficiently prepared for an incident of terrorism. There are simply hundreds of thousands of assets in our country that must better secured.
• I remain greatly concerned the Bush Administration is not up to the task of preparing for future terrorist attacks.
• Almost 2 years have passed since the events of September 11th. Yet we do not have any comprehensive list of national critical infrastructure assets that assesses risks and vulnerabilities. To my knowledge, the Department of Homeland Security is not giving advice to or sharing information with states and cities on how best to secure important facilities.
• I am particularly concerned about the threat of some sort of cyber attack. A recent study by the Pew Internet and American Life Project found that nearly half of all Americans surveyed say they are worried that terrorists could launch attacks through the networks connecting home computers and powerful utilities.
• In the past month, several computer worms have struck computer networks and systems around the world. There are reports that these worms are swamping network systems with traffic, causing denial of service to critical servers within organizations, and adversely affecting government and emergency response operations.
• As long as worms such as Blaster, Welchia, and SoBig.F can adversely affect our computer networks, then our weakest links are insecure and the entirety of our infrastructures and communications systems is at risk.
• I return to Silicon Valley every weekend. I am constantly approached by people in the tech industry—from CEO's to programmers—who wonder what the Department of Homeland Security is doing to prevent cyber attacks. I am frustrated because I can't give them an answer.
• The DHS announced almost 3 months ago the creation of a National Cyber Security Division within the Information Analysis and Infrastructure Protection Directorate (June 6). On August 3, Secretary Ridge said that a director for the cyber division would be chosen soon. I have heard countless rumors for over a month about personnel announcements, and yet as of today, no one has been chosen to lead this division.
• Three months is just too long to wait. Either the Department is in complete disarray, or it does not consider cybersecurity to be a priority. Perhaps it is both, and that is very troubling.
• I want to thank our witnesses for appearing before us today. I look forward to hearing your testimony. I hope you will focus in particular on your personal dealings with DHS. I also hope you can persuade me that there is some good work being done within the Department to protect our nation's critical infrastructures.

Ms. LOFGREN. I will submit my questions for the record.

Mr. CAMP. Mr. Pascrell.

Mr. PASCRELL. Thank you. Thank you, Mr. Chairman. I have a few questions.

First, to Mr. Mefford, who has been before our committee—subcommittee a few times and appreciate his candidness and his forthrightness. You are a credit to the FBI and to this country for the service that you have presented. I mean that. If you know me, if I didn't feel that way, I would say nothing or to the contrary.

Mr. MEFFORD. Thank you.

Mr. PASCRELL. But I want to congratulate you for what you have done.

I want to ask you a question. Has the creation of the DHS and all of the apparatus of Homeland Security clarified, in your estimation, or confused Federal leadership on security? What is your estimate of that? And then I am going to ask Mr. Black that question, also.

Mr. MEFFORD. In the area of critical infrastructure protection, in my view it has clarified the role. Historically, prior to the formation of that Department, the FBI was involved, as you know, investigating terrorism threats and in working with our counterparts in private industry to the degree that we were able to identify vulnerabilities and assess threats to the vulnerabilities. Today, that is the role of the Department of Homeland Security; and, frankly, it frees us up to focus on the operational end of counterterrorism, being the investigative phase so that we can run down every threat and that we can use our personnel, frankly, in a way that they are trained and focus them in a greater degree.

So, in my view, in the area of critical infrastructure protection, it has helped. It is a new department, but I think that they have made tremendous progress, and I look forward to working closely with them to achieve their goals. But, having said that, I understand that it is very challenging to form a large organization quickly.

Mr. PASCRELL. Would you say that you have anticipated any confusion in the formation of this apparatus, Homeland Security apparatus, in terms of Federal leadership? What do you anticipate that could be confusing or perceived as confusing so that the message is not clear as to who is working on this and who is trying to resolve the problems?

Mr. MEFFORD. Well, in the FBI I think, if we are talking about critical infrastructure protection, it is very clear to us and we have no doubt about the role of the FBI and the role of Homeland Security and we see our role as being complementary and to assist them as we can. Clearly, if we focus on identifying terrorism threats and we focus on prevention and disruption of terrorist activities in the country, our role is to pass that information rapidly to DHS to allow them to improve their evaluation process and their analysis of vulnerabilities. But it really is a complementary arrangement; and in that area, in the area of critical infrastructure protection, I think we are making progress.

Mr. PASCRELL. This was the largest that I know of—I will stand corrected—the largest, the most widespread blackout we have had in many moons, right? Mr. Chairman, were you prepared? Was the FBI's apparatus prepared to deal with it just in case there was sabotage involved and did it work? I mean, you went into action immediately. What did you do?

Mr. MEFFORD. We immediately convened a conference call with all of the special agents in charge of the eight field offices that were affected by the power outage and based on backup energy sources were able to communicate and use the telephone and other devices. And we laid out what we knew, what we didn't know. We strategized and prioritized, and then we brought in the Joint Terrorism Task Forces which I referred to in my opening comments. They are really the bedrock of all of our counterterrorism efforts, and that brings in the State and local law enforcement piece and the Federal law enforcement and intelligence piece. So working hand in glove, we immediately went out to the private industry folks involved, coordinated and started our efforts basically to investigate, looking backwards to see if we could assist in identifying the cause of the outbreak.

Mr. PASCRELL. Mr. Black, if I may, Mr. Chairman, we know that this is a vulnerable area. In fact, we have been warned that this could happen again, this blackout; and we have responded to—what measures have you taken, specifically in concrete, since this time, since the time of the blackout which caused devastating losses throughout the Northeast and central United States? What have you done in the Department of State to avoid this in the future or being better able to respond to it if it happens again?

Mr. BLACK. First of all, the contributions that we can make is from an international standpoint. We—.

Mr. PASCRELL. I didn't hear you. I am sorry.

Mr. BLACK. Is from an international standpoint. We support other agencies in their work.

I think you asked for a clarification on Department of Homeland Security. I think its mission from a State Department standpoint is absolutely critical. Because it is that entity that rationalizes the threat information, things that can happen to us. Match that up with the potential vulnerabilities and do that key work from an international standpoint, from an information processing standpoint. That is the most important to us.

We do not see an element of confusion here. We see an element of adjustment. When you have such a new department that is playing such a key role, the other agencies that are supporting this homeland defense adjust.

As an example, my job is contacts with foreign countries in terms of policy formulation and coordination from counterterrorism. The Department of Homeland Security has an international unit. We have personnel assigned to that, and our job is to facilitate their interaction in the protection of the homeland.

So our contribution in this is the facilitation of contacts with foreign countries that are affected, whether it is close allies like the Canadians or British or others, depending upon the threat that materializes here in the United States.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. CAMP. Thank you.

Ms. Dunn may inquire.

Ms. DUNN. Thank you. Thank you very much, Mr. Chairman.

Ambassador Black, I wanted to ask a you question based on what you were just saying. I gave a speech last month on cyberterrorism in London. We were meeting with members of Par-

liament, and I was amazed at how much attention they are paying to the very same things that we are dealing with. I had used as an example of potentials for cyberterrorism the power grid in the United States, and 2 Yays later we saw that happen.

I guess, first of all, I would like to know, briefly, how did you know it wasn't terrorism at the beginning? And, secondly, I would like you to expand on what we have learned from people in other nations. Are there things that they have accomplished that we can learn from and are we doing our work in cooperation with them as the experience I had in London last month told me we were?

Mr. BLACK. Yes, ma'am. I do understand that you are very interested in this, as are a number of our allies. The reason that I knew it wasn't terrorism was because my colleagues in the FBI and the U.S. Intelligence Community advised us of that fact. We were the recipients of their good works. So that was a very comforting thing, and I think they were able to determine that pretty early on in this process.

I think there has been great interest in cyberterrorism. It has been going on for years. And this is something that the State Department—our role is to facilitate contacts to make sure that the links are there and that our colleagues in the FBI and the American Intelligence Community are matched up with their foreign counterparts. In this area of expertise we are primarily facilitators, and we also provide training to countries that have the will to work against this problem but not the capacity. So we facilitate the making of contacts as well as provide training programs to appropriate foreign recipients overseas.

Ms. DUNN. Mr. Mefford, how did you know it wasn't terrorism?

Mr. MEFFORD. Our Joint Terrorism Task Forces are looking at this issue from various perspectives. One is the external threat, to see if there is physical damage, to see if we have actual signs of sabotage. We have not found any. And we determined that fairly quickly, although I indicated in my opening comments our inquiry is ongoing, and so I am not giving you a definitive answer at this point. But preliminarily we have not found any evidence of that.

We also looked at the Intelligence Community for input regarding their knowledge of plots and efforts on behalf of our adversaries around the world that may want to do something like this, and we haven't found that.

In addition, we are very concerned about the insider threats, somebody that would have access to critical systems, both from a physical standpoint, the sabotage standpoint and a computer intrusion. And that applies also for somebody clearly on the computer intrusion side, on degrading capabilities and attacks through the computer networks. That applies on the external threat, also. We have not yet seen evidence of that.

But this very preliminary assessment that I am giving you, because we are working with the Department of Energy, Department of Homeland Security and NERC to review the computer logs for evidence of that type of malicious activity. We have not seen that to date but it is still ongoing.

Ms. DUNN. Now the threat of insider action of terrorism is becoming a very broad theme as we investigate what could be harmful to us in the United States. Let me ask you another question.

You acknowledged in your testimony that terrorists could choose a variety of means to attack the Nation's power grids. In your opinion, what should we as a committee be focusing on? Where should we be directing the Department of Homeland Security's oversight, and what should the Department of Homeland Security to be focusing on? What are the means that are most concerning to you?

Mr. MEFFORD. I think in our view you look historically at what—when we see our number one threat today remains al Qaeda. There are other terrorist groups and members that concern us, also. But the number one threat remains al Qaeda today. And if you look at their historical activities you have to look at things such as what occurred on September 11; the attacks in Riyadh, Saudi Arabia, on May 12; the attacks in Casablanca, Morocco, I think on May 16 of this year; and other various attacks overseas where we are seeing basically truck bombs and assaults of individuals.

We have not seen any indication that al Qaeda possesses a sophisticated computer intrusion capability. While potentially they may have expressed an interest, we have seen no evidence that they possess this capability today. Clearly, it is of concern to us, because at some point in the future we are going to have to address those types of issues. But at this stage it is our view that we have seen very, very basic computer functionality on the part of identified terrorists in the world. We have not seen sophisticated capabilities if you talk about the attacks to networks.

But we have seen sophisticated capabilities on the physical side, sabotage and the traditional terrorist attacks using explosives and what we saw on 9/11. So I think we would recommend priority to physical, to protect against physical sabotage at this point, including the insider threats with individuals that have access to your most sensitive components—potentially are vetted to ensure that we don't have the wrong person in the wrong place.

Ms. DUNN. Is—just a follow-up on that. Is there an area with we ought to be sending more resources?

Mr. MEFFORD. I am not educated to the degree that I think I can answer that appropriately today.

Ms. DUNN. Thank you, Mr. Chairman.

Mr. CAMP. Thank you.

Ms. Christensen may inquire.

Mrs. CHRISTENSEN. I thank you, Mr. Chairman.

Let me see. Let me follow up with a question to Mr. Mefford following up on the Ranking Member's question. I think he asked a general question on critical infrastructures which pose the greatest security concerns and whether or not there had been assessment of vulnerabilities. In your testimony, you say that you are clearly aware that the terrorists are clearly aware of the importance of electrical power; that al Qaeda and other terrorist groups have considered energy facilities, et cetera, et cetera. Have you received an assessment of vulnerabilities specifically related to the electrical power grid?

Mr. MEFFORD. No, we have not.

Mrs. CHRISTENSEN. You need that to be able—in your collaboration with the Department of Homeland Security, that is their role in that partnership; is it not?

Mr. MEFFORD. Yes. And I understand that it is in progress at this point, and that they are working towards that end, and we are cooperating in assisting to whatever degree we are capable.

Mrs. CHRISTENSEN. Another question occurs to me, because, for example, in the instance of the blackouts, there is a need to immediately restore and repair the break. Does the need for immediate repair in any way compromise our ability to determine the cause or to investigate where the breakdown may have occurred or whether or not it may have been caused by international or domestic terrorism?

Mr. MEFFORD. In reality it does not impede our ability because we have ample experience now, unfortunately, in responding to terrorist bombings where clearly the priority is protecting and saving human life. At the same time, while that process is ongoing, we have devised the capability inside the FBI to conduct forensic efforts and crime scene—traditional scientific efforts at the crime scene in a way not to impede the priority of saving human lives. And I think that same principle would apply in the case that you outlined.

Mrs. CHRISTENSEN. The CT Watch that you outline seems to be a very coordinated way of disseminating information. Is the response as coordinated, and has that ever been exercised?

Mr. MEFFORD. I guess I am not sure exactly what you are referring to. The response to a blackout?

Mrs. CHRISTENSEN. Under the CT Watch the information, the notification of potential threats are immediately disseminated to all the relevant agencies, which evokes the need to respond.

Mr. MEFFORD. We think—

Mrs. CHRISTENSEN. Has that been exercised? Are the responses as coordinated as the dissemination of information seems to be?

Mr. MEFFORD. I think there is room for improvement, but we are definitely making progress, and we are getting better each and every day. And based on the volume of threats—and, as you know, the vast majority of all these threats overwhelmingly are unfounded. The unfortunate part is we have to expend the resources because we can't take a chance. We have to follow up on each and every threat. We have had over 4,000 in the Intelligence Community since September 11. So it is keeping us very busy. But we have had ample opportunity to exercise the coordination, and I think we are getting much, much better at it.

Mrs. CHRISTENSEN. I have one last question. The InfraGard program, you say, serves as an important link of over 8,000 companies located in all 50 States. Did you mean States and territories, or territories not included in that; and where are you in making sure we are included?

Mr. MEFFORD. Let me check on that real quick.

Yes, ma'am. They include territories also.

Mr. CAMP. Thank you.

Mr. Etheridge may inquire.

Mr. ETHERIDGE. Mr. Mefford, let me ask you a question on the testimony you forwarded as it relates to the role of TTIC, Terrorism Threat Integration Center, as you mentioned earlier about the critical infrastructure, and here I am expanding beyond the blackout because they have that, and you talk about potential im-

pact, and you are looking at banking and a whole host of things. What role does that play in the analysis of threat information against our critical infrastructure?

Mr. MEFFORD. The FBI furnishes TTIC with all of our threat information, all types, whether it impacts the power grid or banking systems or water systems and whatnot, because they are the single entity that not only has possession of all this information, I think it enhances our capability, as I say, to connect the dots and make sense of the information that we possess.

Mr. ETHERIDGE. That being said then, as we look at the blackout that we just went through, and whether it was that or many others for that matter, whether they be terrorist-instigated or whether they be mechanical or something else has the same devastating economic impact as if we look at a situation where there is a hurricane or tornado or terrorists initiated it. At the end of the day it has the same impact. My question deals with the blackout. How will you characterize the FBI's communication with local and State authorities due to this last blackout; what did you learn from that situation that hopefully in the future, not only for the FBI, but other agencies, that will allow us better to deal with something of this nature in the future?

Mr. MEFFORD. I mean, the Bureau's role is basically twofold in this case: Number one, on the preventive side, to collect intelligence information and to do so within the confines of our Constitution and rules and policies and laws, and to do that in conjunction with State and local agencies that are members of our joint terrorism task forces. Right there at the very basic level it enhances our coordination from the beginning. Secondly, if there is an incident, and to respond efficiently and to integrate into a broader U.S. Government response, the FBI has a very specialized role to play. We are not in the driver's seat. We are not directing the response to a significant incident like the blackout. We have a very specialized role, and to focus our individuals in the FBI and our terrorism task forces in that very specialized role is that we see the value we can add.

Clearly there is always room for improvement. We think we mustered our investigative capabilities quickly. We responded with our partners in State and local law enforcement. We always look to ways to improve communication, but overall I think we did a very successful job of that. It is still ongoing, and it is premature for me to give you any definitive report on exactly what we found from a criminal or terrorist standpoint. Preliminarily, as I indicated, at this stage we don't have any indication of that type of activity.

Mr. ETHERIDGE. Finally, let me ask a question of both of you because you indicated in previous testimony you saw no evidence of al Qaeda or others being involved in something this sophisticated as attacking the power grid, banking or water or sewer, et cetera, or as it relates to our computers. However, we just heard of an 18 17 year-old youngster, pretty bright, probably smart enough that he should use his talents otherwise, but I would venture to say that it is not restricted to the United States. There are very bright youngsters around the world. If they can do it, then the potential for the future has to be there.

So my question is this: As it relates to that, I hope you will comment on the whole issue of that tied to this final question. You might want to touch this one, but I think this is a critical piece, and this is a critical piece of our software development that has a lot of bugs and trap doors and other things linked into it of where it is developed, whether it is inside this country or outside this country—the security that was mentioned earlier with our current situation so dependent on software and computers to move and disseminate information.

Mr. MEFFORD. In reference to your first point, the Director of the FBI created the FBI Cyber Division specifically to address the vulnerability that you outlined, and that is while we may not see indications of a sophisticated capability on the part of our terrorist adversaries today, it would be foolish and unprofessional of us to neglect that area of concern, and therefore we are rapidly moving to increase and improve our internal capabilities in the FBI. We are working very closely with Homeland Security and other agencies for a coordinated approach because we see that not only long term, but see that—if the training continues on these tracks, it is probably an inevitable vulnerability.

In response to your second issue, that is a very, very complicated issue, and I will have to refer it to the technical experts, and I don't have the education to respond appropriately.

Mr. BLACK. The issue is for us to facilitate a positive process. We seek to make sure that the right contacts are in place, that the communication is robust and is sustainable over time. I want to make sure that our military is hooked up with militaries overseas, and the law enforcement of the United States, the FBI, is in contact with the right people overseas, and this exchange is working out.

Cyberterrorism is a threat. We see more of it every day. I think the experts involved with this certainly are looking at it from the State Department perspective. Our job is to make sure they have the right contacts and the velocity of communication interaction meets the needs of our country.

Mr. CAMP. Mr. DeFazio may inquire.

Mr. DEFAZIO. Thank you, Mr. Chairman. I guess probably I will direct this to Mr. Mefford, or perhaps it will have to come from a later panel. I guess specifically on the issue of electricity and the transmission and the grid, we have had some cyberattacks on nuclear plant security that have been documented, but what progress have we made since it has been identified, as far as I know, for some time as a potential target of opportunity? I remember it being a target of opportunity. Back in my region of the country, it was thought at the time of the millennium both because of inadvertent failures, but also because of potential attacks. What progress have we made since 2000 or since 9/11 on hardening, safeguarding the backbone of the grid and our system of electric generation or transmission?

Mr. MEFFORD. I am going to defer that to experts. I am not privy to the specifics of that.

Mr. DEFAZIO. I guess even though the hearing is theoretically on that, is there someone in the FBI who specifically—

Mr. MEFFORD. That is the type of question I think is beyond the purview of the FBI and is beyond our role in this.

Mr. DEFAZIO. Since you monitor threats, you must have some contact with the industry and some idea of steps or suggestions that might be—

Mr. MEFFORD. And my general impression is that it is improving, but there is significant work to be done. And one of the improvements relates to education regarding a problem, and there is an acknowledgment and understanding of the problem or potential problem far greater than what we have had historically. But as to actual physical improvements and software and improvements to the networks, I would have to defer to the experts.

Mr. DEFAZIO. Thank you, Mr. Chairman.

Mr. CAMP. Thank you.

Mr. Dicks may inquire.

Mr. DICKS. Thank you.

Mr. Mefford, let me ask you something. The vice chairman of our panel Ms. Dunn asked you about whether there was any indication of a terrorist involvement in the attacks on the power system. What kind of things would you look for if there was a criminal or a terrorist attack? What kind of things would you be trying to find out?

Mr. MEFFORD. Obviously there was not an obvious sabotage here. We would have known it.

Mr. DICKS. Like a bomb?

Mr. MEFFORD. Number one, we look for those types of issues. Because the network is so widespread and components are in very remote areas, you can't ascertain that immediately, and it would take a number of hours or days to find the source of that. But we clearly didn't find any evidence of that.

We then looked at the cyber piece, at the computer intrusion piece, to see if anybody has maliciously entered the networks that has some kind of access or control to the physical system. That is ongoing. To date we are working in a joint group with the agencies I have outlined, and my understanding that we have not found indications of that, but it is still ongoing. And then thirdly, it is a significant issue, and that is the insider threat. Did anybody do something that potentially has access to sensitive equipment and components that is not readily apparent on first review? That means potentially vetting employees and whatnot. We have not seen indications of that, but it is something we are concerned about.

So it is a layered approach, and we start with the most obvious. If you look at al Qaeda, for instance, they have been involved in physical acts of terrorism. We have not seen anything other than that so far. Doesn't mean they won't shift gears, and we have to be attuned to that, but we would start from that premise and then work up.

Mr. DICKS. Basically we have not seen al Qaeda launch cyberattacks against infrastructure in the United States or anywhere else.

Mr. MEFFORD. They have not.

Mr. DICKS. They are using cruder techniques, the car bombs and things that you mentioned.

Mr. MEFFORD. Yes, sir.

Mr. DICKS. We hear about the cyberattacks. Is it pretty much random, or are there any terrorist groups that have used cyberattacks or trying to test it against U.S. systems? I know the Defense Department, the State Department have been somewhat vulnerable.

Mr. MEFFORD. There is a lot of misinformation out there today indicating that terrorists have launched attacks in attempting computer intrusions and whatnot. We have found no evidence of that. Now granted, there are very significant and often—we have seen in the last 30 days several significant attacks that have been a costly annoyance to U.S. governments and businesses, and we have seen various worms and viruses. And we have seen that impact on the private industry with the power grids and whatnot. We have not seen to date a very precise launched attack from a terrorist group. We are attuned to that, and we are careful to look for signs for that activity, and we have not seen that to date.

Mr. DICKS. Ambassador Black, let me ask you, are we working with either—can you tell us what we are doing—I may have missed this in your statement, and forgive me. We had a lot of votes today. What are we doing with Canada and Mexico on these issues of international perspective in terms of the power grid? We know for a fact we are not investing enough money in the United States itself to keep our grid up to speed, but are we working and trying to cooperate with Canada and Mexico on these grid issues?

Mr. BLACK. We have a very close relationship with both Canada and Mexico. As an example, we have a conference with my Canadian counterpart and his delegation in an interagency context. We exchange—we go there, and they come here. This is going to be here in DC.

Mr. DICKS. Are there experts involved in this, or is it all policy?

Mr. BLACK. There are all experts involved, but again, this is sort of a recurring theme with the State Department. Our job is to facilitate the process; to make sure that everyone is communicating correctly, and that the quality of the exchange is good. We do not get involved in the mechanics of infrastructure defense. It is a process by which we make sure the lines of communication between the right agencies and the right experts between our two countries is there, ongoing, healthy, and it is good. Where there is a problem, we can step in and make sure that the appropriate adjustments are made.

We do a lot of work across the board, in the security field, in the law enforcement field, and in the immigration and naturalization. So we look to make sure that this relationship with these two countries is healthy and is across the board. And I think the quality of the exchange is very good. We participate in not only looking at the areas of common concern along the border, we look at ways we can assist each other in the common mission of counterterrorism elsewhere in the world, South America, with Canada, and other places in the world where they have a particular perspective or insight that is useful in the common defense of our respective homelands.

Mr. DICKS. Mr. Mefford, you made a comment about how DHS was doing in terms of developing analysis of the vulnerability of our critical infrastructure. Do you have any idea—maybe others

can speak to this, but how long it is going to take us to get a good handle on the major infrastructure of the country? I suspect that is going to take a few years to get done.

Mr. CAMP. If the witness could answer quickly. The gentleman's time has expired.

Mr. MEFFORD. The time line, I do not know.

Mr. DICKS. It is not done as of now.

Mr. MEFFORD. That is correct.

Mr. CAMP. Mr. Andrews may inquire.

Mr. ANDREWS. Thank you, Mr. Chairman. Thank the witnesses for their testimony.

I wanted to follow up on Mr. Dick's line of questioning, sort of ask the first half of the question. Mr. Mefford, if a utility company that was involved in the power grid experienced what they believe was an intrusion into their networks or their database, under what legal circumstances are they required to contact the FBI, and under what circumstances are they permitted—or is it discretionary for them to contact the FBI?

Mr. MEFFORD. That is a good question, and I would have to do some research to give you a specific answer from the legal context, because I do not think that I am aware of the mandatory requirement they contact us.

Mr. ANDREWS. I am sure the Chairman is keeping the record of the hearing open, and I would be interested in hearing the answer to the question.

Mr. MEFFORD. I am not sure if there is a specific requirement for somebody in that business, because I know in other lines of business there is not a mandated requirement.

Mr. ANDREWS. Let us hypothesize chillingly that the next time something like this happens in the United States, a blackout like this, in fact, was intentional, that someone tried to get in and cause a blackout. To whom—let us say a utility company sees an intrusion into its database and believes it was an intentional attack and wants to let someone know. Who do they tell?

Mr. MEFFORD. They can contact the nearest FBI office and relay that information. And the FBI Cyber Division would be assigned to look into that.

Mr. ANDREWS. Does the FBI tell utility companies that?

Mr. MEFFORD. Yes, I think so.

As far as your earlier question about the potential mandated requirement, let me just ask an expert.

I am informed that there is no mandated requirement.

Mr. ANDREWS. I would be interested in the Agency's thoughts about what such requirement might look like, whether it is desirable or undesirable.

Mr. MEFFORD. Also, I might add clearly the company that experiences this type of intrusion can contact the Department of Homeland Security, for instance, because we work with them in these cases, and if they notify the government, it would get to the right hands.

Mr. ANDREWS. This, frankly, is one of my concerns, and I don't fault the FBI for this, or anyone. There is a lot of different people they could contact, and it seems to me that information can move awfully slowly in a situation where we are not sure what it means,

as I think you testified. When you have 4,000 reports you got to run down, you don't jump every time you hear one report.

I think one of the things we ought to look at is some type of centralized protocol for the utility industry and for other critical infrastructure industries to report such an intrusion in one place in real time for the information to be shared with the relevant players in real time so there could be an assessment done to perhaps prevent such a problem.

Secretary Black, let me ask you a question. Let us assume that such an intrusion originated from another country that was somehow linked to us through networks and through other computer systems for critical infrastructure. Is there any international treaty or international law that requires countries to notify us—the scenario would be there is an intrusion which is initiated in a European country, let us say, that manifests itself in the United States with a breakdown of the power grid. Is there any international legal obligation for the neighboring state to tell us that?

Mr. BLACK. I would have to check, Congressman, and get back to you in writing, definitively, the legal aspects and requirements to do so. I will get back to you with that answer, sir.

Mr. BLACK. Practically, an assault on the infrastructure, the cyber infrastructure, among most countries would be communicated in one fashion or the other as it had an impact for the United States. Either internationally or here domestically in the United States, the process would be started and led by the Department of Homeland Security.

Mr. ANDREWS. I hear you say that is a matter of custom and not a matter of treaty or obligation.

Mr. BLACK. I would have to check on the legal obligation. But in addition to that, in the interim, practically, information like this is exchanged in a security context.

Mr. ANDREWS. As a secure communication among the foreign ministries or State Department?

I thank both of you for your testimony, and I would be interested on your thoughts on the question I raised.

Mr. CAMP. Ms. Slaughter may inquire.

Ms. SLAUGHTER. Thank you, Mr. Chairman.

Gentlemen, it is nice to have you here today. It was really one of the most beautiful days. I was about a mile away from the Niagara power facility when the lights went out. First thing I heard was Niagara Falls, it is their fault; a lightning strike. It was probably the best day we had all summer, and you can count those on two hands. And the big trouble was—you know, is what has happened. I think our first thought was we were perfectly content in our minds that that would never happen again; that after the last blackout, that all kinds of fail-safe measures were put in place. I don't really believe up in my part of the area—we were so worried about the terrorists that might have done something, we weren't sure what we were doing to ourselves. So we do what we often do: We blame the Canadians. And then the mayor of Toronto comes. And he has had a perfectly awful year—SARS—and he throws up his hands and says, have you ever known the Americans to take the blame for anything? Then we say we would all collectively blame Cleveland, and then it got over to Detroit.

As far as I know today, we are really not able to pinpoint what in the world happened there. This is probably the most frightening part of it to me, that we don't even know after 2 weeks what happened. And you have to ask yourself, if such a benign factor as somebody made a mistake somewhere could trigger the largest blackout in the history of North America, what in the world could we ever do to prevent something that is more malignant against us? And that is probably the thing that bothers me the most today. We not only don't know what happened then, we certainly don't know that we have anything in the world to stop anything in the future.

Couple of things we have been trying to do since September 11 is get a northern border coordinator. Since I have been in Congress now 17 years, we concentrate on the troubles of the southern border with Mexico. We have always had a great relationship. But a billion and a half dollars' worth of trade crosses that border every single day, and it is critical that we do everything we can not only to protect it, but to keep it open for trade. And we need a northern coordinator there because there are questions my colleagues have asked that are terribly important. Nobody knew who to call. All they knew is the lights are out, and they were working very hard to get them on. I assume they were talking to each other, but it was very, very difficult for any of us to know who to call. And I am afraid that we are going to get off balance like that again.

My major concern, and I don't know whether either of you have anything to do with it, but why we can't get answers as to precisely what happened, where we broke down? And the deregulation of electricity has been a terrible thing. We forced utilities to divest themselves of generation capacity for electricity. The transmission lines have been neglected. The prices have gone sky high. The history of Montana is replete with it. They had the lowest rates in the country until they deregulated. We are about to make some more mistakes here in Congress on an energy bill in throwing something in that we think might try to solve the problem of the blackout.

My biggest disappointment is the inability to really have any confidence at all in what happened there. While I am sure that it was benign, I really believe that, that it could not happen again in any given time, and it might give us a sense that we will not be able to—whether it was something we had done ourselves—unless they came in with bombs or blow up the place. But we can really destabilize the harm to this country by having this power grid that works well. And I am so impressed by this picture that is making the rounds of the United States with the blackout part in the New England and the Northeast, just dropped off the face of the Earth. And while we—I have a little municipal power plant in the town I live in, and we had one old coal-fired plant that went right along producing power like it was supposed to do all the time.

But I think we have come not too far in agreements concerning the possibilities. I am more worried about nuclear power, the vulnerability of nuclear plants than I am of the power grid itself. But I am not going to be happy first until I know what happened here and to have the will in this Congress to fix it, because that is really important. There is no import in me asking—you have good contact. We appreciate what you are doing very much. And if I could

ask a personal favor, Mr. Mefford, before you leave, I would like to ask you to talk about an incident that happened in my district last week.

Mr. CAMP. The gentlewoman's time has expired. Ms. Jackson-Lee may inquire.

Ms. JACKSON-LEE. Thank you very much, Mr. Chairman, and I will make a comment. I know that we have—if I might inquire, because as I am reading it, it is not listed on the front cover as two panels, but I assume we have two panels.

Let me—I hope I will be able to hear. Let me thank the witnesses for their presentations and just simply make the point, my delay was because we were having hearings on the Columbia 7 tragedy, and we decided that the important responsibility of Congress is, one, the accountability question, and then the what happened question so we would hope we wouldn't travel the same journey again.

I also made a comment that is associated with the Homeland Security Committee when the Columbia 7 incident happened on February 1, the fact that it happened post-9/11, you can imagine the thoughts that occurred as related to that incident, whether it was an act of terror. The same, I think, came to a lot of our minds with this incident dealing with the blackout. So I would hope that this committee would proceed with that focus, accountability, without shame, because without saying who did it, we can't help those in the future not to do it; and then a pathway, if you will, of how we should correct this issue.

So I would just offer to say to Mr. Black if I could, and maybe he could give me this brief answer, is that the approach being taken by the government agencies? Will we have a sense of accountability? And will we also have a pathway as it relates to homeland security, the question that we determined—I assume we have completed that, and maybe I am premature, that that was not an act of terror. Then how do we stand in the way of that?

Mr. BLACK. In terms of the blackout and terms of accountability, I know from the State Department perspective that we all—all of us Americans are looking to—seeking to get a full determination in the causes of what happened so this cannot happen again. And for additional information I turn it over to Mr. Mefford.

Mr. MEFFORD. The FBI is participating with a number of agencies in an integrated approach to find out what occurred, and clearly our perspective is the terrorist or criminal perspective; in other words, was somebody involved in criminal activity, were there terrorists involved? That is the scope and extent of our inquiry. To the degree we can contribute to the interagency understanding of what occurred, we are doing so in that regard.

Ms. JACKSON LEE. I thank you.

So the accountability and what happened partnership you think is a fair one?

Mr. MEFFORD. From my perspective, yes.

Ms. JACKSON LEE. I yield back.

Mr. CAMP. Thank you very much. I want to thank our panel.

Mr. PASCRELL. Could I ask just one more question?

Mr. CAMP. Briefly.

Mr. PASCRELL. I wanted to ask this before, but time ran out. Were there any intelligence operations or communications affected by the blackout?

Mr. MEFFORD. No, sir, not in the environment in which we are active. I can't speak for the broader Intelligence Community, but from the FBI standpoint, no.

Mr. PASCRELL. Your systems operated 100 percent during that blackout even in the areas affected?

Mr. MEFFORD. To my knowledge, yes.

Mr. CAMP. Again, I want to thank our panel. I appreciate you being here and your testimony. And this is a joint hearing, and I will turn the gavel over to Mr. Thornberry, who will chair the second part of this hearing.

Mr. THORNBERRY. [Presiding.] These witnesses are excused, and we would ask the second panel to come up and take your places.

First let me thank these witnesses for your patience, and I appreciate very much each of you taking the time to be with us today. As with the previous witnesses, we are going to make your full statement a part of the record. We are going to ask each of you to summarize in 5 minutes your statement and then turn to questions. We are going to start with Paul Gilbert, former panel Chair on Energy Facilities, Cities and Fixed Infrastructure, for the National Research Council.

Mr. Gilbert, thank you for being here. You are recognized for 5 minutes.

STATEMENT OF PAUL H. GILBERT, FORMER PANEL CHAIR, ENERGY FACILITIES, CITIES, AND FIXED INFRASTRUCTURE, NATIONAL RESEARCH COUNCIL

Mr. GILBERT. Thank you, sir. Good afternoon, and thank you, Chairmen, and all the members of the committee.

I am Paul Gilbert. I am a senior officer of Parsons Brinckerhoff as well as a member of the National Academy of Engineering, and was Chair of the National Research Council panel responsible for the chapter on energy systems in the NRC report, Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Copies of that report have been submitted to the subcommittee.

It is a pleasure to come before you today to assist in focusing attention on the vulnerabilities of our electric power system, including the cyber subsystems and the enormous dependency of our critical infrastructure on the electric supply. Over the past decade our electric supply system has been tasked to carry ever-increasing loads. It has also undergone a makeover from being a highly regulated, vertically integrated utility to one that is partially deregulated, far less unified, not so robust and resilient as it was. The generation side is essentially deregulated and operating under an open market set of conditions. At the same time the transmission sector remains fully regulated, but under voluntary compliance reliability rules, resulting in diminished investments in maintenance and spare parts and lower reliability.

Another concern is that in seeking to reduce operating costs, the operating companies have installed automated cybercontrollers, or SCADA systems, to perform functions that people previously per-

formed. These open architecture cyber units are an invitation for those who would seek to use computer technology to attack the grid.

The in-place electrical utility assets today are typically being operated at close to the limit of available capacity. In this mode another characteristic of such complex systems appears. When operated near their capacity, these systems are fragile, having little reserve within which to handle power or load fluctuations. When load and capacity are out of balance, shutting down becomes the only way a system element has to protect itself from severe damage. However, the loss of a piece of the grid, let us say a transmission line, does not end the problem. A line down takes down with it the power that it was transmitting. The connected power plant that was producing that power, having no connected load, must also shut down. In these highly integrated grids, more lines have imbalance problems, and more plants sense the capacity limitations and they all shut down. The cascading effect spreads rapidly in many directions, and in seconds an entire sector of the North American grid can be down. And this is what we experienced a few weeks ago from an accident, not from an attack.

The exact same consequences could, however, too easily be produced by a terrorist attack from a small, trained team. This was the scenario assumed in the Making the Nation Safer report, where several critical nodes in the grid were taken out in a well planned and executed terrorist attack. The cascading system failures resulted in regionwide catastrophic consequences. Recovery, in the case cited, was estimated to take weeks or months, not hours or days, and the damage done to our people and our economy was estimated to be enormous.

Now, while the report does not speculate in any detail on the extended consequences of such an event. I have been asked to do so here, and so I offer the following as a personal opinion. Based on the critical infrastructure, and because that critical infrastructure is so extensively integrated, with power out beyond a day or two in our cities, both food and water supplies would soon fail. Transportation systems would come to a standstill. Wastewater could not be pumped. And so we would soon have public health problems. Natural gas pressure would decline, and some would lose gas altogether, very bad news in the winter. Nights would become very dark with no lighting, and communications would be spotty or nonexistent. Storage batteries would have been long gone from the stores, if any stores were still open. Work, jobs, employment, business and economic activity would be stopped. Our economy would take a major hit. All in all our cities would not be very nice places to be. Some local power generators such as at hospitals would get back up, and so there would be islands of light in the darkness. Haves and have-nots would get involved. It would not be a very safe place to be either. Martial law would likely follow, along with emergency food and water supply relief.

At our core we would rally and find ways to get by while the systems are being repaired. In time the power would start to come back, tentatively at first, with rolling blackouts, and then in all its glory. Several weeks to months would have passed, and the enormous recovery and clean-up would begin. This is simply one per-

son's view, but based upon a fairly in-depth understanding of the critical interdependency of our infrastructure.

Chapter 6 of the Making the Nation Safer report addresses actions that are designed to minimize or control the vulnerabilities that exist in the electric power system. Those recommendations that were made some 15 months ago are as on point today as they were then. In some cases actions have been initiated. The blackout last month drew attention to the areas of critical infrastructure need and to the frightening dependence we have on power supplies.

We at the Academies are committed to continue to contribute our efforts to effectively resolve these issues. Thank you for inviting me today and for your leadership in holding these hearings, and I will be happy to answer any questions.

Mr. THORNBERRY. Thank you.

[The statement of Mr. Gilbert follows:]

PREPARED STATEMENT OF PAUL H. GILBERT

Good afternoon, Chairman Thornberry, Chairman Camp, and members of the Subcommittees. My name is Paul Gilbert. I am an officer and director emeritus of Parsons Brinckerhoff, Inc. I am also a member of the National Academy of Engineering and was Chair of the National Research Council Panel responsible for the Chapter on Energy Systems for the NRC Branscomb-Klausner Report, Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Copies of this report have been submitted to the subcommittees. As you know, the NRC is the operating arm of the National Academy of Sciences, National Academy of Engineering and the Institute of Medicine, chartered in 1863, to advise the government on matters of science and technology. The subject report was the product of the mobilized academies following the 9/11 attacks. Some 130 volunteers from every branch of science, engineering and medicine assembled to undertake this work on an urgent basis with the report production financed entirely with private funds of the Academies. The report was first presented in June of 2002. It is a pleasure to come before you today to assist in focusing attention on the vulnerabilities of our Electric Power Systems, including their cyber sub systems, and the enormous dependence of other critical infrastructure on the electric supply.

Our basic infrastructure systems include our electric power, food, and water supplies, waste disposal, natural gas, communications, transportation, petroleum products, shelter, employment, medical support and emergency services, and facilities to meet all our basic needs. These are a highly integrated, mutually dependent, heavily utilized mix of components that provide us with vitally needed services and life support. While all these elements are essential to our economy and our well being, only one has the unique impact, if lost, of causing all the others to either be seriously degraded or completely lost. And that, of course, is electric power. Our technically advanced society is literally hard wired to a firm, reliable electric supply.

Over the past decade, that electric supply system has been tasked to carry ever-greater loads (power demands). It has also undergone a makeover from being a highly regulated, vertically integrated utility industry to one that is partially deregulated, far less unified, and not so robust and resilient as it was. The generation side is essentially deregulated and operating under an open market set of conditions where competitive price, low operating costs and return on investment are rewarded with profits and bonuses. Applicable regulations are broad and not consistent state to state. At the same time the transmission sector remains fully regulated but under voluntary compliance reliability rules. Reported uneven voluntary compliance with reliability rules and diminishing investments in maintenance and spare parts by the transmission companies have pointed to the need for the legislation pending which intends to make mandatory the rules for transmission operations. This result is clearly a necessity for our national safety.

Another concern is that in seeking to reduce operating costs, operating companies have installed SCADA units and LANs, automated cyber controllers, to perform functions that people previously performed. These open architecture cyber units are an invitation for those who would seek to use computer technology to attack the grid.

The dramatic changes described have played out with the result that the in-place electrical system assets today are, of necessity, typically being operated very effi-

ciently at close to the limit of available capacity. In this mode, another characteristic of such complex systems appears. When operated near their capacity, these systems are fragile, having little reserve within which to handle power or load fluctuations. When load and capacity are out of balance, shutting down becomes the only way a system element has to protect itself from severe damage. However, the loss of a piece of the grid, a section of transmission line, does not end the problem. The line down takes with it the power it was transmitting. A connected power plant that was producing that power, having no connected load, must also shut down. In these highly integrated grids, more lines have imbalance problems and more plants sense capacity limitations and so they also shut down. This cascading failure spreads rapidly in many directions and in seconds, an entire sector of the North American grid can be down. We had a living example of this event, last month, caused by an accident. We were fortunate to see the power return in so short a time.

The exact same consequences could too easily be reproduced by a terrorist attack from a small trained team. This was the scenario assumed in the Making the Nation Safer report where several critical nodes in the grid were taken out in a well planned and executed terrorist attack. The cascading system failures resulted in region-wide catastrophic consequences. Recovery, in the case cited, was estimated to take weeks or months, not hours or days, and the damage done to our people and our economy was estimated to be enormous.

While the report does not speculate in any detail on the extended consequences of such an event, I have been asked to do so here, and so offer the following as a personal opinion. Because our critical infrastructure is so very integrated, with power out beyond a day or two, both food and water supply would soon fail. Transportation systems would be at a standstill with no power to pump the fuels. Wastewater could not be pumped away and so would become a health problem. In time natural gas pressure would decline and some would lose gas altogether. Nights would be very dark, and communications would be spotty or non-existent. Storage batteries would have been long gone from the stores, if any stores were open. Work, jobs, employment, business and economic activity would be stopped. Our economy would take a major hit. All in all, our cities would not be very nice places to be. Some local power generators and grids would get back up and so there would be islands of light in the darkness. "Haves" and "have-nots" would get involved. It would not be a very safe place to be either. Marshal law would likely follow along with emergency food and water supply relief. At our core, we would rally and find ways to get by while the system is being repaired. In time, the power would start to come back, tentatively at first, with rolling blackouts, and then in all its glory. Several weeks to months would have passed, and the enormous clean up and recovery would begin. This is one person's opinion, based on an understanding of this highly dependent infrastructure system.

We have the means to limit the kind of disaster that has been speculated upon above. The recommendations provided in Chapter 6 of the report address actions that are designed to minimize or control the immediate vulnerabilities that exist in the electric power systems and then to seek longer-term, more permanent solutions. Those recommendations are as on-point today as they were when published 15 months ago. In some cases actions have been initiated along the lines recommended. To paraphrase key points:

- Immediate attention is needed to mobilize the leadership, and then the resources of people and organizations to first determine the proper roles for each interested party, and then to come together, meet and develop needed plans. Some of this recommendation has been achieved.
- Issues that deter open discussions among the private and governmental parties need to be quickly resolved. These include matters of antitrust, liability and FOIA.
- Review by government of the institutional and market settings for the industry (regulated, deregulated, and open free market) need attention to refocus the included incentives on what the nation needs to live safely.
- Tools now employed by the military to analyze facility vulnerabilities should be mobilized for use on the grids, perhaps by transferring them to DHS.
- Coordinated studies are indicated to identify the most critical equipment in the respective power systems and to describe the protective measures to be taken with each. Some progress has been reported here.
- For these highly complex grids, simulation models that are capable of identifying points of greatest vulnerability and transmission reserves remaining in critical sections of the grid are needed.
- Statutory action is indicated to allow recovery crews to immediately enter what would then be a crime scene following an attack to quickly commence the work of repair, recovery, and restoration of service.

• Regulatory bodies must be encouraged to find the means for transmission organizations to define costs for counter terrorism improvements and for recovering those costs from their operations or from other sources.
• The use of SCADA systems in unprotected configurations should be addressed, and expert advice obtained regarding the options available to correct the vulnerabilities now present.
• Research is indicated that addresses particular critical system equipment needs. First among the list is the potential value of modular universal EHV transformers to support rapid grid recovery.
• For the longer term, research is needed to determine the equipment, technology and processes required for transition our grid systems to become smart grids, intelligent, adaptive power grids.

There is more substance and detail in Chapter 6 of the referenced report. The unfortunate black out last month has drawn important attention to this area of critical infrastructure need and to the frightening dependence we have on our power supplies. We at the Academies are committed to continue to contribute to the efforts to effectively resolve these issues.

Thank you for inviting me today and for your leadership in holding these hearings. I will be happy to respond to your questions.

Mr. THORNBERRY. And a copy of that report from the National Research Council has already been made available to each member of the subcommittee. So we thank you.

Our next witness is Peter Orszag, senior fellow from the Brookings Institution. You are recognized for 5 minutes.

STATEMENT OF PETER R. ORSZAG, Ph.D., JOSEPH A. PECHMAN SENIOR FELLOW, BROOKINGS INSTITUTION

Mr. ORSZAG. Thank you very much for the opportunity to appear before you this afternoon.

The blackout of 2003 has underscored concerns about the vulnerability of our Nation's critical infrastructure to both accidents and deliberate attack, providing an immediate connection to the Nation's homeland security efforts. But the blackout may offer a deeper lesson. A common explanation for the problems facing the electricity system is that private firms have had inadequate incentives to invest in distribution lines.

An important point is that market incentives are extremely powerful, but for that very reason it is essential that they be structured properly. As the FERC Chairman has put it, we cannot simply let markets works, we must make markets work.

In the context of homeland security, we simply can't let markets work either. They won't. So we have to make them work. We have to change the structure of incentives facing private firms so market forces are directed towards reducing the cost of achieving a given level of security instead of providing a lower level of security than is warranted. Given the significance of the private sector in homeland security settings, this task is critical.

To be sure, private firms do have some incentive to avoid the direct financial losses associated with a terrorist attack on their facilities or operations. In general, however, and despite claims to the contrary made by many homeland security officials, that incentive is not compelling enough to encourage the appropriate level of security and therefore must be supplemented with stronger market-based incentives to increase the level of security.

My written testimony provides several reasons for why private markets by themselves do not generate sufficient incentives for investments in homeland security. As just one example, consider the

effect of bankruptcy laws. Such bankruptcy laws limit the corporate and individual financial exposure to the losses from an attack and can thereby attenuate the incentives to protect against attacks, especially in the context of catastrophic failures of network systems that can cause losses that far exceed the net worth of any individual company.

The general conclusion is that we just can't leave it up to the market in protecting ourselves against terrorist attacks. The market has an important role to play. Government intervention in some form and in some markets will be necessary to fashion the appropriate response to the threat of terrorism.

Now, the need for government intervention in some cases and some markets doesn't tell you how the government should intervene or precisely when. And in my written testimony I do provide some guidelines for when intervention is appropriate, and also point to a model that I think is the most auspicious in terms of being cost-effective, at least over the longer term, which combines some minimal level of regulation and an insurance requirement and third-party inspections. Under this system, the government would set some level of security regulations for private firms and then mandate the purchase of antiterrorism insurance. Private insurance firms would then provide incentives for safer behavior by offering premium reductions to firms that improve their security. And third-party auditors would help insurance firms make sure that the insured firms are actually doing what they are saying they are doing, and also helping ensure that the minimum level of government regulations are being met without a huge government bureaucracy.

A mixed regulatory insurance system similar to this is already applied in many other sectors, such as owning a car or a house. Consider your house. There are local building codes that regulate the structure of that house. That is a regulatory approach. But in general, when you go to get a mortgage, you also have to have insurance, and insurance firms provide incentives for going beyond the minimum level of the building code. If you put in a security system, you will get a premium break for doing so. So the insurance firm is providing you an incentive to have a safer house than the minimum regulatory standard would suggest.

And I offer other examples that already exist. This sort of mixed system of minimum standards coupled with an insurance mandate can not only encourage private firms to act more safely, but can also provide incentives for innovation to reduce the cost of achieving a given level of security over time, and I think that is particularly important in the homeland security context. It also has the advantage of being flexible also, an important attribute in an environment in which threats are evolving.

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 to test-pilot this type of approach with regard to making chemical facilities safer not against terrorist attacks, but safer against accidents, and I think that this basic model could be applied in many homeland security settings.

In conclusion, this typed of mixed system of minimum regulatory standards, insurance and third-party inspections could harness market forces to provide homeland security in a cost-effective way. Of course, this approach can and should be supplemented or replaced when there is evidence that other approaches would be more efficient.

But my important bottom line is that we cannot simply assume that the market will ensure that we are adequately—and by "we," I mean our private facilities and operations which are so critical to our economy—are adequately protected against attack. They won't. We have to make markets work better than they would in the absence of government intervention.

Thank you very much, Mr. Chairman.

Mr. THORNBERRY. Thank you very much. I appreciate it.

[The statement of Mr. Orszag follows:]

PREPARED STATEMENT OF PETER R. ORSZAG[1], PH.D., JOSEPH A. PECHMAN SENIOR FELLOW IN ECONOMIC STUDIES, THE BROOKINGS INSTITUTION

The blackout of 2003 has underscored concerns about the vulnerability of our nation's critical infrastructure to both accidents and deliberate attack, providing an immediate connection to the nation's homeland security efforts. But the blackout may offer a deeper lesson beyond the vulnerability of the nation's electricity grid to terrorist attack. In particular, a common explanation for the problems facing the electricity system is that private firms have had inadequate incentives to invest in distribution lines.

The important point is that market incentives are extremely powerful. For that very reason, however, it is essential that they be structured properly. As Patrick Wood, chairman of the Federal Energy Regulatory Commission, has put it: "We cannot simply let markets work. We must make markets work."[2]

In homeland security, private markets do not automatically produce the best result. We must therefore alter the structure of incentives so that market forces are directed toward reducing the costs of providing a given level of security for the nation, instead of providing a lower level of security than is warranted. Given the significance of the private sector in homeland security settings, structuring incentives properly is critical.

To be sure, private firms currently have some incentive to avoid the direct financial losses associated with a terrorist attack on their facilities or operations. In general, however, that incentive is not compelling enough to encourage the appropriate level of security—and should therefore be supplemented with stronger market-based incentives in several sectors.

My testimony argues that:

- Private markets, by themselves, do not provide adequate incentives to invest in homeland security, and
- A mixed system of minimum regulatory standards, insurance, and third-party inspections would better harness the power of private markets to invest in homeland security in a cost-effective manner.

Incentives for homeland security in private markets

Private markets by themselves do not generate sufficient incentives for homeland security for seven reasons:

- Most broadly, a significant terrorist attack undermines the nation's sovereignty, just as an invasion of the nation's territory by enemy armed forces would. The costs associated with a reduction in the nation's sovereignty or

[1] The views expressed here do not necessarily represent those of the staff, officers, or board of the Brookings Institution. I thank Michael O'Hanlon, Ivo Daalder, I.M. Destler, David Gunter, Robert Litan, and Jim Steinberg for the joint work upon which this testimony draws, Emil Apostolov for excellent research assistance, and Howard Kunreuther for helpful comments. For related details, see *Protecting the American Homeland: One Year On* (Brookings Institution Press: 2003). Also see Howard Kunreuther, Geoffrey Heal, and Peter Orszag, "Interdependent Security: Implications for Homeland Security Policy and Other Areas," Policy Brief #108, Brookings Institution, October 2002, and Howard Kunreuther and Geoffrey Heal, "Interdependent Security," Journal of Risk and Uncertainty 26: 231–249 (March/May 2003).

[2] Quoted in David Wessel, "A Lesson from the Blackout: Free Markets Also Need Rules," Wall Street Journal, August 28, 2003.

standing in the world may be difficult to quantify, but are nonetheless real. In other words, the costs of the terrorist attack extend well beyond the immediate areas and people affected; the attack imposes costs on the entire nation. In the terminology of economists, such an attack imposes a "negative 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.[3] Without government involvement, private markets will thus typically under-invest in anti-terrorism measures.[4]

• 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.[5] 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 reason-

---

[3] 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.

[4] 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 indirectly by a terrorist attack, the costs of negotiation are prohibitive, making the Coase theorem essentially irrelevant in the terrorism context.

[5] 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.

able 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.

• 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.

The relative strength of these potential justifications for government intervention varies from case to case. Furthermore, the benefits of any government intervention must be weighed against the costs of ineffective or excessively costly interventions—that is, that the government intervention may do more harm than good. Even if an omniscient government could theoretically improve homeland security in a manner that provides larger benefits than costs, it is not clear that real-world governments—suffering from political pressures, imperfect information, and skewed bureaucratic incentives—would. The potential for government failure depends on the characteristics of the particular government agency and the sector involved. For example, it seems plausible that government failure is a particular danger in innovative and rapidly evolving markets.[6]

Both the need for government intervention and the potential costs associated with it thus vary from sector to sector, as should the policy response. Government intervention will generally only be warranted in situations in which a terrorist attack could have catastrophic consequences. Nonetheless, the general conclusion is that we can't just "leave it up to the market" in protecting ourselves against terrorist attacks. The market has an important role to play, but government intervention in some form and in some markets will be necessary to fashion the appropriate response to the threat of terrorism.

Modifying incentives for the private sector to invest in homeland security

The need for some sort of government intervention to protect private property and activities against terrorism does not determine how or in which situations the gov-

[6] As the great British economist Alfred Marshall emphasized, "A Government could print a good edition of Shakespeare's works, but it could not get them written. . .Every new extension of Governmental work in branches of production which need ceaseless creation and initiative is to be regarded as prima facie anti-social, because it retards the growth of that knowledge and those ideas which are incomparably the most important form of collective wealth." Alfred Marshall, "The Social Possibilities of Economic Chivalry," *Economic Journal,* 1907, pages 7–29.

ernment should intervene. The various tools that the government could employ, furthermore, will likely determine how costly the intervention will be, as well as who will bear those costs. For example, to improve safety in commercial buildings, the government could:

- Impose direct regulation: The Federal government could require that certain anti-terrorist features be included in any commercial or public building.[7]
- Require insurance: The Federal government could require every commercial or public building to carry insurance against terrorism, much as state governments now typically require motorists to carry some form of auto liability insurance.[8] The logic of such a requirement is that insurance companies would then provide incentives for buildings to be safer.
- Provide a subsidy for anti-terrorism measures: The Federal government could provide a subsidy—through direct government spending or through a tax incentive—for investing in anti-terrorism building features or for other steps to protect buildings against attacks.

More broadly, each of the various approaches for minimizing the dangers and potential damages related to terrorism likely entails a different level of aggregate costs, and also a different distribution of those costs across sectors and individuals.[9]

Direct regulation

The principal benefit of a direct regulatory approach is that the regulatory standard provides a minimum guarantee regarding anti-terrorism protection, assuming the regulations are enforced.[10] For example, if skyscrapers are natural targets for terrorists, requiring security measures in such buildings accomplishes two goals:

- First, it ensures that the buildings are better protected against attack.
- Second, it raises the costs of living in skyscrapers and therefore discourages people from living there—which may be appropriate as a means of diminishing the nation's exposure to catastrophic attack, given the buildings' assumed attractiveness to terrorists.

There are, however, also downsides to direct regulation:

- First, the minimum regulatory threshold may be set at an inappropriate level.[11]
- Second, a regulatory approach, especially one that reflects a "command and control" system rather than market-like incentives, can be an unnecessarily expensive mechanism for achieving a given level of security.[12] Such an approach

---

[7] Although building codes traditionally fall within the jurisdiction of local governments, the Americans with Disabilities Act (ADA) mandated changes in buildings. A precedent therefore exists for Federal pre-emption of local building codes. It should be noted that the ADA does not directly affect existing building codes. But the legislation requires changes in building access and permits the Attorney General to certify that a State law, local building code, or similar ordinance "meets or exceeds the minimum accessibility requirements" for public accommodations and commercial facilities under the ADA. Such certification is considered "rebuttable evidence" that the state law or local ordinance meets or exceeds the minimum requirements of the ADA.

[8] The McCarren-Ferguson Act delegates insurance regulation to the states. The Federal government could nonetheless effectively impose an insurance mandate either by providing strong incentives to the states to adopt such a mandate, or perhaps by mandating that all commercial loans from a federally related financial institution require the borrower to hold such insurance.

[9] In theory, the different approaches to implementing a security measure could be separated from how the costs of the measure were financed—for example, firms adhering to regulatory standards could be reimbursed by the Federal budget for their costs. In practice, however, the method of implementation often implies a method of financing: the cost of regulations will be borne by the producers and users of a service, and the cost of a general subsidy will be borne by taxpayers as a whole. In evaluating different implementation strategies, financing implications must therefore be taken into account.

[10] Fines could be adopted as part of the regulatory system to ensure compliance with minimum standards for preventative measures.

[11] In other words, an anti-terrorism standard for, say, athletic arenas could impose an excessively tight standard (which would involve unnecessary costs) or an excessively loose standard (which would involve insufficient protection against terrorist threats).

[12] For example, in the environmental context, placing the same limit on emissions of harmful substances by all firms or individuals ignores the differences in costs of preventing pollution. That is why economists have long advocated market-based approaches to emission reductions, such as a permit trading system (which is currently in place for sulfur dioxide emissions) or a tax on emissions. Either market-based approach to regulation can achieve the same level of environmental protection at lower overall cost than a regulatory approach because it encourages those who can most cheaply control pollution do so (to avoid paying for the permit or the tax). A key requirement for a permit trading system or a tax, however, is some system for measuring "outcomes," such as the monitoring of pollution emitted by parties subject to the tax or participating in the system. In the context of anti-terrorism measures, the appropriate metric would be related to the expected loss from a terrorist attack. Yet it is difficult to see how such expected losses could be quantified and thus provide the basis for a permit trading system or a tax.

may be particularly inefficient because of the substantial resources required to enforce the regulations.

• Third, the regulatory approach does not generally provide incentives for innovation. Firms would have an incentive to meet the minimum regulatory standard, but little incentive to exceed it. Indeed, depending on how it is written, regulation may impede innovation in finding new (and less costly) approaches to improving protection against terrorism, especially if the rules are of the standard "command and control" variety.

These costs of regulation can be reduced, although not eliminated, through careful attention to the design of the regulations. In particular, the more regulations focus on outcomes and performance, rather than specific inputs, the better. For example, a regulation affecting an indoor athletic arena could state that the arena's air ventilation system must be able to contain a given type of bio-terrorist attack within a specific amount of time, rather than that the system must include specific devices. Compliance with the performance-based regulation can then be tested regularly by government inspectors or third-party auditors. Such a performance-oriented set of regulations provides at least some incentive for firms to design and implement less expensive mechanisms for achieving any given level of security.

Insurance requirement

An insurance requirement is a possible alternative to direct government regulation.[13] At first glance, an insurance requirement may seem counterproductive: Firms and individuals who have insurance against terrorism 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. Furthermore, and perhaps more importantly, the insurance companies themselves have an incentive to encourage risk-reducing activities.[14] Insurance firms could provide incentives for measures that reduce the exposure of buildings to terrorist attack (such as protecting or moving the air intake), or that reduce the likelihood of a successful cyber-attack on a computer system or intranet (such as improved firewalls and more advanced encryption).

An insurance requirement is clearly not a panacea, however. One issue is the degree to which the insurance market would discriminate among terrorism risks (or would be allowed to do so by regulators). For example, consider the higher risks for such "iconic" structures as the World Trade Center, the Empire State building, and other tall structures elsewhere in the country. If insurers are not restricted by government policy from charging appropriately risk-related premiums, insurance markets will discourage the construction of such potential terrorist targets in the future. Such an outcome may be efficient in the sense of reducing potential exposure to terrorist attacks, but it may have other social costs.

In evaluating the effects of variation in insurance premiums, a distinction should be drawn between existing buildings and new construction. The owners of existing buildings likely did not anticipate the terrorist threat when the buildings were constructed. Any additional costs on such existing buildings would reduce their market values, imposing capital losses on their owners. Some may not view this outcome as fair: it effectively imposes higher costs on the owners (or occupants) of an existing building to address a threat that was largely unexpected when the buildings were constructed. Others may view the outcome as eminently fair, since the alternative would be to have the population as a whole effectively provide a subsidy to the owners of prominent buildings.[15] For new construction, the case for differentiated insurance premiums is stronger, since the prospective owners are now aware of the

---

[13] The insurance requirement would complement the use of the liability system to encourage protective measures: Insurance coverage would be relatively more important in the context of large liability exposures.

[14] By similar reasoning, insurers should not be able to use genetic information to discriminate in rates charged for health coverage since individuals cannot control their genetic makeup.

[15] Failing to allow insurance firms to discriminate across risks in pricing policies could also induce "cherry-picking" of the lowest risks by the insurance firms and make it difficult for the higher risks to obtain the insurance from any firm. It is worth noting that in the United Kingdom, a government-sponsored mutual insurance organization, Pool Re, provides anti-terrorism insurance. The rates vary by location, with the highest in Central London and the lowest in rural parts of Scotland and Wales. See Howard Kunreuther, "The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage" *Business Economics* April 2002 For further analysis of the Pool Re and other programs abroad, see General Accounting Office, "Terrorism Insurance: Alternative Programs for Protecting Insurance Consumers," GAO–02–199T, October 24, 2001, and Congressional Budget Office, "Federal Reinsurance for Terrorism Risks," October 2001.

threat of attack and since differentiated premiums could play an important role in encouraging safer designs of prominent buildings.

Another potential problem with an insurance approach involves the capacity of insurers to price the insurance and provide incentives for specific anti-terrorism steps. If government regulators find it difficult to undertake comparative benefit analysis in fighting terrorism, it is likely that private insurers would face similar challenges—especially in the face of network effects. The problem is exacerbated by the absence of solid actuarial information on the risks involved, which in turn reflects the nation's good fortune thus far in not being exposed to a large number of terrorist attacks. Nonetheless, as the Congressional Budget Office has noted, "Not every new risk has proved to be uninsurable. For example, the changing legal environment for product liability, which makes predicting losses difficult, has affected how insurers manage such risks, but it has not resulted in insurers' dropping all product liability coverage. Rather it has produced a combination of more restricted coverage, shared responsibility, and modifications in producers' behavior."[16]

Perhaps most fundamentally, an insurance system won't work if insurers won't offer the insurance or offer it only at extremely high prices relative to their underlying actuarial models, or if firms are not required to purchase the insurance and don't see a need for it. Some economists and market observers have raised important questions about whether capital market imperfections impede the ability of insurers to provide coverage against catastrophic risks, such as those involved in terrorist activities.[17] A particular concern involves reinsurance: the transfer of risk from the primary insurance company to another entity. Rather than maintaining high reserves to meet the potential costs of extreme events, primary insurance firms buy reinsurance from other firms. The reinsurance covers at least part of a severe loss, attenuating the risks faced by the primary insurers. To ensure that primary insurers continue to cover terrorism risks, the Federal government has provided terrorism reinsurance. A temporary Federal program makes sense; over time, as new approaches to spreading the financial risks associated with anti-terrorism insurance develop, the need for any government reinsurance program could be reduced.[18] A substantial flaw with the current reinsurance program, though, is that no fee is imposed. A better approach to federal reinsurance would have the government share the risk, but also the premiums, from primary terrorism insurance.[19]

Despite these potential problems, it is plausible that a broader system of anti-terrorism insurance could develop over the medium to long term, and thereby play a crucial role in providing incentives to private-sector firms to undertake additional security measures when such steps are warranted given the risk of a terrorist attack (at least as viewed by the insurance firm).

Subsidies for anti-terrorism measures

A third form of government intervention would take the form of subsidies for anti-terrorism measures undertaken by private actors. Subsidies could affect firm behavior, and (if appropriately designed) provide some protection against terrorist threats. Subsidies, however, carry four dangers:

- First, they can encourage unnecessarily expensive investments in security measures (or "gold plating").[20]
- Second, a subsidy approach would likely spark intensive lobbying efforts by firms to capture the subsidies—which not only dissipates resources that could

---

[16] CBO also notes that private insurers in Israel provide some anti-terrorism coverage (involving indirect losses such as the costs of business interruptions from terrorist attacks). Congressional Budget Office, "Federal Reinsurance for Terrorism Risks,' October 2001.

[17] See, for example, Kenneth Froot, "The Market for Catastrophic Risk: A Clinical Examination," NBER Working Paper 8110, February 2001.

[18] For alternatives to a federal reinsurance program, see J. Robert Hunter, "How the Lack of Federal Back Up for Terrorism Insurance Affected Insurers and Consumers: An Analysis of Market Conditions and Policy Implications," Consumer Federation of America, January 23, 2002.

[19] See, for example, David Moss, Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, October 30, 2001.

[20] Consider, for example, a tax credit equal to 50 percent of the cost of building improvements that protect against terrorism. Such a high subsidy rate may encourage firms to undertake too much investment in security against terrorism—in the sense that the costs of the investment are not fully justified by the protections they provide against terrorism. For example, reinforced windows may provide protection against shattering in the event of a terrorist attack. Even if the protection provided is minimal, the firm may find it worthwhile to undertake the investment since so much of the cost is borne by others, and since the reinforced windows may provide other benefits (such as reduced heating and cooling costs because of the added insulation). Relatedly, a subsidy provides a strong incentive for firms to classify changes that would have otherwise been undertaken as "anti-terrorism" measures in order to qualify for the subsidy.

have been used more productively elsewhere, but may skew the definition of what qualifies for the subsidy toward inappropriate items.[21]

• Third, subsidies could provide benefits to firms that would have undertaken the activities even in the absence of the subsidy—raising the budget cost without providing any additional security.

• Finally, subsidies financed from general revenue are effectively paid for by the entire population. The fairness and feasibility of that approach is debatable, especially in face of the dramatic deterioration in the Federal budget outlook over the past several years and the recognition that other pressing needs will put increased pressure on the budget even without subsidizing private-sector protective measures.

Toward a mixed system: Minimum regulatory standards, insurance, and third-party inspections

As the discussion above has highlighted, all of the various approaches to government intervention have shortcomings, and the relative importance of these drawbacks is likely to vary from sector to sector. Nonetheless, in many cases that require government intervention, one longer-term approach appears to be the least undesirable and most cost-effective: a combination of regulatory standards, insurance requirements, 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]

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.[23] The presence of minimum regulatory standards also helps to attenuate the moral hazard effect from insurance, and can provide guidance to courts in determining negligence under the liability laws.[24]

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

---

[21] Lobbying would undoubtedly occur in the context of a regulatory approach, but since regulations are made on the basis of some kind of evidentiary record and are subject to judicial review, the room for lobbying is restricted. In contrast, subsidies are expenditures of the government and handed out by Congress, which is inherently much more amenable to lobbying.

[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 attacks. 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] Moreover, an insurance *requirement* (as opposed to an insurance option) avoids the adverse selection problem that can occur in voluntary insurance settings. In particular, if anti-terrorism insurance were not mandatory, firms with the most severe terrorism exposure would be the most likely to demand insurance against terrorist acts. The insurance companies, which may have less information about the exposure to terrorism than the firms themselves, may therefore be hesitant to offer insurance against terrorist attacks, since the worst risks would disproportionately want such insurance. The outcome could be either that the insurance companies do not offer the insurance, or that they charge such a high price for it that many firms (with lower exposure to terrorism but nonetheless some need to purchase insurance against it) find it unattractive. This preference for mandatory insurance assumes no constraints or imperfections on the supply side of the insurance market.

[24] 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.

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.[25]

Applying the mixed system

Three examples of homeland security issues seem relatively well-suited to a mixed system of regulatory standards, anti-terrorism insurance, and third-party inspections:

- Security at chemical and biological plants. Such plants contain materials that could be used as part of a catastrophic terrorist attack, and should therefore be subjected to more stringent security requirements than other commercial facilities. The regulatory standards could be supplemented by an insurance requirement, which would then allow insurance firms to provide incentives for more innovative security measures.
- Building security for buildings that house thousands of people. The Federal government could supplement existing building codes for large commercial buildings with minimum performance-based anti-terrorism standards. Those regulations could then be supplemented by requiring the owners of buildings to obtain anti-terrorism insurance covering some multiple of the value of their property. Adjustments to the basic premium could encourage building improvements that reduce the probability or severity of an attack (such as protecting the air intake system or reinforcing the building structure).
- Cyber-security. Since the steps involved in protecting a computer system against terrorist attack are similar to those involved in protecting it against more conventional hacking, the case for Federal financing is relatively weak. Federal subsidies of anti-terrorism cyber-security measures at private firms would likely induce excessive "investment," since the firms would not bear the full costs but would capture many of the benefits (through improved security against hacking attempts). Nonetheless, a successful terrorist cyber-attack could cripple the nation's infrastructure, at least temporarily. Some performance-oriented regulatory steps may therefore be warranted. For example, the government could require critical computer systems to be able to withstand mock cyber-attacks, with the nature of the cyber-attack varying from firm to firm. Given the ease with which mock attacks and tests could be conducted—which could provide a basis for pricing the insurance—an insurance requirement may be feasible and beneficial. One could even imagine insurance firms hiring cyber-experts to advise insured firms on how to reduce their exposure to cyber-attacks. To be consistent with reasonable thresholds for government intervention, any regulatory or insurance requirements could be imposed only on larger firms or those that have direct access to critical computer infrastructure components.

Conclusion

This testimony argues that a mixed system of minimum standards, insurance, and third-party inspections could harness market forces to provide homeland security at minimum cost. This approach can and should be supplemented or replaced when there is evidence that other approaches would be more efficient or when there are significant externalities associated with a given type of terrorism. For example, in some cases, the insurance requirement may not be necessary because lenders already require terrorism insurance to be carried before extending loans—and a government mandate is thus effectively superfluous. Furthermore, it will undoubtedly take time for the insurance industry to develop appropriate ways of pricing policies covering potentially catastrophic attacks.

---

[25] For further information, see Howard Kunreuther, Patrick McNulty, and Yong Kang, "Improving Environmental Safety Through Third Party Inspection," *Risk Analysis.* 22: 309–18, 2002.

The degree of government intervention should clearly vary by circumstance. For example, consider the difference between security at a mall and security at a chemical facility. Poor security at a mall does not endanger remote areas in the nation to nearly the same degree as poor security at a chemical facility. The products of chemical plants could be used as inputs in a terrorist attack, and therefore the facilities warrant more aggressive government intervention than shopping malls. Thus security regulations for chemical plants may make sense, even if they don't for shopping malls.

A critical challenge is deciding how extensive government regulation should be. It is one thing to set standards for commercial facilities such as chemical and biological plants. But should the government attempt to provide anti-terrorism regulations for all commercial buildings? For hospitals? For universities? Where does the regulatory process stop? One answer to this question is provided in *Protecting the American Homeland,* which focuses on reducing the risk of large-scale terrorist attacks.

A final issue is who should pay for improved security in the private sector. My general answer is that the costs should be imposed on the users and providers of a particular service. Such a "stakeholder pays" approach ensures that those who engage in the most dangerous activities (in terms of their exposure to terrorist attacks) pay for the costs associated with those risks.

Mr. THORNBERRY. Next is John McCarthy, who is executive director of the Critical Infrastructure Protection Project at George Mason University. Thank you for being here. You are recognized for 5 minutes.

STATEMENT OF JOHN A. McCARTHY, EXECUTIVE DIRECTOR, CRITICAL INFRASTRUCTURE PROTECTION PROJECT, GEORGE MASON UNIVERSITY

Mr. MCCARTHY. Thank you, Mr. Chairman, and thank you, distinguished members of the committee, for the honor of appearing before you today.

As a preliminary matter I would like to introduce the Critical Infrastructure Project within George Mason University's School of Law, where I serve as the executive director. The CIP Project has a unique role in building an interdisciplinary research program that fully integrates the disciplines of law, policy and technology. We are developing practical solutions for enhancing the security of cybernetworks, physical structures and economic processes underlying the Nation's critical infrastructures. The project is specifically charged with supporting research that informs needs and requirements outlined by the various national homeland security strategy documents.

Since its inception a little over a year ago, we have sponsored more than 70 substantive research projects touching leading scholars at 20 universities, with James Madison University as a lead partner, and focusing more than 200 graduate and undergraduate students on security-related studies. The CIP Project-sponsored research ranges from highly technical efforts designing new security protocols for cybersystems to mapping infrastructure vulnerabilities, to exploring legal and business government implications of information-sharing, to experimental economic analysis by the most recent Nobel Laureate in economics. In addition, GMU leads an academic consortium of regional scholars supporting CIP vulnerability analysis and interdependency identification for homeland security planning efforts here in the National Capital region. We are working closely with the Department of Homeland Security to ensure vulnerability assessments and modeling tools built locally that could be deployed nationally.

The Northeast blackout provides a clear example of disruption to our vital infrastructures. I will focus my comments today on those issues I believe are key areas of critical infrastructure protection that require continued emphasis, these being the need to develop a comprehensive understanding of infrastructure vulnerabilities and tools to assess those vulnerabilities; the need to better understand the complex interdependencies between infrastructure sectors; and the need to develop effective systems of public/private partnership that afford true information-sharing.

The blackout and its consequences serve as an effective yardstick by which to measure critical infrastructure protection since 9/11. On a positive note, most areas that were affected by the blackout had power restored within 24 hours. Considering the large geographic area, the number of jurisdictions involved and the international aspect of the blackout, this was a sound response. Particularly noteworthy were the cross-sector public-private communications that took place away from the eyes of the media. These communications involved industry, State, local and national decision-makers. I believe these relationships were not ad hoc responses to the blackout, but the results of efforts of the past decade in developing a means for enhancing information exchange between the public and private sector.

First, the blackout experience highlights our Nation's serious problems with infrastructure, including poor comprehension of our vulnerabilities and lack of awareness or preparedness for the interdependencies of those infrastructures. The blackout stresses the need to further identify, map, define our critical assets and properly assess their vulnerabilities, as 9/11, the first bombing of the World Trade Center, Y2K and numerous debilitating cyberattacks have shown us also. Comprehensive infrastructure mapping allows us to assess exactly where vulnerabilities are, what redundancies are needed, and how to recover quickly from a disruption by physical or cyber means.

It is important to map out each of the critical infrastructures and how they work with each other and study the possible effects that losses on one infrastructure will have on another. This type of mapping is vital in addressing and managing future infrastructure disruptions. These analyses must also include evaluation of myriad possible scenarios that may pose threats to critical systems and provide identification of physical and process actions, as well as economic incentives to industry that afford greater resiliency and security of key infrastructure assets. For example, in the short term, the use of redundant electrical generation at hospitals in New York resulted in virtually no loss of service delivery capability for emergency and health care providers.

Next, the blackout also highlights infrastructure interdependencies, which underscore the need to develop a comprehensive understanding of how these infrastructures work together. The loss of power to the energy grid implicated more than just our energy infrastructure and cascaded into other infrastructures. For instance, as sewage piled up in Harlem because there was no power to pump it through the facility, a diver had to be sent in through 40 feet of liquid sewage to get the pump working again. GMU, as well as other research universities, have particular technical expertise to

bear in both risk assessment of critical assets and advancing the understanding of infrastructure interdependencies.

Finally, the interconnectivity of modern infrastructures goes beyond the technical systems themselves. The human element of critical infrastructure protection is equally, if not more, important. People must communicate in order to prevent and respond to critical infrastructure failures. This high-level communication process is complex and involves many layers of connectivity. It is perhaps the most vital piece of effective infrastructure protection that we can provide because we cannot anticipate every contingency.

Robust information-sharing must afford sufficient levels of detail at both the executive and the operational levels. As a former first responder and trained incident commander, I believe management of these complex social response networks at all levels of the Federal structure will be increasingly important in the successful resolution of future incidents of national significance relative to our infrastructure.

The CIP project has the primary goal of research with the real-world issues and problems faced by industry and government leaders that face the important—face us at this important time in our history. We thank the committee for its support of academia in this area, and I look forward to your questions.

Mr. THORNBERRY. Thank you, sir.

[The statement of Mr. McCarthy follows:]

PREPARED STATEMENT OF JOHN A. MCCARTHY

Thank you, Mr. Chairman and distinguished members of the Committees for the honor of appearing before you today. I am here to testify about issues and challenges in providing for critical infrastructure protection in the context of the recent blackout and how George Mason University is assisting in this agenda.

As a preliminary matter, I'd like to introduce the Critical Infrastructure Protection (CIP) Project, within the George Mason University School of Law, where I serve as Executive Director. The CIP Project has a unique role in building an inter-disciplinary research program that fully integrates the disciplines of law, policy, and technology. We are developing practical solutions for enhancing the security of cyber networks, physical structures, and economic processes underlying our nation's critical infrastructures. The CIP Project is specifically charged with supporting research that informs needs and requirements outlined in the various National Homeland Security Strategy documents. Since its inception a little over a year ago, we have sponsored more than 70 substantive research projects, touching leading scholars at 20 universities and focusing more than 200 graduate and undergraduate students on security related studies. CIP Project sponsored research ranges from highly technical efforts to design new security protocols for cyber systems, to mapping the vulnerabilities of various infrastructures, to exploring the legal and business governance implications of information sharing, to experimental economic analysis of the energy sector under the direction of Dr. Vernon Smith—the most recent Nobel Laureate in economics. In addition, GMU leads an academic consortium of regional scholars, supporting CIP vulnerability analysis and interdependency identification for homeland security planning efforts here in the National Capital Region. We are working closely with the Department of Homeland Security to ensure vulnerability assessment and modeling tools are developed locally that can be deployed nationally.

The Northeast Blackout provides a clear example of disruption to our vital infrastructures. I will focus my comments today on those issues I believe are key areas of critical infrastructure protection that require continued emphasis. These are:

- The need to develop a comprehensive understanding of infrastructure vulnerabilities and tools to assess these vulnerabilities;
- The need to better understand the complex interdependencies between infrastructure sectors; and
- The need to develop effective systems of public-private partnerships that afford true information sharing.

The Blackout and its consequences serve as an effective yardstick by which to measure critical infrastructure protection development since 9/11. On a positive note, most areas that were affected by the blackout had power restored within 24 hours. Considering the large geographic area, the number of jurisdictions involved, and the international aspects of the Blackout, this was a sound response. Particularly noteworthy were the cross-sector public-private communications that took place away from the eyes of the media. These communications involved industry, state, local and national decision-makers. I believe these relationships were not ad-hoc responses to the Blackout, but the result of the efforts of the past decade in developing a means for enhanced information exchange between the public-private sectors.

First, the Blackout experience highlights our nation's serious problems with infrastructure, including poor comprehension of our vulnerabilities and lack of awareness or preparedness for the interdependencies of infrastructures. The Blackout stresses the need to further identify, map and define our critical assets and properly assess their vulnerabilities—as have 9/11, the first bombing at the World Trade Center, Y2K, and numerous debilitating cyber attacks. Comprehensive infrastructure mapping allows us to assess exactly where vulnerabilities are, what redundancies are needed, and how to recover quickly from a disruption by physical or cyber means. It is important to map out each of the critical infrastructures, how they work with each other, and study the possible effects that the loss of one infrastructure will have on others. This type of network and vulnerability mapping is vital in addressing and managing future infrastructure disruptions. In addition, this will afford the insurance and reinsurance industries the opportunity to gather sufficient information so they can determine their appropriate role in the terrorism risk insurance arena.

These analyses must also include evaluation of myriad possible scenarios that may pose threats to critical systems and provide identification of physical and process actions, as well as economic incentives to industry that afford greater resiliency and security of key infrastructure assets. For example, in the short term, the use of redundant electrical generation at hospitals in New York City resulted in virtually no loss in service delivery capability for emergency responders and health care providers during the Blackout.

Next, the Blackout also highlights infrastructure interdependencies, which underscore the need to develop a comprehensive understanding of how these infrastructures work together. The loss of power to the energy grid implicated more than just our energy infrastructure; it cascaded into several other infrastructures. For instance, sewage piled up at a Harlem treatment plant because there was no power to pump it through the facility. A diver had to be sent in through 40 feet of liquid sewage in order to get the pumps working again. GMU, as well as other research universities, have particular technical expertise to bring to bear in both the risk assessment of our critical assets and the advanced understanding of infrastructure interdependencies. We are fully supporting DHS's efforts to accelerate understanding in these key areas.

Finally, the interconnectivity of modern infrastructures goes beyond the technical systems themselves. The human element of critical infrastructure protection is equally, if not more important. People must communicate in order to prevent and respond to critical infrastructure failures. This high-level communication process is complex and involves many layers of connectivity. It is perhaps the most vital piece of effective infrastructure protection we can provide because we cannot anticipate every contingency. Robust information sharing must afford sufficient levels of detail at both the executive and operational levels. It should candidly identify vulnerabilities, prioritize key infrastructure assets, and allow public and private officials to prevent, respond to, and recover from potential disruptions. By the same token, sufficient safeguards and incentives must be structured for all stakeholders to fully participate in the process. As a former first responder and trained incident commander, I believe management of these complex social response networks at all levels of the federal response structure will be increasingly important in the successful resolution of infrastructure incidences of national significance, be they physical, cyber, or both. The establishment of a public-private liaison as a senior advisor to Secretary Ridge is an important and needed step in developing and advancing this emerging need.

The Committee has chosen to address these issues at the right time, and I commend you in holding this hearing. The CIP Project's primary goal is to match scholarly research with the real-world issues and problems faced by industry and government leaders at this important time in our Nation's history. With your continued support, the academic community can continue to provide unique fora to assist decision-makers in discussing and developing solutions to these pressing issues.

Thank you. I look forward to answering any questions you may have.

Mr. THORNBERRY. Our next witness is Karl Rauscher, founder and president of the Wireless Emergency Response Team. Appreciate you being with us, and you are recognized for 5 minutes.

STATEMENT OF KARL F. RAUSCHER, FOUNDER AND PRESIDENT, WIRELESS EMERGENCY RESPONSE TEAM

Mr. RAUSCHER. Chairman Thornberry, Chairman Camp and other distinguished Members, thank you for the opportunity to speak today and provide a perspective from the communications infrastructure.

My name is Karl Frederick Rauscher. I am the founder and president of the Wireless Emergency Response Team, a nonprofit organization supported by expert volunteers from the private sector and government. The mission of WERT is to provide vital help by using advanced wireless technology to support search and rescue in a national crisis, by conducting focused research, and by providing emergency guidance for 911 centers, law enforcement, and family members. My experience related to today's subject matter includes 18 years of experience at Bell Labs and Bell Communications Research. As the vice chair of the industry's Network Reliability Steering Committee, I oversee deep dive cause analyses for major network outages. These analyses are conducted voluntarily by the industry for the purpose of determining if existing best practices are sufficient to prevent similar future events. The ATIS NRSC publishes an annual report on the health of the Nation's public networks.

As a member of the Telecom-Information Sharing and Analysis Center, I am routinely involved in industry mutual aid responses, including the activities for the recent power blackout. I have led combined government and industry efforts to produce over 500 best practices for network reliability and homeland security. These FCC NRIC best practices are the most comprehensive and authoritative guidance in the world for public communications networks. These best practices, while totally voluntary, are implemented at a high level throughout the industry and are consistently credited for preventing network service disruptions.

My perspectives include very human aspects of this discussion. My experiences have made a lasting impression on the vital need to connect the best minds of the industry with the most vital needs of its subscribers in an emergency.

Wireless communications are vital in disaster response. On the morning of September 11, wireless communications were used by countless Americans in their usual ways. And then evil terrorists emerged to make their dark mark on human history. During those same moments, wireless devices such as cell phones and PDAs were used by brave hostages in the skies to report the hijacking of their planes, and then by expectant victims to speak their last "good-bye" and "I love you", and then by rescue teams as they rushed to bring aid. Instruments routinely used for conducting business and nurturing relationships were then, in their final mission, being used to secure the safety of the United States of America, or bring two individuals together for a final, treasured moment.

In the following hours, an unprecedented wireless industry effort sprang into action to support search and rescue efforts at the World Trade Center disaster site.

WERT's final report documents its key lessons and recommendations. May God forbid that such a tragedy and horror would ever be visited on us again, but if it does, WERT will be ready to bring the best minds and resources of the wireless industry to work hand in hand with traditional first responders on the never-changing top priority after disaster-saving human life.

Most of the characteristics of the recent power blackout were similar to crises already experienced by the communications industry. For example, the duration was similar to power outages caused by large ice storms. Other characteristics, while familiar, were turned up a few notches in intensity. And a third set of characteristics was mostly new; for example, the most notable being that, like September 11, this event was unanticipated. Also there were multiple cyberthreats in play around this time.

Concerning wireless networks, during the first half hour after the power was lost, enormous spikes in the number of call attempts were seen, up to 1,000 percent of normal traffic levels. During the next several hours, traffic hovered around 100 percent above normal levels. Any service problems during the early time frame were likely due to congestion caused from this very unusual demand.

For the most part, the wireless systems and networks were working as designed. When commercial power was lost, cell towers drew power from back-up batteries until power was restored or until the battery power was consumed. The wireless industry will factor new insights gleaned from this historic event into future risk assessments and emergency planning capabilities.

During times of heavy congestion, a text message attempt is more likely to succeed than a voice call because there are lower requirements for bandwidth. It is encouraging that early reports indicate there was a marked increase in the use of "exting" during the blackout.

The national communications system's ISAC is now part of the Department of Homeland Security Information Analysis and Infrastructure Protection Directorate. This ISAC interacted effectively with the Electricity Sector ISAC during the blackout, an immense demonstration for the potential of what could be accomplished in the future with ISAC-to-ISAC coordination.

Another lesson learned during the blackout is that homes should have a corded phone as an emergency back-up. As many learned, cordless phones depend on commercial power.

Concerning government industry partnerships, make no mistake about it, the communications industry is a fiercely competitive battlefield, yet a remnant of something tremendously precious survives. An aspect of the culture of the traditional phone company lives on. It is one that ascribes to itself an obligation to the safety of society. As the head of a nonprofit volunteer organization, this is tremendously encouraging. WERT has captured some of that spirit in harnessing the expertise, will and compassion of so many volunteers along with their companies or agencies. Intergovernmental partnerships are supported by significant volunteer effort and are highly effective.

I hope that my insights today will be useful to the committee. Thank you.

Mr. THORNBERRY. Thank you. I appreciate your testimony.

[The statement of Mr. Rauscher follows:]

PREPARED STATEMENT OF KARL F. RAUSCHER

Chairman Thornberry, Chairman Camp, Congresswoman Lofgren, Congresswoman Sanchez, Congressman Cox, Congressman Turner, and other Distinguished Members: thank you for the opportunity to speak today and provide a perspective from another critical infrastructure—the telecommunications and Internet services industry

Introduction

My name is Karl Frederick Rauscher. I am the Founder and President of the Wireless Emergency Response Team, a non-profit organization supported by expert volunteers from the private sector and numerous government agencies. My experience related to today's subject matter includes . . .

- 18 years of communications industry experience at Bell Communications Research & Lucent Technologies Bell Labs
- I have led numerous highly successful improvement programs in quality and reliability. With a background of advanced concepts in software, systems, architectures and networks, I have invented software testing techniques that have delivered dramatic breakthrough quality improvements. I am a recipient of the Bell Labs President's Award for bringing the first telecommunications network switch to "6 9's" of reliability, which means 99.9999% uptime, or less than 30 seconds of downtime per year (independently verified with pubic data). In my 10 years at Bell Communications Research, I have personally uncovered over 1000 software design errors in programs running on live network systems. I have recently conducted Homeland Security research at an offshore software development outsourcing facility.
- As Vice Chair of the industry's Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC), I oversee the "deep dive" cause analyses that occur for each major network outage. These analyses are conducted voluntarily by the industry for the purpose of determining if existing Best Practices are sufficient to prevent similar, future events. The NRSC also provides an annual report on the health of the nation's public networks.
- As a member of the Telecommunications-Information Sharing and Analysis Center (ISAC), I am routinely involved in industry mutual-aid responses. I was directly involved in the communications industry's coordination and response to the recent Power Blackout—from the initial report assessments through ongoing after-action reviews.
- I have led combined government and industry efforts to produce over 500 Best Practices for network reliability and Homeland Security. The Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) Best Practices are the most comprehensive and authoritative guidance in the world for public communications. Best Practices, while totally voluntary, are implemented at a high level throughout the industry, and are consistently credited with preventing network service disruptions. In addition, I have led industry discussions on blended physical and cyber attacks.
- I am the Chair-Elect of the international IEEE Technical Committee on communications Quality and Reliability. I oversaw Best Practice guidance on ultra-high reliability and ultra-high security for world-class events, which benefited the Olympics, among others.
- I am on the Board of Advisors for the Center for Resilient Networks
- I have participated in the President's National Security Telecommunications Advisory Committee (NSTAC)
- Most importantly, I have access to the right people—those who are world-class experts, who will tell it like it is, and then take the necessary actions.

My perspective includes very human aspects of this discussion. In pressure-heated crises, I have brainstormed with brave first responders and listened to family members—pleading for everything to be done with technologies that they do not understand—to save their loved ones. In moments of heavy telephone silence, I have connected on a personal level with strangers in distant places—this has made a lasting impression on the vital need to connect the best minds of the industry with the most vital needs of its subscribers in an emergency.

Role of Wireless Communications in Disaster Response

On the morning of September 11, *wireless communications* were used by countless Americans in their usual ways.

And then evil terrorists emerged to make their dark mark on human history.

During those same moments, *wireless communications* were used by brave hostages in the skies to report the hijacking of their planes, then by expectant victims to speak their last "GOOD BYE" and "I LOVE YOU", and then by rescue teams as they rushed to bring aid.

Wireless devices, such as cell phones and PDAs, played a vital role on September 11 because they are popular, easy to operate, one of the few items carried everywhere by their users, and can still function when severe damage is done to surrounding infrastructure. Instruments routinely used for conducting business and nurturing relationships were then, in their final mission, being used to secure the safety of the United States of America, or bring two individuals together for a final, treasured moment.

That night, news reports stated that cell phones were being used to call for help from the rubble in New York City. At this point, the vision for a coordinated industry emergency response was conceived. In the following hours and days, an unprecedented wireless communications industry mutual-aid effort sprang into action to support Search and Rescue efforts at the World Trade Center disaster site. The Wireless Emergency Response Team was formed.

Due to the nature of the building collapse, the team was not able to rescue victims from the rubble. However, value was realized in several ways: keeping rescue teams from danger by quickly discrediting false reports, confirming those thought to be missing as safe, and helping to bring closure for family members. WERT's Final Report documents the key lessons-learned and recommendations, so that this capability can be enhanced and optimized. May God forbid that such a tragedy and horror would ever be visited on us again. But if it does, WERT will be ready to bring the best minds and resources of the wireless industry together to work hand-in-hand with traditional first responders on the never changing top priority after a disaster—saving human life.

The August 2003 Power Blackout

Observed Characteristics

Most of the characteristics of the recent Power Blackout were similar to crises already experienced by the communications industry.

1. The duration was similar to very large power outages, for example the result of large ice storms
2. The hot and humid seasonal climate was challenging for electronic equipment
3. There were rolling blackouts and requests for load shedding

Other characteristics, while familiar, were turned up a few notches in intensity and resulted in more pressure on our industry:

4. While ice storms, heavy snowfalls and hurricanes have been widespread, the August Blackout was even more widespread, affecting multiple major U.S. cities.
5. The cause was unknown
6. Many people have cordless phones in their home that could not function
7. Because of the times we are living in, New Yorkers were more jittery, intensifying their need for wireless communications

The third set of characteristics was mostly new, and their study will be the source of new lessons-learned from this event:

8. The most notable being that, like September 11, this was a widespread catastrophic event that was unanticipated (unlike ice and snow storms, or hurricanes)
9. Also, there were multiple cyber threats in play around this time
10. Air and other public transportation was halted
11. There were new levels of pressure on fuel suppliers, who are critical in supporting back-up power generators

Wireless Network Observations

During the first half-hour after the power was lost, enormous spikes in the number of call attempts were seen—up to one thousand percent of normal traffic levels. During the next several hours, traffic hovered around one hundred percent above normal levels. Any service problems during the early timeframe were likely due to congestion caused from this very unusual demand.

For the most part, the wireless systems and networks were working as designed. When commercial power was lost, cell towers drew power from back-up batteries until power was restored or until the battery power was consumed. The wireless in-

dustry will factor new insights gleaned from this historic event into future risk assessments and emergency planning capabilities.

New Areas That Worked Well
Mobile Text Messaging

The WERT Final Report points out that during times of heavy congestion, a text message (e.g., SMS) attempt is more likely to succeed than a voice call because there are lower requirements for bandwidth. Interestingly, mobile text messaging also has consumes less power in both the network and the handset. It is encouraging that early reports indicate that there was marked increase in the use of text messaging during the Power Blackout.

Telecom—ISAC and Electricity Sector ISAC Interactions
Inter-ISAC interaction was effective. This was an immense demonstration for the potential of what could be accomplished with ISAC-to-ISAC coordination.

Other Lessons Learned

- It is better to have one national point of government-industry information sharing through the various sector's ISACs for efficiency and accuracy
- Homes should have a corded phone as an emergency back-up, because the batteries of cordless phones can run out
- Businesses should conduct risk assessment to determine the criticality of back-up power capabilities to their operations

Government—Industry Partnerships

Make no mistake about it: The communications industry is a fiercely competitive battlefield. Yet a remnant of something tremendously precious survives. Through the divestiture of the 1980s and the Telecommunications Act of 1996, a precious aspect of the culture of the traditional telephone company lives on—it is one that ascribes to itself an obligation to the safety of society.

As the head of a non-profit volunteer organization, the spirit that was exhibited by thousands on September 11, and the recent Power Blackout, is tremendously encouraging. WERT has captured some of that spirit in harnessing the expertise, will and compassion of so many volunteers, along with their companies' or agencies' support. Two years ago, for 3 weeks, we knew that, if there were victims in the rubble with cell phones, we may be their only hope. WERT volunteers did everything possible to listen for any signal from a possible survivor. By continuing to fulfill the mission of WERT, the wireless industry shows itself good stewards of its powerful technologies.

The President has called on the people to be volunteers. In addition to soup kitchens and mentoring programs, critical infrastructure technology experts have figured out what they can "do for their country" in these anxious times. There are countless individuals who give of their vacation time, evenings and weekends because of their sense of duty and love for this country. They develop Best Practices and standards, conduct research, provide explanations to government officials and are on call 24 by 7 for the next crisis.

Industry-Government partnerships are supported by significant volunteer effort and are highly effective.

Dependence on Cyber and Wireless Capabilities

There are awesome advantages for a society connected by high-speed mobile communications. More information, in a variety of formats (voice, data, video) will be delivered. Wireless communications and the Internet play increasingly important roles in society, and particularly in emergency response. In the not-to-distant future . . .

- A firefighter may have hands-free constant communication with his team
- His vital signs may be monitored remotely from the safety of a distant command center
- As he carefully walks from room to room, infrared imaging data from the floors and walls may be combined with that of other firefighters to alert those in harm's way to possible danger.

The possibilities are endless, for every aspect of society. On the horizon is a world where cell phones, household appliances and even vehicles are nodes on many interconnected networks.

But with this increased connectedness, come inherent vulnerabilities and risks of an imperfect cyber world. The consequences of a software design error can have far reaching effects throughout society. Previous testimony has articulated numerous concerns related to cyber security vulnerabilities, threats, and proposed solutions. In the context of this testimony, I offer several points.

In addition to strengthening reactionary measures—our cyber threat detection and response capabilities—the appropriate investment needs to be made for longer

term fixes that address the root of all these problems. Those bailing water out of the boat tend to get a lot of attention because they can show results. We need the patience and resolve to plug the holes and/or build other boats. What are often referred to as "vulnerabilities" in the cyber community are usually the manifestation of a software design error. The kind of thinking that reserves the term "vulnerability" for those characteristics that are truly intrinsic weaknesses of the programming language and operational environments will provide a better grasp of how to get control of this situation. Following on this, I expect that those bold enough to develop new, robust paradigms for programming and those applying classical quality control principles will make major contributions in this area.

Conclusion

The next time you click your "SEND" button to send an email, I ask you to consider the previous effort of the message-bearing marathon runner of ancient Greece. We are now living what has only been dreamed of for centuries before us—and we are just about there—being able to communicate in any fashion, at any time, at any place.

May it be that when a generation from now looks back on how we faced these cyber and physical challenges, that the scientists and engineers were found to be unimaginably innovative; may our leaders be found to have been enablers of life, liberty and the pursuit of happiness; and may the horrors of terrorism and cyberhackers . . . be only distant memories.

I hope that my insights offered today on the recent power blackout, government-industry partnerships, and dependencies on wireless and cyber infrastructure will be useful to the committee.

Mr. THORNBERRY. Finally, we have Mr. Kenneth C. Watson, president and chair of the Partnership for Critical Infrastructure Security. Thank you for being here. Mr. Watson, you are recognized for 5 minutes.

STATEMENT OF KENNETH C. WATSON, PRESIDENT AND CHAIR, PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY

Mr. WATSON. Thank you very much, Mr. Chairman and distinguished Members. I appreciate the opportunity to testify today regarding the interdependence of critical infrastructures.

I am president and chairman of the Partnership for Critical Infrastructure Security, the PCIS, launched in December of 1999 as one of the industry responses to the Federal Government's call for public-private partnerships in critical infrastructure protection. The PCIS is the forum for cross-sector, public-private dialogue on reducing vulnerabilities, mitigating risks, identifying strategic objectives, and sharing sound information security practices. Currently the PCIS is working on an interdependency risk assessment handbook, and the board meets monthly by teleconference to discuss cross-sector critical infrastructure protection issues.

In 1998, the Federal Government recommended the appointment of industry sector coordinators in each critical industry to coordinate critical infrastructure protection efforts across each sector and with appropriate Federal lead agencies. The PCIS board of directors is structured so that the sector coordinators always comprise its majority.

Mr. WATSON. Across industry and government the role of the sector coordinator is growing in importance and needs to be better understood. The Department of Homeland Security is developing a best practices guideline for sector coordinators and working with lead agencies and industry leaders to organize the new sectors and identify appropriate coordinators.

Initial interdependency research has only been sufficient to illuminate the importance of modeling analysis and exercises. Sandia and other national labs have studies of various sector intersections with energy.

The National Security Telecommunications Advisory Committee, or NSTAC, has done similar work addressing intersections with telecommunications. The National Infrastructure Advisory Council, or NIAC, has a current effort to develop policy recommendations on interdependency risk assessments, and at the invitation of the NIAC working group, the sector coordinators are involved in that study which will become available after delivery to the President. The PCIS is coordinating with this working group so that the handbook we develop aligns with NIAC policy recommendations.

Cross-sector vulnerability assessments must be built on high fidelity models of each sector. Each sector model must describe how the network elements work, their capacities, and how and where they connect to each other. Network owners already know their key assets and critical nodes. What they don't know is whether they are in the same geographic vicinity as those of their competitors or whether underlying infrastructure is truly diverse.

Models must use up-to-date industry data, and infrastructure owners and operators must be the primary beneficiaries of results. A comprehensive infrastructure modeling project will require additional government funding, and the sectors are prepared to work with DHS to develop the best approach for each sector. Capabilities from various national labs and Federal departments will be needed to develop a model that can be built once, routinely refreshed by industry, and used by many to analyze vulnerabilities and develop mitigating strategies. Without higher funding levels, this may take a decade to accomplish and only marginally benefit the sectors.

DHS has begun to sponsor regional exercises to identify vulnerabilities, dependencies, and cross-sector points of contact to develop contingency plans to respond to physical and cyber attacks. TOPOFF and TOPOFF II represented small steps toward addressing physical threats, but these included little private sector input or expertise. Livewire is an upcoming cyber exercise that will have some private-sector input.

Feedback from the sectors to date is that these small-scale exercises do not benefit critical infrastructure owners and operators who have the responsibility of acting first during a crisis. To be effective, they must include private-sector experts to help build the exercises' design scenarios and participate as key stakeholders.

The PCIS and sector coordinators would be happy to work with DHS and other government stakeholders to plan and execute such a series of interdependency exercises.

I have three recommendations for Department of Homeland Security:

First, coordinate with lead agencies and industry leaders to rapidly organize the newly named sectors, named by the national strategy for homeland security; identify appropriate sector coordinators and clarify sector coordinator roles; and actively promote the sector coordinator function to key industry and government executives.

Second, improve coordination among all appropriate national labs and Federal departments to apply computer models and simulations to critical infrastructure mission areas; ensure that sector coordinators and their constituents are involved in establishing modeling objectives, peer reviews of model creation, data mining and results; and ensure the protection of this very sensitive data.

Third, sponsor comprehensive regional and national exercises that cover the physical and cyber aspects of attacks on critical infrastructures as well as dependencies; ensure that sector coordinators and their constituents are involved in the exercise design, scenario creation, participation, and are the primary recipients of exercise lessons learned.

DHS leadership has been very inclusive of industry as they organize to protect critical infrastructures. The department cannot be expected to protect critical infrastructures alone. Industry must be part of its organizational culture as our Nation's approaches to homeland security mature. The industry leaders I work with are willing to do their part to protect our national and economic security.

Thank you for the time. I would be happy to answer any questions.

[The statement of Mr. Watson follows:]

PREPARED STATEMENT OF KENNETH C. WATSON

Chairman Thornberry, Chairman Camp, Congresswoman Lofgren, Congresswoman Sanchez, Congressman Cox, Congressman Turner, and other Distinguished Members: thank you for the opportunity to testify today regarding the interdependence of our critical infrastructures. The nearly universal dependence on privately owned and operated infrastructures, their dependence on computer networks, and their interdependence on each other, were the primary drivers prompting the creation of the President's Commission on Critical Infrastructure Protection (PCCIP, "The Marsh Commission"), which reported its findings in October 1997. We have made a lot of progress in the six years since the Marsh Commission published its report, but there is still much to be done. The attacks of September 11, 2001, the northeast blackout of August 14, 2003, and the rapid sequence of Internet worms seen in the last three weeks highlight the need to maintain a sense of urgency as we continue to address these issues.

My background. I am President and Chairman of the Partnership for Critical Infrastructure Security (PCIS), launched in December 1999 as industry's response to the Federal government's call for public-private partnerships following the publication of the Marsh Commission report and the subsequent issuance of Presidential Decision Directive 63 (PDD–63) in May 1998. I also manage Cisco Systems' involvement in critical infrastructure assurance activities. In 1997 I retired from the US Marine Corps after 23 years of service, the last eight of which were devoted to what is now known as Information Warfare or Information Operations. My last tour of duty in the Marines was as Marine Liaison Officer to the Air Force Information Warfare Center in San Antonio, Texas, where we advanced the art of defending against attacks against information and information systems. The thought processes behind the defensive planning, modeling, and exercises we conducted ten years ago apply directly to the problem of critical infrastructure protection today.

PCIS. Following the Marsh Commission recommendations, in 1998 the Federal government established several organizations and positions to coordinate critical infrastructure protection efforts, and recommended the creation of "sector coordinators" in each critical industry sector to coordinate across each industry and with appropriate Federal lead agencies. Working with industry leaders, lead agencies initially appointed eight individuals, most from industry trade associations, as sector coordinators. Some sectors have more than one coordinator because of their size and complexity.

The PCIS is the forum for cross-sector and public-private dialog on reducing vulnerabilities, mitigating risks, identifying strategic objectives, and sharing sound information security practices. It is a public-private partnership that is also a non-

profit organization run by companies and private-sector associations representing each of the critical infrastructure industries. When we created the PCIS, we structured the Board of Directors so that the sector coordinators would always be its majority. The number of Directors is flexible, anticipating the creation of additional sectors and naming of new sector coordinators. There are currently twelve sector coordinators, representing five of the thirteen sectors outlined in the National Strategy for Homeland Security. Ten of these are on the PCIS board. The current list, including the Federal lead agencies and representatives, is attached. The mission of the PCIS is to coordinate cross-sector initiatives and complement public-private efforts to promote the reliable provision of critical infrastructure services in the face of emerging risks to economic and national security.

In the four years since its creation, the PCIS has accomplished a great deal. A PCIS public-policy white paper on barriers to information sharing got the attention of Congressmen Davis and Moran, who co-sponsored the first bill to provide a narrowly written exemption to the Freedom of Information Act (FOIA) for critical infrastructure information. Senators Bennett and Kyl followed with a similar bill, and after conference committee work, the provision is now part of the law that created the Department of Homeland Security (DHS). PCIS also coordinated industry input to the National Strategy to Secure Cyberspace, offering each of the sectors' strategies and an overview document comparing commonalities and differences on the PCIS web site. The PCIS developed an information sharing taxonomy, including the terms commonly used by all industry Information Sharing and Analysis Centers (ISACs) and government agencies that share cyber vulnerability, threat, and solution information. Currently, the PCIS is working on an interdependency risk assessment handbook, and the board, including the sector coordinators, meets monthly by teleconference to discuss cross-sector critical infrastructure protection issues.

Interdependence Examples. We all depend on telecommunications—in fact, when recently asked to list their dependence on other sectors, the sector coordinators rated telecommunications as first or second on their list. Nearly equal to telecommunications was electric power. Without electricity, there is no "e" in e-commerce. However, without railroads to deliver coal, the nation loses 60 percent of the fuel used to generate electricity. Without diesel, the railroads will stop running. Without water, there is no firefighting, drinking water, or cracking towers to refine petroleum. Without financial services, transactions enabling all these commodity services cannot be cleared. Yet, these are not just one-way dependencies. When the railroads stopped running after 9/11 to guard hazardous material, it only took the city of Los Angeles two days to demand chlorine or face the threat of no drinking water—the railroads began operating again on the third day. Throughout the Northeast, dependencies on electric power were obvious. Some areas had electric water pumps, and they had to boil their drinking water for days after the blackout.

Gaps and barriers

Sector Coordinator Roles Poorly Understood. The role of the sector coordinator is not well understood, either in industry or government. DHS is developing a "best practices" guideline for sector coordinators, and working with sector agencies and industry leaders to organize new sectors from which candidates for the job will emerge. In many critical infrastructure industries, CEOs and other executives are not aware of the role of sector coordinator, do not know who their coordinator is, and use other means to coordinate their critical infrastructure assurance actions. Industry sectors are neither homogeneous nor hierarchical, but in the rapid-paced, complex world of critical infrastructure assurance, single "belly-buttons" are absolutely needed to coordinate actions within and across critical sectors.

Interdependence vulnerability research inadequate, incomplete, and underfunded. All of our critical infrastructures are interlinked in complex, sometimes little-understood ways. Some dependencies are surprising, contributing to unusual key asset lists. Studies, modeling, and exercises represent the three primary interdependence research methods.

Studies. Some rudimentary research has been done on interdependencies, but it has only been sufficient to illuminate how important this type of modeling and analysis could be. Sandia and other national labs have initiated interdependency studies, looking at intersections with the energy sector. The National Security Telecommunications Advisory Committee (NSTAC) has done similar work, addressing intersections between telecommunications and other sectors. The National Infrastructure Advisory Council (NIAC) has a current effort to develop policy recommendations on interdependency risk assessments. The sector coordinators are involved in that study, which will become available after delivery to the President in the October timeframe. The PCIS is coordinating with this NIAC working group to

ensure that the handbook we develop is in harmony with NIAC policy recommendations.

In the FY2004 Budget submitted to Congress, approximately $500 million has been requested to assess the security of the nation's critical infrastructure. Of this, $200 million is allocated to develop and maintain a primary mapping database, and $300 million has been allocated to work with states and industry to identify and prioritize protective measures to mitigate any risks identified through the ($200M) database consequence-mapping activity. We expect this level of funding to grow at a rate of about 2% per year over the next five years.

While this seems like a lot of money, there is concern that the complexity associated with this type of analysis is not readily recognized. Conducting cross-sector vulnerability assessments presumes that each of the individual sectors has already been modeled. This is not the case. Each sector will need to be modeled to some degree of fidelity before any cross-sector studies can be accomplished. These individual sector models must incorporate how the network elements work, their capacities, how they connect to each other, and where they connect to each other. It is not sufficient to simply ask the sectors' major infrastructure owners for a list of their key assets and critical nodes, so that they can be "mapped." Mapping an asset without modeling how it works or how it connects to or impacts the next element in the network is an exercise without merit. The network owners already know their key assets and critical nodes—what they don't know is whether their key assets and critical nodes are in the same geographic vicinity as their competitors' nodes, or whether underlying or supporting infrastructure is in fact, truly diverse. In highly competitive sectors, such as telecommunications or finance, it would not be unusual to find that each of the major providers has intended to buy diversity and redundancy from numerous entities, only to find that all these entities use the same underground conduit for transport that goes through the same underground tunnel, and they are powered by the same power generation plant. The NSTAC has studied the implications of these types of cross-sector dependencies and has developed a number of programs that the telecommunications sector uses to mitigate these risks. It is time, however to take it to the next level, covering all cross-sector and multi-sector interdependencies.

Modeling. Existing computer modeling and simulation has not been effectively utilized for critical infrastructure protection purposes. DoD operates high-fidelity models to support military missions. DoD is not funded for homeland security, and its modeling capability is probably fully utilized for the purposes for which it was designed. However, DHS could take advantage of DoD model designs and algorithms, applying critical infrastructure data and missions. DoE national labs use sophisticated models to help with energy planning, and they have developed the National Infrastructure Simulation and Analysis Center (NISAC), which is now part of DHS. NISAC capability is still being developed by DHS. Modeling can help develop plans, and it can save some of the expense and time required for regional exercises, but (a) the data used must be up-to-date industry data; and (b) sector coordinators (and the infrastructure owners they represent) must be the primary beneficiaries of modeling results—after all, the sector coordinators are responsible for developing and executing plans to protect critical infrastructures. One of the challenges will be that much of the data required may be proprietary.

To date, the NISAC has centered its modeling efforts on the energy sector. To understand the complexity of this modeling problem, consider the NISAC model of the energy sector as a baseline, and apply it as a level of magnitude to the telecommunications sector. While we do not know the precise amounts, it is our understanding that the current electrical sector modeling cost about $30–40 million to develop and was done over the course of 3 to 8 years. If you assume that the level of detail developed within the electrical sector model is appropriate (and we do not know that to be the case) and simply multiply this $30–40 million times the number of facilities-based networks that comprise the telecommunications sector, then you would conservatively multiply this estimate by a factor of 9 networks (5 wireless + 1 wireline + 2 IXC + 1 paging), resulting in a baseline model for telecommunications in the $270–$360 million range. Even if all $200 million was dedicated to telecommunications modeling, it would take 1 to 2 years of currently allocated funding, and an even longer actual modeling effort, to model telecommunications alone. Multiply that by 12 sectors, and then you can start on the cross-sector interdependency modeling.

The sectors, particularly the telecommunications sector coordinators, have initiated conversations with the national labs to determine how this important work could be undertaken, and what level of support the national labs would need to marry their modeling, testing and data mining expertise with industry knowledge regarding how the various networks work and how they interrelate to each other

within the sector. This project will require government funding, and the sectors are prepared to work with DHS to develop the most appropriate approach for each sector. It is our sense that various capabilities from numerous national labs (DoE, DoD, etc) will be needed to develop a model that can be built once, routinely refreshed by industry and used by many, in the analysis of vulnerabilities and the development of mitigating strategies. It is also our sense that in the absence of higher funding levels, this statutory requirement may take a decade to accomplish and any benefits to the sectors watered down significantly. This information has not been communicated fully to DHS–the department is still undermanned in this area. This is not an accusation or complaint, but simply a reflection of start-up reality. The sectors are prepared to work closely with DHS once it is ready.

Exercises. DHS has begun to sponsor regional exercises to identify vulnerabilities, dependencies, and cross-sector points of contact for the purpose of developing contingency plans to respond to physical and/or cyber attacks. This effort must be accelerated and expanded to cover every region of the country. Lessons learned must be shared with the sector coordinators so that all the critical industries on the front lines of defense can understand what they need to do and with whom to coordinate.

"TOPOFF" and "TOPOFF II" represented small steps toward addressing physical threats, but these were exercises with little private-sector input or expertise, and certainly no funding for the insertion of this expertise into these exercises. "Livewire" is an upcoming cyber exercise that will have some private-sector input. Feedback from the sectors to date is that these small-scale exercises serve primarily to educate government consultants and do not benefit critical infrastructure owners and operators, who have the responsibility of acting first during a crisis. Regional exercises are a must for the physical dimension, and sometimes cyber exercises will be national in scope. To be effective, they must include private-sector experts to help build the exercises, design scenarios, and participate as key stakeholders. Funding must support private-sector participants' time as it currently does that of the government consultants. More importantly, their design should encourage private sector involvement by telling them things they need to know (e.g., business continuity planning). These exercises must include both the cyber and physical dimensions of critical infrastructure planning, and must involve all the critical infrastructure sectors to ensure a complete understanding of interdependency. The PCIS and the sector coordinators would be happy to work with DHS and other government stakeholders to plan and execute such a series of interdependency exercises.

Recommendations for DHS

Coordinate with lead agencies and industry leaders to rapidly organize the newly named sectors, identify appropriate sector coordinators, and clarify sector coordinator roles. Actively promote the sector coordinator function to key industry and government executives, and within the federal government.

Coordinate with all appropriate National Labs to apply appropriate computer models and simulations to critical infrastructure mission areas. Ensure that sector coordinators and their constituents are involved in model creation, data mining, and results. Assure the protection of sensitive data.

Sponsor a comprehensive set of regional and national exercises that cover the physical and cyber aspects of attacks on critical infrastructures, as well as dependencies. Assure the protection of sensitive data, and ensure that sector coordinators and their constituents are involved in exercise design, scenario creation, participation, and are the primary recipients of exercise lessons learned and other information they need to defend their part of the critical infrastructures.

Conclusion. DHS leadership has been very inclusive of industry as they organize to protect critical infrastructures. Everyone in government must understand that in this area, public-private partnership is not just for appearances?it is absolutely essential. Since critical infrastructure owners and operators are on the front lines, the sector coordinators must be part of all critical infrastructure planning, strategy development, exercises, remediation, and responses to threats and attacks. DHS cannot be expected to protect critical infrastructures alone—industry must become part of its organizational culture as it matures. National and economic security are forever intertwined. The industry leaders I work with understand and embrace their role as front-line defenders, and are willing to do their part to protect our national and economic security.

Appendix A: Critical Sector Points of Contact: 4–14–03

#	Sector & Sub Sectors	Lead Agency	Sector Liaison	Sector Representative	Sector Coordinator	
	(as found in the HS Strategy)	(as found in the HS Strategy)		Government	Organization	Name
1	**Agriculture**	Department of Agriculture	Jeremy Stump (USDA)	James Smith (USDA)		
2	**Food**					
	Meat & poultry	Department of Agriculture	Jeremy Stump (USDA)	James Smith (USDA)		
	All other	Department of Health & Human Services	Stuart Simmonson (HHS)			
3	**Water**	Environmental Protection Agency	Mary Kruger (EPA)		**AMWA**	Diane VanDe Hei
			Janet Pawlukiewicz (EPA)	Cayce Parrish (EPA)		
4	**Public Health**	Department of Health & Human Services	William Raub (HHS)	Roberta Lavin (HHS)		
5	**Emergency Services**	Department of Homeland Security	DHS			
			DHS		**NYSP**	Dave Christler
6	**Government**					
	Continuity of government	Department of Homeland Security	DHS			
	Continuity of operations	All departments and agencies				
7	**Defense Industrial Base**	Department of Defense	Glenn Price (DoD) (Acting POC)			
8	**Information & Telecommunications**	Department of Homeland Security	Nancy Wong (DHS)	Kathleen Kenyon (DHS)	**ITAA**	Harris Miller

Appendix A: Critical Sector Points of Contact: 4–14–03—Continued

#	Sector & Sub Sectors	Lead Agency	Sector Liaison	Sector Representative	Sector Coordinator	
	(as found in the HS Strategy)	(as found in the HS Strategy)		Government	Organization	Name
					TIA	Matthew Flanigan
					USTA	Daniel Pyhthyon
					CTIA	Kathryn Condello
9	**Energy**	Department of Energy	Patrick Burns (DHS)		**NERC**	Mike Gent
					ConocoPhlllips	Bobby Gillham
10	**Transportation**	Department of Homeland Security	DHS/TSA		**AAR**	Ed Hamberger
					ACI–NA	David Plavin
					APTA	Bill Millar
11	**Banking and Finance**	Department of the Treasury	Michael Dawson (Treasury) Brian Tishuk (Treasury)	Eric Robbins,	**BOA**	Rhonda Maclean
12	**Chemical Industry &** Hazardous Materials		EPA	Mary Kruger (EPA)		
			Tom Dunne (EPA)	Craig Matthiessen (EPA)		
13	**Postal & Shipping**	Department of Homeland Security	Pat Mendonca (USPS)			
14	**National Monuments & Icons**	Department of the Interior	Steven Calvery (DOI)			

Mr. THORNBERRY. Thank you. I appreciate your testimony.

Again, I appreciate the testimony of all the witnesses. I think we have heard each of you provide interesting and helpful perspectives, coming from different places, on the challenges that we face.

Let me first turn to Chairman Camp for any questions he would like to ask.

Mr. CAMP. Well, thank you. And I agree with Chairman Thornberry; I appreciate your testimony today. It is very helpful. I just have a few questions.

Mr. Watson, what do you really think is the weak link in terms of our electrical and other security?

Mr. WATSON. Mr. Chairman, I am not sure you can point to a single weak link. Over the last 20 years, all of the infrastructures have become more and more dependent on networks, and they have become more and more interconnected. I think the key that we need to study in research and modeling and exercises is interdependency. Each of the sectors is dependent on each of the others and sometimes we don't even know what these dependencies are without modeling and exercises.

Mr. CAMP. I realize the information may not all be available, but in your opinion, the August 2003 blackout, was that primarily a cyber problem or a human error problem?

Mr. WATSON. From what—and I am not an expert on that, and I haven't seen any firsthand information that they are using to conduct the investigation, but what I have seen in the press and what I have heard from experts is that it was not cyber related; that it was an unintentional fault that cascaded.

Mr. CAMP. What do you think the Federal Government should do or what mechanisms might the Federal Government employ to assist in preparing for a recovery from an outage of that kind?

Mr. WATSON. To assist preparing for a recovery, there are a range of things from prevention to response. But the first thing I think the Federal Government can do is provide guidance on priorities. Just as the President provided guidance that the financial market should be up and running within a week of the terrorist attacks of September 11, that kind of guidance and motivation would be appropriate in a large-scale attack or outage if that—if we needed that kind of guidance.

Mr. CAMP. It seemed as though there was a chain reaction shutdown in August, and what sort of safeguards can we put in place to prevent that, a more segmented system or what is your thought there?

Mr. WATSON. I don't have the technical expertise in the electric power sector. I would recommend talking to the North American Electric Liability Council or the Department of Energy, who both have more details on that.

Mr. CAMP. Would any other witnesses care to comment on that question?

Yes, Mr. Gilbert.

Mr. GILBERT. As far as the recent loss on the 14th, it is a failure of a system that is being too heavily used, that hasn't got the ability to deal with normal fluctuations within its operation, and so it caps out and has to shut off. And the question is how to contain

that event in as small a zone as possible, how to "island" the problem.

The industry has been working on better switches and better control mechanisms in order to be able to do that and clearly not all of the different properties within the grids have implemented such changes as yet.

I think we saw an excellent example in Pennsylvania and New Jersey, where the system was robust. They did have a good set of switching and controls and cyber, and they stopped the surge coming towards DC in Pennsylvania. So that is an illustration of the kind of configuration that might be looked upon as a model of what other systems might go towards.

But I think the discussion also brought here on motivation is very important, because the reason that these other systems haven't instituted the kinds of improvements is in part motivational and in part simple economics. The amount of return on investment that is available is insufficient to make the investment to improve the systems. That can be corrected.

Mr. CAMP. Thank you.

Mr. Rauscher, I wondered if you could just for a minute talk about our telephone and Internet, wireless and the wire line systems and how susceptible you think they are to cyber attack; and do you think that is more than other sectors? And what efforts might be made to prevent that, or have they already been made?

Mr. RAUSCHER. It is difficult for me to make a comparison to other infrastructures. I would say that we take very seriously in our industry the possibilities of planned attacks, whether physical or cyber. In fact, the FCC's Network Reliability Interoperability Council has been focused for nearly 2 years now, since September 11, on developing best practices in a very aggressive time frame. There is both a focus on cyber prevention and restoration best practices, and physical prevention and restoration best practices. In addition, there are blended attack discussions. I am involved in leading some of those.

So looking at a combination of cyber and blended attacks, the thing that gives me the most assurance is the additional rigor that we are now taking. These best practices I have been referring to have been around for about 10 years, and they have been developed largely from historic analogy. So whenever we would see a major outage, we would do a deep-dive analysis and determine what would prevent this, what more could be done. And pretty much whenever there is a major outage, we know there was a best practice that existed that for some reason wasn't implemented.

Going forward, instead of just looking at the historic analogy, we are saying, independent of any threat knowledge, systematically, "what are all the vulnerabilities?" and "what are all the different ingredients that make up the communications infrastructure?" And then we have systematically addressed those vulnerabilities with best practices. And this is something new that is provided much additional rigor and you can find more information out about that from the [NRIC and NRSC] reports.

Mr. CAMP. Okay. Thank you. My time has expired. Thank you very much.

Mr. THORNBERRY. I thank the gentleman. The gentlelady from California, the ranking member of the Border Subcommittee.

Ms. SANCHEZ. Thank you, Mr. Chairman. My questions are going to be directed, I think, to Mr. McCarthy and maybe Mr. Watson and maybe Mr. Orszag. I am glad all of you gentlemen are before us today, and I know you have a deadline, so I was interested, Mr.—Dr. Orszag on the whole issue of there not being enough incentive for private industry to ensure that it works through the whole issue of security.

You know, if you own something quite large, whatever type of infrastructure it is, most of the time you can't build it if you don't have some type of insurance on it. You can't continue to operate it even if you are self-insured. Most States have some type of regulation with respect to some type of fund set up and set aside and reserves for that.

Why do you think that is not sufficient, really, to encourage people to protect their own assets if that is the way they are making their money?

Mr. ORSZAG. Let me give you an example that I think is particularly timely, involving chemical facilities.

Let's say that you have a chemical facility. It is worth a billion dollars. It houses chemicals. There are 123 chemical facilities in the United States that contain chemicals that could injure or kill more than a million people. The value of a million lives can easily exceed, well exceed a billion dollars.

You may well have some incentive to make sure that there is some level of security to ensure that your plant is not intruded upon and those chemicals are not dispersed and harm people. But it is not adequate because your financial loss is much smaller than society's loss that would occur if a successful attack did unfortunately take place.

And that kind of example occurs, you know, in a wide array of settings. And I—in my written testimony I provide lots of other types of examples, but I think that might be a particularly timely and compelling one, where any time that private financial losses that you suffer are vastly smaller than the losses that we as a society would suffer, you don't have enough incentive, bottom line.

Ms. SANCHEZ. So even if I am operating and I have liability insurance, you think that a carrier of liability insurance wouldn't take a look at the worst-case scenario of, you know, hundreds of thousands of lives, given the type of chemicals that I control in my facility.

Mr. ORSZAG. In some cases they will, but I think it is—I don't know if "naive" is the word, but "too optimistic" to think that without a push that this will automatically happen. So, for example, when you argue that insurance firms may be providing that kind of incentive already, a requirement that you have insurance would just back that up.

You know, to the extent that insurance firms are already doing this, a requirement that they do so doesn't add any extra burden. To the extent that insurance firms are not doing this, and I would add in the context of smaller chemical facilities that they may not be, I think that the danger is these. Then a requirement will push them up to the appropriate level of activity.

So in some cases, clearly, insurance firms are already playing the role that I, for example, would envision that they play under the sort of mixed system that I laid out. In other cases, they are not. The important point is that they should be in all the cases in which there would be catastrophic losses from a terrorist attack.

Ms. SANCHEZ. Okay. Thank you.

Mr. McCarthy, I think you have a student that was recently in the news with respect to using some public information to map out every business and industrial sector in the American economy and layering on top of it the fiber-optic system that exists throughout the United States. And I think it was pretty much on target. Of course, he ran into some problems with that I think because it was considered a danger to national security.

I have been pushing and a lot of us on this committee have been pushing the Department of Homeland Security to, in fact, come up with a vulnerability list or risk assessment with respect to infrastructure that we have out there, not only in the public sector, but also in the private sector. And I think it is fair to say that it has been a difficult process to even get information about what kind of criteria, et cetera, they are using.

What would you—what would be your guideline? Do you think that it is possible to do that, in particular with respect to private industry and what infrastructure we have out there? And how long do you think that type of a vulnerability risk analysis would take for someone to do, given that you had a graduate student who was able to do it with respect to fiber-optic in a not-too-short time frame?

Mr. MCCARTHY. Well, first of all, that student is one of our best and brightest and we are very proud of his work and stand behind it.

The particular study that you refer to actually has garnered a tremendous amount of interest from every element, ranging from our Defense and Intelligence Communities, to the homeland security and civilian agency community, to the private sector, which tells me that there is an information vacuum, that people saw what this student was doing; and we have been deluged with questions regarding his work and the work of the type that was behind it.

With respect to the time frame, let me give you a little perspective on that student, using it as the case model. This student's graduate work is in the area of mapping and geospatial visualization, which Ken Watson referred to in his testimony as a critical area, and I fully support that. The supervisor of his research, the Ph.D., her work is in the area of transportation networking. And what they have done is combined two disciplines to begin to look at a completely different sector or infrastructure. In this case, it was fiber-optic, being the fiber-optic network overlayed with the telecommunications network, overlayed with the banking and finance network.

Now, the issue of the data in open source, that was one of the most sensitive elements of the research, tells us a couple of stories. Number one, that data took 4 years to compile and refine. So it wasn't just gathering the data; it was taking the data and refining it and working it through a series of tools and algorithms to come

up with a different element of information out of the data to look at it from a different perspective.

Ms. SANCHEZ. But that was not asking people for information in the form that your graduate student needed it. That was going out and trying to find the information, trying to figure out what type of form do I need it in and what am I going to do to get it into a place where it is equal to all the rest of data I have, correct?

Mr. MCCARTHY. Right. That was going out into the Ethernet, out into the Internet, out into the public domain and bringing the information in and gathering it, which is another public policy lesson out of the research. It is out there and it is happening.

We have a very smart guy and a very smart supervisor, Ph.D., who are loyal, dedicated Americans doing good work, working in a reputable university on reputable research. That research is relative to the discussion and agenda we are talking about today.

I am equally convinced that there are very smart, equally dedicated people who are looking at our infrastructures, who don't have our best interest in mind, who are doing similar types of research; and I think that is a significant emerging area that we have got to focus on fast.

There is a balance. This whole issue transitions into the information-sharing area, which is another broad concern of the—both these committees. You know, how do we make this balance between the government's information that they hold and retain, that is useful to the industry for vulnerability assessment, the data that exists within the industry itself about itself, and the reams of data that exist out in our academia community which heretofore has been significantly ignored, in my opinion, as part of the partnership.

This research is evidence of that. I have gotten dozens of phone calls across some significant universities, calling very quietly, You know, look, John, we would just like to have a quiet conversation off line. How do you deal with this, internal to the university?

You know, how are you maintaining a program where you have to get a Ph.D. candidate published so that they can get their Ph.D. and you have to get a young professor on a tenure track tenured? That happens with publication. The government's instinct is to collect the information and classify it. The industry's instinct is, it is proprietary, it is going to give away a trade secret. The academic's instinct is to want to publish it.

How do you balance that? That is a key issue.

Ms. SANCHEZ. Mr. McCarthy, I agree with that and I would like to go over to Mr. Watson, because, you know, one of the biggest problems we have is that, of course, private business doesn't want to be regulated, Doctor; as you know, it is a difficulty.

But more importantly, if 80 percent of our critical infrastructure is in private hands, Mr. Watson, how do we—the biggest concern that we have heard out of private industry is, well, if we give you the information or we collaborate with you, and then there is a set of plans somewhere of everything and—everything that is going on, then we are afraid that just makes another level of information available for cyber attack or ability for the terrorist to get—in other words, the more information there is out there about what we actually have, which is what we are trying to protect from a proprietary

standpoint or just from a security standpoint, all of a sudden the government also has it and we don't really trust you guys to be able to really keep this under lock and key.

What's your answer representing those types of companies that are worried about this?

Mr. WATSON. That is a good question. And leaks occur everywhere, not just in the government; but they do occur from government and they do occur from industry on occasion.

You know, if you have a secret and you tell it to someone, it is no longer a secret. The problem that industry wants to avoid is giving information that the bad guys can use before the good guys have a chance to do something about it.

We are very heartened by the narrowly written exemption to the Freedom of Information Act that is in the Department of Homeland Security law, that provides for industry, their voluntary sharing of information on cyber, critical infrastructure threats, vulnerabilities and countermeasures with the DHS and have that information protected. That is something that has been needed for some time, and we are glad that it is there.

As far as its usefulness, we will have to see how it is used in the future and go from there. The provision is there, and I think that we are going to see opportunities to share information. We have already seen some sensitive information shared across public and private sectors.

The ISACs have been brought up earlier today, the information-sharing analysis centers. There are some 15 ISACs, if you count them one way, maybe 10 ISACs if you count another way, that have stood up to support each of the vertical industries.

After the blackout, the telecommunications ISAC asked for some updates from the electricity sector ISAC, and they got updates every 2 yours. And the ES ISAC and the telecom ISAC were on the phone together, which was an extraordinary amount of collaboration between those two sectors.

The ES ISAC also collaborated with the IT ISAC to discuss cyber threats and vulnerabilities and understand that.

There is an informal ISAC council that has formed that has the leadership of the 10 largest ISACs to share information; and then I understand the telecom—well, the telecom ISAC and the ES ISAC are also sharing information with the government. The ES ISAC has reporting responsibility with the FBI, and the telecom ISAC is housed within the Department of Homeland Security's NCS function.

So information sharing is getting better. We are overcoming the trust barriers and those trust circles are widening.

Ms. SANCHEZ. Mr. Chairman, I think you probably forgot to turn on the—

Mr. THORNBERRY. I turned it off for the gentlelady because she was asking such good questions.

Ms. SANCHEZ. Well, thank you, Mr. Chairman. I appreciate that.

I have a lot of other questions. I think I will submit them for the record, because I think this has been an incredibly good panel and I do have a lot of concerns about whether the Department of Homeland Security is really doing what we need it to do in order for me to feel safer as an American.

But considering that I have other colleagues who have waited a while, thank you, Mr. Chairman for your indulgence. And thank you, gentlemen.

Mr. THORNBERRY. I thank the gentlelady.

The gentleman from Texas.

Mr. TURNER. Thank you, Mr. Chairman.

First, I want to compliment Mr. Rauscher's son, who I think is about two rows back, who has been back there listening carefully today and taking a few pictures. I think he has got a great future.

Mr. RAUSCHER. Thank you.

Mr. TURNER. We were talking about the work of one of your graduate students, Mr. McCarthy, and I read the article in the Washington Post. It is dated July 8. It describes the shock that government officials, as well as some folks in the private sector had when they saw the results of his work. And I gather all of this was produced with publicly available information.

Obviously, it could be very useful to terrorists; and as you said, you have a feeling that there are those out there who may be collecting that same information to do us harm rather than to do us good.

What is the answer to this? What should we be doing? Is this information that rightfully should be protected? Or is it already in the public domain and it is going to stay there, and it is just the way things are?

Mr. MCCARTHY. Well, sir, I think yes and no. The information is out in the public domain. I think there are common-sense things that have—as awareness grows, as groups like the Partnership for Critical Infrastructure Security and others raise awareness—critical information and data is taken off. Some of this is the way we do process. There are—a lot of the ways that these gentlemen got information or these researchers got information is they called up the local municipality and they looked for permitting, where were you allowed to dig to go lay a piece of fiber-optic? Some things as simple as that.

It takes a very concerted effort. It takes a very thought-out methodology and it takes lot of time to do it. That is why it takes so long to get a Ph.D., I guess. But the bottom line is that I believe that this kind of work is going to go on in academia, and I think this kind of work should be encouraged in academia.

I think the real story that didn't come out in the Washington Post, because as you all know, you don't get on the front page of the Washington Post without having a real hotshot story, there are some misconceptions about the story. Number one, the government never ever tried to suppress the dissertation. That was never in the mix. The real story that was being—we were being interviewed for was, one, young, smart researchers that are involved in the homeland security agenda. We support that, as a university, in terms of getting that message out.

And, number two, how a university can work with the government and industry.

What didn't come out in the article is that when I came to the university to assume this project and we were looking at funding mechanisms to—what research within the university to fund, obvi-

ously their project came right out at me as one we needed to begin to move forward quickly. So in the process we got funding to them.

And I also engaged in a process to begin to—for lack of a better word, begin to "shop" their research around. Number one, we looked internally to make sure there is a lot of sensitive data here. How are we handling it? And we had very solid procedures in place within the university. Coming from a government career, handling a lot of classified materials, I was very satisfied with the procedure the university had in place. We beefed it up a bit, particularly after the July article. But there were—this is an example of academia acting responsibly. Then we went to government and business alliances that deal with this—that have a use for this type of modeling, and we engaged in discussions with them.

That, to me, is the real message of the article, and that is a positive thing. That should happen all over the universities. I believe that is the way we instill and preserve the academic freedom element; and it is also—another key element of this is, we have to grow the next generation of security professionals.

We have to grow the next generation of thinkers in this area that are going to take us to the next level, to alleviate some of the frustration—some of the kind of frustrating, seemingly, lack of control over our understanding of our vulnerabilities.

I don't think we have—our capability is just emerging to be able to visualize and build the kind of models that are going to help us; and so we are in this kind of gap period. So it is very important that we find a way to make this kind of relationship work, and in our small way at GMU, we tried to do that with this project.

Mr. TURNER. So what you are saying is that the work that Sean Gorman did in his dissertation is, in effect, a kind of model for what you think perhaps ought to go on in a wide variety of critical infrastructure sectors so that eventually we would have the capability to comprehensively map our infrastructure in a way that we could then manipulate the data and identify our critical vulnerabilities and assess the impact that the disruption of one or an other sector might have on other sectors?

Mr. MCCARTHY. Yes, sir. I fully support that statement.

And to piggyback on a comment again that Mr. Watson made relative to the national labs, the national labs play a critical role in helping the sectors. It is defined in the security strategy in helping the sectors help with this modeling and simulation and visualization capability. That is what they do well.

I also think, and I would like the committee to be aware that academia is out doing this also, and it is very critical that we just don't put all of our examples in one basket in that area, that we support the activities going on relative to these kinds of projects. Because, number one, the academia, the—again, the research and information is out there and it is happening, so we have to find a way to capture it and make sure that we develop responsible standards by which academics should act.

And I think that we have plenty of models out there. We have done this with biological research, we have done this with nuclear research, and we are doing it now with cyber and infrastructure research, so we have models to check concerns that are legitimate;

and in the other area, that we should just—we should be opening up.

We have a very rich and robust higher educational structure that we have to leverage to this problem. And we have done it, again, in the past. We did it in World War II. We did it with the Manhattan Project. We did it with getting to the moon. And this is critical infrastructure. And cyber security and terrorism, all of these issues, to me, are equivalent to those processing. We couldn't have done those things without the proper relationship between government, industry and academia working together.

Mr. TURNER. Thank you.

Mr. THORNBERRY. The gentlelady from the Virgin Islands.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

Mr. Gilbert, has—this is a similar question to one that Mr. Turner asked the previous panel. But has your—the panel that you chair formulated an opinion on which of our critical infrastructures pose the greatest security concerns, that is, greatest risks of attack, vulnerability to attack and potential consequences?

Mr. GILBERT. Yes, ma'am. And we wrote about it in the report. And as a matter of fact, we placed that dubious honor with the electric utilities, not only because of the vulnerabilities that they represented, but also the enormous dependency of the other basic infrastructures' support systems, that we all rely upon, that are so dependent upon the constant reliable supply of electricity. We are truly hard-wired as a society and as an economy to the electrical supply.

Mrs. CHRISTENSEN. Thank you.

Mr. McCarthy, obviously, George Mason is doing a great job of providing researchers and growing that next generation of thinkers. You talked about the research projects and your collaborations with the universities. I was wondering, of those 20 or more universities, how many are historically black colleges and universities or minority-serving institutions?

Mr. MCCARTHY. Immediately, off the top of my head, two. Norfolk State University we are working closely with on both cyber security and information warfare which—they are developing a fantastic program down there on that. And we are supporting them closely with that. And they are also supporting us in the National Capital Region Assessment that we are doing. And also Howard University. We have professors from Howard involved in our National Capital Region Assessment.

Mrs. CHRISTENSEN. Great. Thank you. Also, I was interested that your critical infrastructure protection is based in the school of law in the area where, among the many things that you are exploring are the legal implications of information sharing; and I was wondering if—as you are looking at that, if there have been any concerns raised.

Many of us are concerned, for example, with the loss of privacy and intrusions into civil liberties. Have you been discussing any of that thus far?

Mr. MCCARTHY. Oh, yes, ma'am. First let me say, I appreciate your recognizing that we base this project in the school of law. Highly, highly unusual. I am not a lawyer. I am not a technologist.

I come from the information policy arena and a government background.

We based this project in the school of law, and it is really the school of law, economics, and we have made this with a mandate for interdisciplinary research. It comes with the premise that if you just look at the Federal grant process, you would put on the table stacks and stacks of Federal grants for technology development. You put another stack out there for the policy and kind of business governance things. It kind of goes down pretty significantly. Then you go down and you put in for grants that we are sponsoring to develop this agenda in the area of law and you get virtually none.

So we kind of reversed the model for the use of this money. We fund technical research, and the technical research is critical to integrating what we are doing. But our primary emphasis is looking at law, economics, business governance and policy issues relative to the homeland security CIP agenda, and it is to work in complement with what is happening with the technologist, the—and I will give you one quick example.

The technologist. One project we are sponsoring is to look at attacker fingerprinting. When somebody comes into your computer, they are leaving traces; and it is just like when the FBI comes in and dusts. We are looking to develop that. As that research reaches a certain level of maturity, we are going to take that research and bring it into the law school to look at the intellectual and privacy implications of the technology, so when the whole project is released, you see not just the technological application, but you also see the concerns that are raised relative to privacy and intellectual property.

Mrs. CHRISTENSEN. Thank you.

And my last question would be directed to both, I guess, Mr. McCarthy and Mr. Gilbert, but anyone could answer it.

Both of you talk about, for example, Mr. Gilbert, issues that deter open discussions among the private and governmental parties that need to be correctly resolved. And I think that Mr. McCarthy refers to that.

Do you have any recommendations as to how we resolve those issues? Because it comes up not only in this area, but in Project Bioshield and just about everything that the Select Committee looks at.

Mr. MCCARTHY. I will defer to Mr. Gilbert.

Mr. GILBERT. Well, the primary areas that came up in our interviewing of people who had vested interests in the utilities were in antitrust and freedom of information. In the freedom of information, it was the problem that the private sector is quite willing to talk about what they have and what they are doing and all of that, but they don't want those minutes to become a part of a public record where it is then readily available for tomorrow morning's newspaper or for their competitors. So there is—I believe, under the Homeland Security, there is a classification now of homeland security information, "infrastructure information," which is a source of information that can be protected. And I think that is an important step to overcoming the observations that we had when we were putting this report together.

So I think progress is being made. But those are the kinds of issues—antitrust is a big problem, and it is always filled with a great deal of uncertainty as to what is or is not a violation of an antitrust matter and whether or not there will be a knock on the door by the State's attorney and so on and so on.

So clarification in that area is more what is being sought.

Mr. MCCARTHY. I would very much agree with that. We held a seminar at the law school on the antitrust issues relative to this agenda. And the consensus among the legal scholars and legal practitioners was that there really probably aren't that many antitrust issues involved. However, the industry representatives at the forum, their general counsel—predominately the general counsel community is, hey, it is a perception issue; and if my CEO comes to me and says, I want to share the data or not share the data, I am immediately going to say, don't share the data. You know, that is just to protect—that is his job or her job to protect the company.

So there is part of that mentality out there. There is—but I don't think that predominates the discussion.

I think what we need to do is develop islands where we can protect information properly. And again I think there are models out there. The national communications system was mentioned. That is a good model of industry, government and academia working together to create an island of protection.

The ISACs were raised. I think the ISACs have the potential to be those islands of protection for information if we can come down and get past the FOIA and the antitrust and the kinds of things that are bogging down the discussion, and move forward with kind of a vision of articulating what the economic and business model is to incentivize someone to participate in an ISAC and also to lay out, from the government's perspective, what is it that they really want to get from ISACs.

Mrs. CHRISTENSEN. Mr. Chairman, could Mr. Rauscher also answer that? Thank you.

Mr. RAUSCHER. Yes. I agree very strongly with the comments, that the NSC for the communications infrastructure and the telecom ISACs are the right place to do this. I would like to say that for the communications industry, government requests at all levels—Federal, State and local—for information about critical infrastructure are very much a concern. And it is not just for the reasons that were emphasized here about priority information dealing with businesses and business issues, but for, very much, homeland security concerns.

You know, much of the communication infrastructure is privately owned. Most of it is. And the experts, the physical security experts that have been assembled to develop best practices and look at those issues from across the communications infrastructure, are consistently and firmly in agreement on this point. And we believe it would be helpful if we could avoid government at every level, asking for stuff, because if you just think of all the lists that would exist of all the critical sites; and so, while normally you want to manage by facts and collect information, that is the normal approach, there needs to be an exception when you are dealing with sensitive information and those exceptions need to be very clear for

specific purposes and information protected sufficiently and information destroyed and returned when you are complete with it.

One other comment referring to the earlier discussion that hasn't been said, but it should be clear that critical infrastructure designers and operators need to be careful about what they put on public Web sites.

Mrs. CHRISTENSEN. It has come up before. Thank you.

Thank you, Mr. Chairman.

Mr. THORNBERRY. I thank the gentlelady.

Let me ask a series of brief questions because I know we kind of have a hard deadline here of 4 o'clock. Some of the witnesses need to go, and so I don't want to take too long.

Mr. Gilbert started out this panel with his personal opinion about a possible scenario where you have a power failure that affects food, water, all sorts of things. My impression—does anybody on the panel disagree with that as a real possible scenario, where failure in one infrastructure affects other infrastructures?

Mr. Watson.

Mr. WATSON. Mr. Chairman, you asked earlier about the most critical thing to study, and I mentioned interdependency. And this speaks directly to that. Yes, there, the interdependency and the cascading failure issue is the hardest problem to solve. I don't necessarily think that we would see an electric power failure that lasted weeks and months, you know, that would create that kind of a doomsday scenario that was painted.

And some of the sectors are pretty robust. The telecommunications sector has many ways of communicating and to work around problems. But the cascading failure of the dependencies is something that just isn't known. That is why I recommended modeling as one way to solve the problem.

Mr. THORNBERRY. Which is an interesting thing. We do lots of modeling and simulation, of course, in the military.

Mr. Gilbert, did your committee look at modeling? I mean, you mentioned it, I believe, modeling and simulation. And one of the things that concerns me is we could spend, I don't know, maybe Mr. Watson talked about time and money for a long time study. Meanwhile, the terrorists are active.

It leaves us in a little bit of a quandary about—

Mr. GILBERT. Well, fortunately, at least insofar as the electric utilities are concerned, there is in the Electric Power Research Institute an ongoing activity in developing simulation models that deal with the operations of their assets. That needs to be vastly expanded. There has also been some very good work done at Sandia Labs in this area.

Mr. THORNBERRY. On interdependency, how the failure of one affects another?

Mr. GILBERT. Yes. Sandia has gone into more interdependency; the Electric Research Institute has gone—mostly staying within the family in its study work. But there is good framework there. There are good algorithms. The challenge is getting useful data on the condition of existing facilities and on not only what the different switches and components of a piece of the grid might be, but their actual condition with respect to maintenance and remaining

life and functionality and so on, which is giving away a lot of information when you start to gather that kind of—.

Mr. THORNBERRY. And when you start to gather it, it may change by the time you are finished gathering it if you are talking about the condition of things. But that is part of the challenge.

Mr. GILBERT. But it also provides a source of important information which is to begin to get some trend information on different kinds of components—this kind of components 10 years out there, if the weather is looking like this and so on.

Mr. THORNBERRY. Yeah. Good point.

Dr. Orszag, I think that your testimony is very helpful at a level of specificity that we have been trying to cope with, for example, in cyber security. What is the right combination of government regulation and market incentives for the best practices that fits with each sector? And you made some specific recommendations for cyber security, which is one of our primary responsibilities on this particular subcommittee.

Have you run your suggestions past industry trying to ask the question, for example, is this enough? Would this sort of framework affect the way you do business or affect the decisions that you make when you are buying things or trying to figure out how to allocate resources in your company?

Mr. ORSZAG. We have had, or at least I have had, informal discussions with industry reps. I don't know that it is my particular role to interact in that particular fashion with industry. And I would underscore a comment that Congresswoman Sanchez made, which is that, of course, industry is not enthusiastic about any additional requirements.

But I don't think that should be the defining consideration here. In some sense, there is a national objective that private interests in this area, and you know, it is unfortunate that the incentives need to be realigned, but we need to push them closer together.

Ms. SANCHEZ. I wasn't necessarily agreeing.

Mr. ORSZAG. No. I understand. I got it.

Mr. THORNBERRY. But it is very important.

Mr. ORSZAG. It makes it harder.

Mr. THORNBERRY. Mr. Watson, if I could just ask a few things of Mr. McCarthy. What is the time frame? When are you going to have something for us to see or for the Department of Homeland Security to see where you have taken some of the economics that we were just talking about, the legal concerns that Mrs. Christensen was asking about, and merge that together.

Mr. MCCARTHY. Actually, sir, the Department of Homeland Security has already seen a number of our products. A number of our products have been published in peer review.

Peer review is very important, without going into details. And as we speak, we are at the printer right now printing the collective research on the project for the last year, and findings; and I would be happy to provide that to both committees.

Mr. MCCARTHY. And if I could just make one comment relative to this discussion, this question you just had: Comment was made in the first panel, not meaning to be critical, but the term "costly annoyance" was used relative to the cyber attack. I think some-

thing fundamental that has come out the last few months here is the drag on the economy.

I was talking to one international bank, just one bank. They have done their quick economic analysis which you can imagine how that was done pretty quickly and pretty accurately. Fourteen man-years in one week, 14 man-years in one week simply to deal with patching and plugging. That doesn't talk about the impact on the bank itself and the transactions.

I believe that the sectors are going to start doing this economic analysis, which isn't very sophisticated and it is moving much past the idea of ankle biting and annoyance.

Mr. THORNBERRY. Good point. And I am not sure everybody understood that yet, by the way.

Mr. Rauscher, your testimony actually has been some of the most positive that I have heard about ISACs so far. A number of witnesses before, in previous hearings, have been concerned that ISACs were not working as well as they should for a variety of reasons. But eventually what you are saying from your experience is that the telecommunications ISAC and the electricity ISAC were working well together with the IT ISAC for this event. And so maybe there is hope yet.

Mr. RAUSCHER. Yes, and maybe it is—the ISAC. I am familiar with the telecom ISAC, which is the one within the Department of Homeland Security. I was on [the conference bridge] from actually the first minute of that the exercise Responsive coordination began from the start of the blackout through several days and I heard briefings from the other ISAC about whether power was going to be restored and helpful guidance that we could use to position generators and experts and prepare for fuel supplies. Very helpful activity occurred, and as I mentioned in my statement, I think—it was the first time, I think, some really inter-ISAC activity occurred.

Let me also mention that the Wireless Emergency Response Team, which was started on September 11, was a new organization—a capability that involved hundreds of people being mobilized within hours, was able to be done because the support of the telecom ISAC. This was on September 11, before all the readjustments had been done.

I am really hoping that the positive, trusted and environment that exists there continues.

Mr. THORNBERRY. Absolutely. Maybe we can learn from what is going well with some ISACs and apply those to some that are having more trouble, and that is helpful.

And finally, Mr. Watson, you spent a fair amount of time talking about sector coordinators within the government. In your—should they be the ones to be a primary, if not the primary, contact with the ISACs for their sector as the key, as a key contact within the government?

Mr. WATSON. No, Mr. Chairman. Let me clarify what I said.

Sector coordinators are in industry. They are nominated with consultation between government and lead agencies and industry leadership to identify those leaders and coordinators across the sector. And yes, they should be the primary contact.

Mr. THORNBERRY. On behalf of the ISACs?

Mr. WATSON. On behalf of the industry sector, because they have a broader reach than some of the ISACs, and one of their responsibilities is to establish information-sharing capability which includes the ISAC for the sector.

Mr. THORNBERRY. Okay. I think your chart probably confused me, because you had the USDA and various agencies beside some of the names. But what you are saying is that is who they interact with?

Mr. WATSON. There are sector leaders in the lead agencies and sector coordinators in each industry sector.

Mr. THORNBERRY. I've got you. Okay.

Mr. MCCARTHY. Sir, if I could just make one comment very quickly. We just had a seminar and called and asked all of the ISAC community to come in, along with the Department of Homeland Security, again to provide some independent third-party kind of analysis.

One of the key elements that jumped out at us, there isn't—there are no standard models of action. There are functions at all different levels of operational activity and maturity, and I think one key action item that can come out of this is the development of, A, what is the standard? What is it that we want out of an ISAC? What is the standard? Does the industry adhere to that standard?

And you can make better evaluation.

Mr. THORNBERRY. What are the characteristics? They may have to be somewhat different from this industry's best.

The gentleman from Arizona is recognized.

Mr. SHADEGG. Thank you, Mr. Chairman.

Mr. Watson, I want to begin with you and follow up on a question that the chairman just propounded dealing with your testimony that the sector coordinator rules are poorly understood. I guess I would like you to give a further explanation of that than I see in your testimony, and in doing so, explain to me how you think the sector coordinator should be working with the ISACs and how that would work.

Mr. WATSON. I will do my best to do that.

The original idea of sector coordinators came out of the President's Commission for Critical Infrastructure Protection that reported in October 1997; and they recommended that the government identify, in coordination with industry, a leader in each sector to coordinate across the sector. It is very difficult to coordinate, you know, with 80,000 IT companies and 6,000 electric power companies or whatever. You know, one from the government, from DHS, or whatever agencies the government is dealing with.

Mr. SHADEGG. Let's stop right there and then say, who then is the sector coordinator?

Mr. WATSON. That is another hard problem. It varies by sector. DHS's working to developing a best practice for sector coordinators.

Mr. SHADEGG. Sector meaning the IT sector, like telecom?

Mr. WATSON. Yes industry sectors.

Initially most sector coordinators were industry groups (associations). However, currently the sector coordinator for financial services is an individual at the Bank of America.

So a company is representing that sector and coordinating across the sector. The sector coordinator for financial services has devel-

oped a Financial Services Sector Coordination Council that includes all of the trade associations throughout the financial services industry, and part of that includes the ISAC.

One of the responsibilities the sector coordinator is to establish and maintain an information-sharing capability within the sector, across the sectors, and between the industry and government.

In the electric power sector the sector coordinator is the president of NERC, the North American Electric Reliabilty, and they also operate the ISAC, so it is a different model for that sector. NERC provides for automatic membership of all the trade associations in the electrical power industry to participate in this ISAC as well as other sector responsibilities. The sector coordinator is responsible for things beyond information sharing, like research prioritization, public policy and other kinds of areas that are concerned with some of this information sharing.

Mr. SHADEGG. With the creation of the Department of Homeland Security do we need to formalize the sector coordinator role and give it structure so that they are the same from sector to sector and have some degree of authority that they apparently lack at the moment?

Mr. WATSON. I would like to see the sector coordinator role promoted in industry and government, and the DHS is coming out, is developing sector coordinator best practices guidelines. They don't want to go so far as to decree what is right or wrong for the sector coordinator, because industries differ. But if they can come up with what works and what doesn't work and publish a best practices guideline, that will be very helpful to be able to meet those guidelines and do the job of sector coordinator.

A definition of the role of sector coordinator is needed and then promoting that responsibility is also needed.

Mr. SHADEGG. Let me ask all of you a question, and maybe it is too broad to be susceptible of an easy answer; but it seems to me that you look at different sectors and you look at interdependencies, and some are better than others. It seems to me, for example, in telecom there are—the telecom industry seems to me does a pretty good job. If you can't take this route, you have got this route and this route and this route. And we covered some things that went down on 9/11, but we discovered they were able to quickly come back by some other routes.

I was just downstairs in a hearing on this issue, on the blackout. We have—we really have a system there of, if one goes down, then usually the others can cover and you don't wind up with a blackout. But your testimony, all of you today, kind of illustrates how to kind of step beyond that.

When you go from sector to sector, you get in deep trouble. For example, power goes out and the next thing you know, you can't pump water, so the water system goes down. You can't pump the sewage. In your testimony, you talked about a diver having to go through 40 feet of sewage to restart a pump. Sewage goes out. And fuel pumps go out. You can't pump gasoline, you can't pump diesel fuel.

Who is responsible?

And it—should it be DHS's function, should it be something that this committee is looking at for forcing some coverage to make sure

that, you know, there is an—somebody is examining the missing link and says, Okay, well, we should mandate backup power plants for these kinds of things like we have for hospitals.

I mean, somebody obviously thought through if the hospital goes down we had better have a generator sitting outside to bring it back up so that the discussion that is ongoing can be complete. But we apparently haven't done that for the sewage plant that is mentioned in the testimony, and there may be too many other places where we haven't.

My question is, who has got that responsibility?

Mr. WATSON. I think DHS has the responsibility within the IAIP Directorate. That is information analysis infrastructure protection to identify the problem, work with industry to develop solutions together in a public-private partnership. Industry owners and operators understand their key notes and critical assets, but they don't know all of where they depend on other infrastructures and that—that higher level problem is something that DHS could provide some guidance and help with.

Mr. SHADEGG. Anybody else want to comment?

Mr. RAUSCHER. In infrastructure protection—speaking for the telecommunication infrastructure we should understand not only its vulnerabilities, but do risk assessments and make appropriate plans for how to deal with those.

Mr. SHADEGG. Do you agree DHS has that responsibility?

Mr. RAUSCHER. Many of these infrastructures are privately owned. So what about the expertise? The first question is the duplication of the expertise. There has to be a partnership with the industry and I think there are things like the President's National Security Telecommunication Advisory Committee that has policy issues, the industry does bring those forward. So much of the ideas are going to come from the experts within the industry.

Mr. MCCARTHY. I believe the Department of Homeland Security has responsibility to build and manage a comprehensive framework that allows the industry, depending on the sector, to be able to hang their issues and their problems and to be able to do the analysis they need to do. The success stories for information sharing and ISACs come from the fully funded governmental—the national communications fully funded. I mean, it is an entity that the industry has invited to come into. The FSISAC is coming from pure industry funds, but there is a significant amount of money to it.

So that tells me something. And you analyze the water industry, and that is a very decentralized activity than the cascading effect is is a local cascading effect and the true threat is the undermining of public confidence across—you know, it is not the connection between the infrastructure; it is if you do this in New Jersey, what is going to happen in Detroit?

Mr. ORSZAG. I do think the responsibility rests with the Department of Homeland Security. I would just say that obviously one needs to be careful. I would not want an array of government bureaucrats coming in and saying you, firm A, needs a backup generator. Instead, you need to be thinking about the government structure that provides incentives for that firm to do that on its own. And I frankly think that this is, I don't want to say the—one of our biggest failures in homeland security. I do not think the De-

partment of Homeland Security is thinking through incentives that should be provided to the private sector in, as far as I can tell, any kind of systematic fashion. And I think it comes back to the concern about changing the incentives in any way and I think that that is a very substantial and critical vulnerability that this committee and others should frankly force them to change.

Mr. GILBERT. Add my two cents. I want to be very careful about what we say the homeland security should do, because I think it may serve the role as convener, it may serve the role of facilitator, may serve the role of organizer, but you have got all levels of government involved in these various elements of your infrastructure and a lot of private parties as well. And so each one has their own set of issues they have to deal with. So I think if the homeland security organization can help to focus and plan and describe and lay out what the interlinked needs requirements are and then work with these various levels and organizations, where the means by which financing and implementing and so on can take place, then I think we can make some progress.

I was involved with the first responders and the early attempts to try to get something out that would improve their situation, and there was a whole lot of talk and a very little bit of delivery and a lot of expectations raised, which didn't get fulfilled. Some still aren't. So I think we have to be cautious about how we rush forward here.

Mr. THORNBERRY. Mr. Watson, I understand that you have to leave and to catch a plane, which is the last chance. So at this point you are excused.

Mr. MARKEY. Could I ask Mr. Watson just one question if you still have time?

Mr. WATSON. I can do it, sir.

Mr. THORNBERRY. Gentleman from Massachusetts is recognized briefly.

Mr. MARKEY. Mr. Watson, what time is your flight?

Mr. WATSON. At 6.

Mr. THORNBERRY. The gentleman from Massachusetts is recognized for a more extended period.

Mr. MARKEY. And that brings me to my point which is that, you know, we got a lot of Federal agencies that really don't ask a lot of questions, you know, to get the real situation identified so that then you can deal with the reality of it the way we just did about when your flight is, which helps so everyone can conform to the reality of the situation. So back in January, the slammer worm disabled computer systems at First Energy Davis Bessie reactor and other utilities. And in at least one case, this was because A, people didn't download their security patch, or B, that the T–1 and remotely-connected computers circumvented the fire wall. So actually, believe it or not, nothing actually happened at the NRC after that in terms of warning other nuclear reactors that there was a problem. Kind of shocking that they didn't do that.

What I did on August 22 was I wrote a letter to the NRC and I asked them about this incident back in January and what they had done and what were their recommendations for the other nuclear utilities since they actually hadn't said a word to any other nuclear utility in 7 months. And then remarkably one week later,

the NRC sent out an information notice to all nuclear power plants in the United States explaining what had happened 7 months before in their nuclear power plant, but they actually had no orders to fix the same problem in their own nuclear reactors if they had such a problem—no orders at all.

So my question to you, Mr. Watson is, shouldn't homeland security be mandating to each of these agencies that work with them that they inform affected parties, potentially affected parties of critical infrastructure and the critical infrastructure sectors of vulnerabilities and then specifically recommending fixes that could prevent the very same problem from occurring in their utility?

Mr. WATSON. Let me make sure I understand the question correctly. You are asking the question should the DHS be responsible for mandating that other Federal agencies provide warnings so that industry could provide—could implement fixes when vulnerabilities are discovered?

Mr. MARKEY. And the Nuclear Regulatory Commission obviously just flubbed this completely until I notified them and that is not a good situation given the fact that we are right now wondering whether or not a worm or blaster might have helped to aggravate the problem at First Energy. This doesn't seem to be an awareness at the Nuclear Regulatory Commission of the pervasive nature of this cyberterrorism threat in terms of its potential consequences for nuclear power plants.

Mr. WATSON. This is a multi-phased question. Patching is a complex problem. The idea of warning and providing information on vulnerabilities is another problem. And the idea of mandates on either area is a third question.

Mr. MARKEY. Should there be a warning first?

Mr. WATSON. I believe there should be a warning. I am not sure whether—and not knowing enough about every kind of possible threat, I am not sure whether that should be mandatory for Federal agencies. As far as patching goes—

Mr. MARKEY. I don't understand what you mean. The Nuclear Regulatory Commission has jurisdiction over nuclear power plants and their safety. Here is a problem that was identified at Davis Bessie with regard to the slammer virus and no warning was given to the other 103 nuclear power plants in the United States that this incident had occurred. So the first question is should the other 103 nuclear reactors have been notified?

Mr. WATSON. I believe they should.

Mr. MARKEY. Does everyone agree they should have?

Mr. WATSON. I am not sure it is NRC's responsibility to make their notification.

Mr. MARKEY. It is their responsibility. Under the Atomic Energy Act, it is their responsibility.

Mr. MARKEY. Who do you think the responsibility would have been with?

Mr. WATSON. The information on the slammer and other cyber kinds of worms and viruses flows through the ISACs action and the energy ISAC, and the electricity sector ISAC had the information and they were spreading it across to industry members of the ISACs. I believe that that information flowed very quickly. As far

as recommendations on when to patch and how to patch, that can be complex.

Mr. MARKEY. Do they have authority to mandate that there be a patch—ISAC?

Mr. WATSON. They do not have the authority to mandate a patch, and I am not sure mandating a patch would be the right idea.

Mr. MARKEY. Do they have—do they have the power to mandate that the utility inspect to see whether or not a similar problem exists within their nuclear—

Mr. WATSON. ISACs do not have power or authority over industry members.

Mr. MARKEY. What I am saying it is inside the Nuclear Regulatory Commission. They are the agency responsible for the safety of nuclear power plants in the United States. And when they were given this information, it was they who had the principle responsibility delegated by this Congress and by ultimately as this committee has now jurisdiction over it by the Homeland Security Committee to ensure that that information is communicated, or else we wind up with a same problem that we had in, you know, in August of 2001, where information was there, but not communicated in a way that could be effectively used.

Mr. MCCARTHY. Your scenario actually raises an additional issue that I think is of vital concern. There has been numerous discussions of infrastructure since the President's Commission report, et cetera. And as you get into the room and we discussed the room almost divides into two camps, one that says never can happen, absolutely never and the other one that says it is happening and the sky is falling. So we have to find that place in between where you know the notion of an intrusion into a nuclear plant, and again, there are many systems in a nuclear plant and whether that intrusion went into a vital critical system is what is at issue rightfully and I think that you point that out. But the key issue there is when you are trying to do this vulnerability assessment and get the data to run the models and to do the visualization and see what is there, you run across this constant tension of can never happen and therefore let us not talk about it anymore, because you are just giving information to bad guys, a road all the way to the world is coming to an end, and we have to get past that.

Mr. MARKEY. I think the problem we identified here was obviously one that is central to the reason why our committee was constructed, which is there is not an effective dissemination of information to potentially affected parties of relevant information of threats that have been identified. And I think that here, if there was a similar problem in another nuclear power plant, that the Nuclear Regulatory Commission had an obligation in a timely fashion, in my opinion, after September 11, that means immediately to send that information to all of the nuclear power plants. That is not proprietary information to Davis Bessie. It is now relevant information to vulnerabilities inside of nuclear power plants that could be exploited.

And I don't think that happened and I just think that unless we have a systematic way of ensuring that these agencies respond not to the utility, but rather to public safety and security as their principal responsibility which, by the way, each of these agencies have

as their principal charter responsibility, then we will have some brilliant al Qaeda Ph.D. from MIT or Harvard or CALTECH some day in the future exploit that vulnerability. Thank you, Mr. Chairman.

Mr. THORNBERRY. The gentlelady from Texas.

Ms. JACKSON-LEE. Dr. Orszag, I would like to focus my questions in your direction and to suggest that the thrust of this committee, my understanding, was to ensure that we would be called the Homeland Security do-something committee as opposed to do nothing. And I say that in the backdrop of the issue of terrorism never announces its entry in our lives. We saw that on 9/11. And so, I believe it is important that we have a mind-set of preparedness and readiness, and therefore, I find it very difficult that we don't take the laboratory of the blackout and really act.

And governmentally we have to act because the private sector responds that we don't want to be intrusive. We want a robust private sector, but they don't respond in many instances, and I understand it unless we give guidance or regulations or defined policies that they can abide by. One of the issues in this committee is to empower citizens, that is more preparedness in neighborhoods and communities. I hope that is very good. I would like to ensure that the ISAC now have legs, teeth and arms and can move.

And frankly, I believe that they were very comfortable advisory committees which I applaud. If we can claim a success on the days of the blackout, I think the success comes from the way local government responded. We can clearly probably see a distinction between 9/11 and now. I think they were efficient, they were calm, they were effective. That means mayors of the respective cities and our first responders and I want to compliment them on that. But I want to focus on some comments that you made regarding the administration's strategy leaves out several key priorities for action, including major infrastructure in the private sector, which the administration largely ignores.

Can you elaborate on how the current policies ignore critical infrastructure protection, what must be done to increase increased critical infrastructure security and from A to F, if you had to grade the Department of Homeland Security, DHS and White House efforts to protect critical infrastructure in the private sector, what grade would you give? And let me say, this is based upon two aspects, and I said it earlier today, accountability and then finding what happened so that we hopefully will not retrace our steps. It is not accountability for its sake simply, but it is to say that my sense of the blackout is urgency, one, a crumbling infrastructure which is no one's fault, it is aging and no intervention.

But I say that in the context that we are so grateful that what that was, as we understand it to date, was a crumbling infrastructure. Suppose it was not. And I think that gives us the extra added burden, the urgency to act yesterday. And as a government entity for us to say that who is responsible or not responsible but for us to be in the context that we can even pause for a moment is a difficult position—I find it a difficult position to be in. And I would appreciate if you comment on that.

And I have one other question. And gentlemen, please, Mr. Watson, we smile because we are dark through the airport one minute

before, but you do it the right way. So if you are able to comment right after him, I would not want you to be in a complex situation. And I don't know if you can comment on the policies, but hopefully you can comment on the question of critical infrastructure protection. Maybe you just want to comment.

Mr. WATSON. I have not been raising my hand to ask to be excused the whole time. I have been trying to get—a lot of questions have been asked about the role of regulation versus market pressure and that is one of the areas that is being studied by the National Infrastructure Advisory Council. They are looking at the role of regulation, or actually the best security driver sector by sector. In some sectors, regulation will impede security. In other sectors, regulation will enhance security. When you look at State and local governments and some of the public sectors that includes some of the utilities, they may need regulation to provide needed funding that they don't have. But in other sectors like the IT industry, regulation tends to inhibit innovation. It tends to mandate the lowest common denominator and those systems and products that are produced from regulation are two or three versions behind the State of the art and actually can harm security for that sector.

So I think that you will be benefitted and all will be benefitted when the NIAC finishes its study and publishes it and looks at what the most effective security drivers are for enhancing security across the sectors.

Ms. JACKSON-LEE. Could you include in your response the point made in your book about the DHS now having responsibility for overseeing critical infrastructure protection and elaborating on the lack of effectiveness on the concept of closer attention, whether close enough attention being paid.

Mr. ORSZAG. I think I suggested before, I think one of the most glaring vulnerabilities that we face as a Nation is precisely in the incentives that private firms have to protect against terrorist attacks. And I think one of the reasons that I have been disappointed by the actions taken thus far, we are almost 2 years after 9/11 is that there does not seem to be recognition of that point. If you listen to the rhetoric that comes from both the Department of Homeland Security officials and others, it is very much of the sort that the private sector has incentives to do all of this and I just fundamentally disagree with that. They do have some incentives but not strong enough.

I also agree that a heavy-handed sort of command and control regulatory approach is probably not the right answer in the vast majority of sectors; I would think that would be the sort of task of last resort. That would be the thing that you would use last. And instead what you want to be thinking about is ways of using private markets to create incentives for better protection so that you can get the innovation over time and have a more flexible system, and it is not a rigid approach.

But I don't see that kind of discussion coming out of the Department of Homeland Security. It is not sort of consistent with the rhetoric. There was one, I think, glaring example of this I remember on NPR several months ago in which a senior Department of Homeland Security official basically said we don't need to worry about this. The private sector will take care of it. Again, for the

reasons I lay out in my testimony, I just think that is dangerously and fundamentally wrong.

Ms. JACKSON-LEE. How would you grade them?

Mr. ORSZAG. Well, having spent 3 years grading students, I am a little reluctant to give a grade, because I know the sorts of complaints it engenders, but it is not a passing grade.

Ms. JACKSON-LEE. And do you think it warrants us acting now and very quickly, thoughtfully but quickly?

Mr. ORSZAG. I think thoughtfully is important. One does need to weigh—I am a firm believer in the power of private markets and incentives that firms face in determining the efficiency with which they do things. And I think you need to be very careful not to intervene in an excessively costly way. That having been said, we are now almost 2 years after 9/11. I raised chemical facilities before. That is just one of many sectors in which there has been absolutely inadequate movement, as far as I can tell, to correct incentives that firms face.

Ms. JACKSON-LEE. Mr. McCarthy.

Mr. MCCARTHY. On your grade, teaching a graduate course myself, I would give the Department of Homeland Security, given beyond the operational and policy things that have to happen, there is a tremendous amount of building that needs to take place. We are trying to build the airplane, design it, fly it and serve drinks at the same time. So from that standpoint I give the Department of Homeland Security a C, which as a professor and a teacher, it tells me the concepts are there, the pieces are there, and I do believe that organizationally we have built the right thing. We have the constructs.

Some levels of maturity gradations out in the private sector we have the right pieces in the government fundamentally to move forward. We have to allow some maturity and some areas in the identification of key assets to deal with the immediate, I agree we have to get that done and get that moving forward, but I would give them a better grade than that.

Mr. ORSZAG. It is the difference between grading on a curve.

Mr. THORNBERRY. Let me thank each of the witnesses because each of you has done and are doing important work that helps us to improve their grade and improve the grade of the whole government and the whole country, and that is what we are here to do. I thank the gentlelady from California for sticking it out as well as all of her work in the area of homeland security. We may have additional questions we will submit. If we don't ask the question but you have a suggestion, send it to us anyway as well as future publications and so forth. Again, I thank all the witnesses and this hearing stands adjourned.

[The information follows:]

[Whereupon, at 4:25 p.m., the subcommittee was adjourned.]

ELECTRIC GRID, CRITICAL INTERPENDENCIES, VULNERABILITIES AND READINESS

WEDNESDAY, SEPTEMBER 17, 2003

SUBCOMMITTEE ON INFRASTRUCTURE
AND BORDER SECURITY,
AND
SUBCOMMITTEE ON CYBERSECURITY,
SCIENCE, AND RESEARCH AND DEVELOPMENT,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittees met, pursuant to call, at 3:30 p.m., in Room 2359, Rayburn House Office Building, Hon. David Camp [chairman of the subcommittee] presiding.

Present: Representatives Camp, Sessions, Dunn, Smith, Weldon, Sanchez, Dicks, Jackson-Lee, Christensen, Etheridge, Slaughter, Lucas, Pascrell, Meek and Cox.

Mr. CAMP. [Presiding.] The Subcommittee on Infrastructure and Border Security and the Subcommittee on Cybersecurity, Science and Research and Development joint hearing will come to order. Today's business is to conclude part two of the hearing entitled Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection, the Electric Grid, Critical Interdependencies, Vulnerabilities and Readiness.

Good afternoon. The vice chair of the Cyber Subcommittee, Congressman Pete Sessions, will join me in this joint hearing, as he has agreed to sit for the chairman, who had a scheduling conflict. I would like to thank all of you for attending today's hearing, The Federal Response to the August 2003 Blackouts.

The two subcommittees will hear first from federal agencies that played a direct role in response and communications procedures during the blackout. We will then hear from a panel offering the state perspective and comments on information sharing. Our witnesses in order of testimony are the Department of Homeland Security Assistant Secretary of Information Protection Robert Liscouski, Department of Energy Acting Director of the Office of Energy Assurance Denise Swink, State of Michigan Assistant Adjutant General for Homeland Security Colonel Mike McDaniel, and General Accounting Office Director of Information Security Robert Dacey.

I want to thank all of the witnesses for their participation. The investigations into the blackout are still ongoing, and I understand that neither Mr. Liscouski nor Ms. Swink will be able to testify

about the cause of the blackout at this time. However, your direct experience in responding to the blackout, and your critical infrastructure expertise, makes your testimony very valuable as the Homeland Security Committee continues to look at ways to strengthen America's critical infrastructure. The committee appreciates your willingness to be here today.

To allow more time for witness testimony and member questions, the chair requests that members agree to a unanimous consent request to waive opening statements. The record will remain open for members to insert their statements in the record. So with no objection and agreement to waive statements, we will proceed.

Again, I want to thank our witnesses for being here today. We will hear testimony from our federal panel first, and we will begin with Assistant Secretary Robert Liscouski. Before you begin your statement, I would like to acknowledge before the committee that you also testified before the Cyber Subcommittee, and I would like to extend the committee's appreciation for your willingness to address this committee 2 days in a row.

PREPARED STATEMENT OF THE HONORABLE JIM TURNER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Thank you, Mr. Chairman.

I greatly appreciate the efforts of the sub-committees to continue their inquiry into the widespread blackout in August that left nearly 50 million Americans without power. Although the power outage does not appear to have been the work of terrorists, it clearly served as a wake up call for us examine not just our electrical grid, but all of our critical infrastructures and ask an important question, "Have we done enough since September 11, 2001, to comprehensively assess and protect our nation's critical infrastructures from potential terrorist attack?"

America's critical infrastructures comprise the backbone of our economy. They are essential to our way of life. In addition to electric power systems, these essential infrastructures include chemical and nuclear plants, water systems, commercial transportation and mass transit.

Our country's infrastructure also includes the extensive computer and information technology systems which we increasingly rely upon to operate and interconnect our many diverse physical assets.

There are hundreds of thousands of potential critical infrastructure targets that terrorists could choose to attack. In light of the potential threats and vulnerabilities we face, I want to draw the committee's attention to Governor James Gilmore's testimony last week before the full committee: "A good national strategy can reduce the risk (of a terrorist attack), and direct our resources to the correct priorities."

A comprehensive risk assessment is central to any robust strategy. Such an assessment should include a thorough assessment of threats, vulnerabilities, and consequences. Furthermore, in order to successfully execute a strategy, you need a robust organization; effective coordination between federal, state, local, and private-sector officials; and a clear set of objectives and standards by which to measure progress.

I remain concerned, however, about whether the administration has done all that it can do to assess the threats to and vulnerabilities of our critical infrastructures, and implement a strategy to protect them.

The problem we face today is that we are attempting to secure the homeland without a comprehensive strategy based on an assessment of threats and vulnerabilities.

This is like building a home without a blueprint or a pilot navigating through the clouds without instruments. Until we have a clear understanding of the likely threats against us and a ranking of our vulnerabilities it is impossible to set priorities, establish security benchmarks, and measure progress.

I hope we will hear today from our government witnesses how far along we are on completing a comprehensive risk assessment of our critical infrastructure. And I am interested in learning what the Department of Homeland Security's plan is for protecting our infrastructure once the assessment has been completed. Specifically, I would like to know what federal assets are going to be dedicated to this task, how the Department of Homeland Security intends to assert leadership at the federal

level, and how it will interact with the private sector to provide an acceptable level of security for all Americans.

I hope to hear that we have a solid plan that will move quickly to remedy the gaping holes in security—only one of which was so clearly exposed by the blackout last month.

I want to thank the distinguished panel. I look forward to your testimony.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Subcommittee Chairman, thank you for your efforts in holdingtoday's joint hearing on this important matter. We take up this subject matter in an extremely timely fashion, given the threat of hurricaneIsabel in this local metropolitan area.

The purpose of this hearing is to expound upon the examination of the blackout of August 14, 2003 that left some 50 million people in 8 states and Canada without power. The areas most affected, according to the North American Electric Reliability Council (NERC) were the Great Lakes, Michigan, Ohio, New York City, Ontario, Quebec, Northern New Jersey, Massachusetts, and Connecticut. This incident, thus far, has not been determined to be terroris-relates; however, the extent by which it crippled the above-referenced expansive sectors of our nation and Canada was frightening to the point that it should have given the Administration a "wake-up call" as to the inadequacy of our existing critical infrastructure. The primary theme, or issue, of to day's proceeding is "Whether we have done enough since September 11, 2001 to protect our nation's critical infrastructures from potential terrorist attack?"

In our task of collaborating and fine-tuning the newly developed Department of Homeland Security against the projected needs of our nation, we must begin our evaluation at the most basic levels. Critical infrastructure protection is important to every member of our national and local communities. In order to implement a program of securing cyberspace and critical infrastructure at a national level, we must follow a course of risk assessment, education, and careful reaction at the local level to protect our schools, hospitals, and rescue facilities. These goals are part of the impetus for the amendments that I offered as to the Department of Homeland Security Appropriations Act and to the Project BioShield Act so that funding mechanisms and the Secretary's discretion contain the control provisions necessary to ensure the proper and effective allocation of resources to the places that have the most urgent needs. An illustration of the disjunct in our infra and super-structure is the television broadcast of the tens of thousands of New Yorkers who had to walk across the Brooklyn Bridge to end their workday. This is vulnerability. Thousands of riders of underground mass transit systems trapped in cars, frugal in their consumption of oxygen and hopeful that their rescue team was near equates to vulnerability. Because we cannot cast blame for this occurrence on a terrorist group means that we are vulnerable to ourselves first and foremost. The Administration must increase our awareness of the status of the areas that are most open to corruption.

In Houston last year, a 21-year old man was sentenced to three years in prison for a terrorist hoax concerning a plot to attack the opening ceremonies of the 2002 Winter Olympics in Salt Lake City. The Houston resident was sentenced by the U.S. District Judge and ordered to pay $5,200 in fines. The Judge told the Defendant that she had sentenced him to three years because he had failed to demonstrate his understanding as to the seriousness of his crime and disruption that he had caused to federal agencies and private citizens.

The perpetrator told the FBI in Houston that he had intercepted e-mails between two terrorists plotting a missile attack during the opening Olympic ceremonies on February 8, 2002. The e-mails supposedly detailed plans to attack Salt Lake City with missiles launched from northern Russia. He later confessed to making up the story during questioning, telling agents that stress led him to tell his tale and that he had fabricated the e-mails.

Just a few months ago, Federal prosecutors charged a University of Texas student with breaking into a school database and stealing more than 55,000 student, faculty, and staff names and Social Security numbers in one of the nation's biggest cases of data theft involving a university. The student, a twenty-year old junior studying natural sciences, turned himself in at the U.S. Secret Service office in Austin, Texas. He was charged with unauthorized access to a protected computer and using false identification with intent to commit a federal offense. This incident sent a wave of fear across the campus of the nation's largest university, causing students and staff to consider replacing credit cards and freezing bank accounts. The studenperpetrator was released without bail and thereafter had limited access to computers. If convicted, the student faced as many as five years in prison and a

$500,000 fine. After searching this student's Austin and Houston residences, Secret Service agents recovered the names and Social Security numbers on a computer in his Austin home. According to the indictment, Phillips wrote and executed a computer program in early March that enabled him to break into the university database that tracks staff attendance at training programs, reminding us how vulnerable we all are even when our Social Security number is misused. To combat the vulnerability linked to Social Security numbers, the university must limit its dependence on Social Security numbers as database identifiers and instead use an electronic identification number that corresponds to Social Security numbers only in an encrypted database. This data theft was probably the largest ever at a university.

Therefore, since the threat to critical infrastructure is realized at a very local level, we must channel our resources and technology to the first-responders and leaders in the local communities. The movement to securing our homeland needs to be expansive, not retracting. If our local hubs and first-responders were disabled by a terror threat, we would have a hard time developing effective protective measures for our nation as a whole.

Just as we must ward against the large threats to our critical infrastructure, the "small" incidents must not be allowed to create a larger vulnerability.

PREPARED STATEMENT OF THE HONORABLE JAMES LANGEVIN

Thank you, Mr. Chairman. I would like to welcome our witnesses, and express my appreciation for your willingness to come here for what I hope will be a very enlightening and productive hearing. I look forward to hearing from these distinguished experts about our infrastructure and what we need to do to protect it.

Mr. Chairman, it was with great expectation that we created the Department of Homeland Security and charged it with protecting us from terrorist threats and responding to emergencies here at home. This means not just controlling the border or patrolling airports, but making sure that the infrastructure that is vital to the daily operation of the United States is protected. Congress was assured that infrastructure protection would be a top priority at DHS, but until the blackout, there has been no indication on the status of those efforts. Despite the open forum we are in, I am hopeful that we may get at least a preliminary update today.

Ultimately, the real problem is that we have not seen meaningful plans or progress from DHS in identifying critical infrastructure and existing risks. That step is critical before we can talk about how to protect it. This is a task DHS needs to be undertaking in close cooperation with local and state governments, though several states have decided to identify their criticalinfrastructure even without DHS support. A graduate student and his advisor took two years to produce a map of our fiber optic network from publicly available information. DHS has far more manpower and resources, so one would assume it could produce assessments much more quickly. I would like to hear from our panel what they think of DHS's efforts, or lack thereof, towards the goals of infrastructure identification and protection, and how they envision DHS either leading or supporting the endeavor.

Again, I greatly appreciate all of our guests taking time to be here to discuss this vital issue.

PREPARED STATEMENT OF THE HON. CHRISTOPHER COX

Good afternoon. I would like to thank the subcommittee chairmen and ranking members for taking the lead on this important continued examination of the lessons learned as a result of the recent power outages, the effects the blackout had on related critical infrastructure around the country, and how the Department of Homeland Security communicated and worked with state and federal agencies, and our international neighbors during the crisis.

I am pleased to join in welcoming all of our witnesses, and especially wish to thank Assistant Secretary Liscouski for returning for a second day of testimony after testifying before the Subcommittee on Cybersecurity, Science, and Research & Development, just yesterday.

It is often said that if we train like we fight, we will fight like we train. How DHS reacted and communicated with other federal and state agencies during the blackouts was the first major test of the Department's Information Analysis and Infrastructure Protection Directorate (IAIP), and I am eager to hear of the Department's successes, failures, and lessons learned from the blackout.

We now know that within less than an hour, DHS officials determined that the blackouts were not the result of a terrorist attack. It has been only a little more than a month since the blackout occurred, and although the exact cause of the blackout remains unknown, it is my hope, that the Committee will learn from to-

day's first panel the present status of that investigation, and when the nation might expect conclusive answers. Also, I look forward to the witnesses' testimony addressing how DHS was able so quickly to determine that the blackout was not the result of a terrorist attack or other bad actor.

Although initial analysis of the blackout indicates that it was not a terrorist event, we can be sure our enemies noticed the effect the blackout had on the nation. I note that in Ambassador Black's prepared remarks, from the first part of this hearing on September 4, he asserted that "the recent blackouts in this country serve as an urgent reminder that there remain vulnerabilities for terrorists to exploit."

The examples of the interconnected nature of our critical infrastructures are endless. As Assistant Secretary Liscouski notes in his prepared remarks "If one infrastructure is affected, many other infrastructures will likely be impacted." Colonel McDaniel's prepared remarks provide dramatic examples of the truth of those remarks.

Furthermore, experience shows us that intentional attacks other than a failure of the power grid can also disrupt the economy. The SoBig computer virus caused certain CSX rail routes to shut down on August 20, until a manual backup system started the trains running again. Without railroads to deliver coal, the nation would lose 60 percent of the fuel used to generate electricity. A computer virus or even a series of targeted terrorist attacks that shut down our rail, telecommunications, or fuel delivery systems could once again plunge significant parts of the nation into blackout and adversely affect the economy.

As recently as September 5, Larry Mefford, the FBI's Assistant Director for Counterterrorism, who also testified at the first part of this hearing, stated that the FBI has evidence of al-Qaeda's continued presence in the United States, and that the FBI's primary worry is that there might be terrorists here whom the FBI has not identified and more who are trying to enter the country. We know that al-Qaeda has assessed the possibility of attacking our power plants and transportation systems. Our ability to assess and protect against the very real threats to our infrastructure is crucial to our war on terror.

We learned many unfortunate lessons from September 11th. One of them is that our first responders often do not have the capability to communicate on shared radio channels even within the same city or town. The blackout confirmed this is still a problem. We need to ensure that additional spectrum bandwidth is in the hands of first responders as quickly as possible. We need to continue our efforts to enhance the communications capabilities of our first responders, as well as communications between federal, State and local officials.

We formed DHS seven months ago with the intent that the attacks of September 11, 2001, would never happen again. I am eager to hear what progress the Department has made towards this goal.

I thank all our witnesses for being with us and look forward to your testimony.

DHS is actively engaged in many areas, and the directorate that you are involved in is of special interest to many members and subcommittees. We have received your written testimony and ask that you just briefly summarize your testimony. You have 5 minutes, and thank you for being here.

STATEMENT OF THE HONORABLE ROBERT LISCOUSKI, ASSISTANT SECRETARY, INFRASTRUCTURE PROTECTION, DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. LISCOUSKI. Thank you Chairman Camp and Chairman Sessions and members of the committee. It is a pleasure to appear before you today to discuss the implications of power blackouts for the nation's cybersecurity and the critical infrastructure protection.

The Information Analysis and Infrastructure Protection Directorate, and specifically my office of Infrastructure Protection, has been actively involved in the analysis of the cause of the blackout, and the implications of the blackout on security of the electric grid as a whole. I would like to provide a brief summary of the efforts. Following the regional power outage in the Northeast on August 14, the Department of Homeland Security set up a crisis action team to monitor the situation and to conduct real-time analysis of

other potential events. The blackout is the first major event of its type that the IAIP team handled, and I am pleased to report that our team simultaneously tackled the issue from multiple angles.

The Infrastructure Coordination Division focused on the outage itself and the operational impact of the infrastructures. The national Cybersecurity Division looked into the possibility that the blackout might have been caused by a cyber-attack. And our Protective Security Division assessed emerging vulnerabilities caused by the blackout to assess the "what is next" picture. Concurrently, the Information Analysis Office analyzed previous and current intelligence traffic, and coordinated with the intelligence community and law enforcement partners to ascertain if the cause of the blackout was attributed to a terrorist or criminal activity.

Additionally, the Homeland Security Operation Center was involved in the response effort, coordinating communications between state and local first responders, the administration and other federal agencies. Situational awareness of the affected area, the entire nation, was maintained throughout the event. DHS coordinated with sectors affected by the outage, both updating them on information related to the cause and responding to requests for information. While no actionable threat information emerged during the event, it is important to note that the ability to communicate with the infrastructure sectors was in place to facilitate the sharing of information. Our coordination and monitoring of activities was not limited to the energy sector, but included telecommunications, banking, finance, health services, transportation and the water sector.

While the national focus was primarily on the blackout and its cause, our teams were hard at work assessing the cascading effects into other sectors. Interdependencies among the sectors were again demonstrated by this event. Seven major petroleum refineries suspended operations, many chemical manufacturing plants were shut down, grocery stores lost perishable inventories, air traffic ceased at several major airports, and emergency services capacity was tested. Web sites were shut down. ATMs did not work in the affected areas and the American Stock Exchange did not operate for a period of time. The effect of the blackout highlighted what we already knew at the department. If one infrastructure is affected, many other infrastructures are likely to be impacted as well. Indeed, all the critical infrastructure sectors were affected by this event. Understanding the vulnerabilities and interdependencies associated with cascading events is an area of great importance to the department. We have people focused on this issue to ensure we can anticipate those affects, prioritize our efforts based upon the bigger picture, not just reacting to the easily and the immediately observed.

Preventing a physical or cyber attack on key nodes of our nation's power grid is a fundamental effort to protecting the homeland. Accordingly, DHS is working closely with the Department of Energy and other federal agencies as we identify factors that caused and contributed to the blackouts and look for protective measures to prevent such an outage in the future.

On August 28, I was appointed the co-chair to the Security Working Group of the U.S.–Canada Power System Outage Task Force.

The Security Working Group is focused on determining if a cyber event directly caused or significantly contributed to the events of August 14. The data collection and analysis is ongoing and much work remains to be done before we have a definitive answer. IAIP was tasked with ensuring that the Secretary and the President had the complete picture of what was happening during the event, looking for areas that might be more vulnerable as a result in coordinating the information flow throughout the sectors with other federal agencies.

We learned valuable lessons. We are incorporating those lessons today. I am proud of the way the IAIP team responded to this event and I am confident that we are developing a solid team that Americans can count on in difficult times, whether they be in times of heightened threats, attempted attacks or blackouts or other natural disasters.

While it will be some time before the task force determines the exact cause of blackout, we know the system is vulnerable and we maintain a daily watch over what parts of the grid might be more vulnerable to attack because of system operations. We have conducted vulnerability assessments at power facilities. We have a protection strategy for key components. And we are working with the industry and our federal partners to determine the best way to implement that strategy. We have made progress. Our work is ongoing. We have a lot of work ahead of us.

I look forward to your questions after the conclusion of Ms. Swink's statement.

[The statement of Mr. Liscouski follows:]

PREPARED STATEMENT OF THE HON. ROBERT LISCOUSKI

Thank you Chairman Thornberry, Chairman Camp and Members of the Committee. It is a pleasure to appear before you today to discuss the implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection.

The Information Analysis and Infrastructure Protection Directorate (IAIP), and specifically my office, Infrastructure Protection, has been actively involved in the analysis of the cause of the blackout and the implications of the blackout on security of the electric grid as a whole. Let me provide you with a summary of our efforts.

Following the regional power outage in the Northeast on August 14, 2003, the Department of Homeland Security (DHS) set up a Crisis Action Team (CAT) to monitor the situation and to conduct real-time analysis of other potential events. The blackout was the first major event of its type that the IAIP team handled and I am pleased to report that our team simultaneously tackled the issue from multiple angles. The Infrastructure Coordination Division focused on the outage itself and the operational impact on the infrastructures, the National Cyber Security Division looked into the possibility that the blackout might have been caused by a cyber attack, and our Protective Security Division assessed emerging vulnerabilities caused by the blackout to assess the "what's next" picture. Concurrently, Information Analysis (IA) entities analyzed previous and current intelligence traffic and coordinated with Intelligence Community and Law Enforcement partners to ascertain if the cause of the blackout was attributed to a bad actor. Additionally, the Homeland Security Operations Center was involved in the response effort, coordinating communications between state and local first responders, the administration, and other federal agencies. Situational awareness of the affected area, and the entire nation, was maintained throughout the event.

DHS coordinated with the sectors affected by the outage, both updating them on information related to the cause and responding to requests for information. While no actionable threat information emerged during the event, it is important to note that the ability to communicate with the infrastructure sectors was in place to facilitate the sharing of information.

Our coordination and monitoring activities were not limited to the energy sector, and included telecommunications, banking/finance, health services, and transportation.

While the national focus was primarily on the blackout and its cause, our teams were hard at work assessing the cascading effects into other sectors. Interdependencies among the sectors were again demonstrated by this event: seven major petroleum refineries suspended operations; many chemical manufacturing plants were shut down; grocery stores lost perishable inventories; hospital emergency rooms treated an above average number of cases of suspected food poisoning; air traffic ceased at several major airports; and emergency services capacity was tested. Websites were shut down, ATMs did not work in affected areas and the American Stock Exchange did not operate for a period of time. The effect of the blackout illuminated what we already knew at the Department: If one infrastructure is affected, many other infrastructures will likely be impacted. Indeed, all of the critical infrastructure sectors were affected by this event.

Understanding vulnerabilities and the interdependencies associated with cascading events is an area of great importance to the Department, and we have people focused on the issue to insure that we can anticipate effects and prioritize our efforts based on the bigger picture, not just reacting to what is easily and immediately observed.

Preventing a physical or cyber attack on key nodes of the nation's power grid is fundamental to protecting our Homeland. Accordingly, DHS is working closely with the Department of Energy and other federal agencies as we identify the factors that caused and contributed to the blackout, and look for protective measures to prevent such an outage in the future.

As has been widely reported, the portion of the power grid affected by the August 14th blackout is made up of a very complex interconnected network of scores of separate companies that includes hundreds of power-generation facilities. In addition to physical connections among the facilities involving the transmission of power, there are numerous cyber connections among their IT infrastructures and those of companies that were unaffected. There is a wide range in age and sophistication of the technologies upon which these systems depend. In recent years, the process control systems that facilitate decision making in critical situations have often been made easier by the use of computer technology. The industry is in the process of moving forward with efforts to reduce possible vulnerabilities and improve cyber security. This information provides a backdrop for why we are investigating the possibility of a cyber connection to the blackout. There is presently no evidence that the blackout was caused by any criminal or terrorist cyber attack, although we continue to coordinate and share information with law enforcement to support our investigation.

On August 28, I was appointed Co-Chair to the Security Working Group (SWG) of the U.S.—Canada Power System Outage Task Force. The SWG, which consists of Federal and State government representatives from the United States, as well as Canadian representatives, is focused on determining if a cyber event directly caused or significantly contributed to the events of August 14th. The data collection and analysis is ongoing and much work remains to be done before we have a definitive answer.

IAIP was tasked with ensuring that the Secretary and the President had the complete picture of what was happening, looking for areas that might be more vulnerable as a result, and coordinating the information flow throughout the sectors and with other federal agencies. We learned some valuable lessons that have already driven some internal changes, such as institutionalizing joint operations within IAIP, and the absolute requirement of maintaining a forward-looking "what's next" posture, not becoming focused exclusively on current events.

I am proud of the way the IAIP team responded to this event and I am confident that we are developing a solid team that America can count on in difficult times, whether they be times of heightened threats, attempted attacks, or blackouts.

While it will be some time before the Task Force determines the exact causes of the blackout, we know the system is vulnerable and we maintain a daily watch over what parts of the grid might be more vulnerable to attack because of system operations. We have conducted vulnerability assessments at electric power facilities, we have a protection strategy for key components, and we are working with industry and federal partners to determine the best way to implement that strategy.

Progress has been made, but the work is ongoing. I look forward to providing this committee and Congress with further updates.

This concludes my prepared statement and I would be glad to answer any questions you may have at this time.

Mr. CAMP. Thank you very much.
Ms. Swink?

STATEMENT OF MS. DENISE SWINK, ACTING DIRECTOR, OFFICE OF ENERGY ASSURANCE, DEPARTMENT OF ENERGY

Ms. SWINK. Chairman Camp, Vice Chairman Sessions and members of the committees, my name is Denise Swink and I am the Acting Director of the Office of Energy Assurance at the U.S. Department of Energy, a position I have held since March of this year.

At the Office of Energy Assurance, we contribute to the Department of Energy's efforts to ensure that America's homes, businesses and industries have a secure and reliable flow of energy. Our activities are designed to protect our critical energy infrastructure, detect problems quickly, mitigate the impacts of a failure attack, and recover rapidly from damage. We respond to a variety of potential threats including natural disasters, accidents, aging of system components and system reliability flaws.

As you know, our energy infrastructure is vast, complex and highly interconnected. It includes power plants, electric transmission and distribution lines, oil and gas production sites, pipelines, storage and port facilities, information and control systems and other assets. Many of these entities own, operate, supply, build or oversee their infrastructure. The private sector owns about 85 percent of these assets and a host of federal and state agencies regulate energy generation, transport, transmission and use.

Necessarily, our program uses a collaborative approach to coordinate all the various players and activities. Within the federal government, coordination efforts are with the Department of Homeland Security, the Department of Transportation, the Department of Defense, the EPA, FEMA, FERC and at least seven other offices within DOE. We assist in state-level emergency response planning and preparedness, working through a variety of state organizations.

For the private energy sector, a sector liaison has been designated for electricity, and one for oil and gas. We share information with key organizations in each of these sectors. On the international front, we have agreements with both Canada and Mexico to coordinate energy assurance across our borders. Several universities are helping us analyze specific physical and cybersecurity issues, and we have set up a laboratory coordinating council to coordinate at least 500 ongoing lab activities related to infrastructure protection.

Training is an important component for improving system resilience. That and energy infrastructure lesson plans are in development for various stakeholder groups, and databases and visualization tools are being assessed to monitor and understand energy infrastructure performance under various scenarios. All these coordination efforts help to provide an effective national response in the face of threats or disruptions to our energy infrastructure.

A review of the events that occurred immediately after the blackout will help to illustrate how we operate. On August 14, the department activated its Emergency Operations Center. Staff members were assigned to monitor, analyze and mitigate impacts of the

events. Regular staff briefings were held with representatives of FERC, Nuclear Regulatory Commission and DHS. And we place representatives at the DHS watch office and the FEMA control center. Our Emergency Operations Center continued to monitor impacts and calculate resources. Specialists looked at diesel fuel for backup generators, remedial actions for pipeline outages, refinery production availability, and associated cascading energy supply impacts.

Based on these analyses, DOE encouraged electric utilities to bring refineries in Ohio back online expeditiously, and we also coordinated dry route extension and fuel waivers for Michigan. Within hours after the blackout, the Secretary directed the New England and New York independent system operators to energize the cross-sound cable, an action that is believed to have prevented rolling blackouts in New York after electricity was restored.

On August 28, the Secretary indefinitely extended operation of the cable to benefit the transmission systems of New York and New England. Direct communications were established with state energy offices and state governors, while the DOE Office of Congressional and Intergovernmental Affairs issued status reports to Congress and responded to inquiries. To keep the public informed, DOE issued an August 14 statement about then blackout, and immediately posted information on its Web site. The Office of Public Affairs responded to hundreds of media calls and interview requests. The Secretary conducted multiple TV interviews on August 15 to 18 to report progress. As power was restored, the Secretary worked with state and local officials to urge citizens in affected areas to restrain their energy use until systems stabilized.

As you know, President Bush and Prime Minister Chretien established a joint U.S.-Canada task force to discover why the blackout occurred, how it spread, and to prevent a recurrence. The task force has been gathering and analyzing information on tens of thousands of events that occurred over 34,000 miles of transmission lines, and involved hundreds of generation stations, switching facilities and circuit protection devices. The investigation is being conducted through three separate, yet coordinated, working groups, electric system working group, the nuclear power group, and the security group. These groups, as Bob mentioned, are making progress. On September 12, the task force released the DTL time line of events that led to the blackout. This is an essential tool for reconstructing the events of August 14.

In summary, coordination among the many entities involved in our energy infrastructure is essential to help us prevent energy outages and ensure quick response and recovery if one occurs. Our planning and coordination efforts prior to August 2003 laid the groundwork for successful coordination after the blackout occurred. The time line released by the joint U.S.-Canada task force will allow the working groups to move forward in uncovering the root causes of the blackout. We are putting the puzzle together and proceeding as quickly as possible without sacrificing accuracy.

[The statement of Ms. Swink follows:]

PREPARED STATEMENT OF DENISE SWINK

My name is Denise Swink. I am Acting Director and Deputy Director of the Office of Energy Assurance in the U.S. Department of Energy, a position I have held since March of this year. The Office of Energy Assurance is responsible for leading the Department of Energy's effort to ensure a secure and reliable flow of energy to America's homes, businesses, industries, and critical infrastructures. Energy assurance addresses a variety of potential threats including natural disasters, accidents, terrorism, aging assets, system reliability, and cascading failures involving related infrastructures. DOE's Office of Energy Assurance addresses these threats using several strategies: protection of energy systems, detecting problems quickly, mitigating the impact of a failure or attack, and recovering rapidly from damage. We work in close collaboration with the Department of Homeland Security (DHS) and in partnership with the energy industry, state and local governments, and other federal agencies. Because of the importance of energy assurance, my Office reports directly to the Deputy Secretary of Energy.

The Office fulfills key federal responsibilities for energy assurance that date back to the origins of the Department of Energy. Selected legislative authorities include the Department of Energy Organization Act, the Federal Energy Administration Act of 1974, the Federal Power Act, the Public Utility Regulatory Policies Act of 1978, and the Robert T. Stafford Disaster Relief and Emergency Assistance Act. Many of these authorities address the powers and responsibilities of the Secretary of Energy during energy emergencies but some cover the broad responsibilities of the Secretary in ensuring that consumers have available an adequate and reliable supply of energy. The Office also fulfills federal responsibilities for securing and improving the energy infrastructure that are outlined in the President's National Strategy for Homeland Security and the President's National Energy Policy.

The Office of Energy Assurance focuses on six priority areas that address these responsibilities and respond to the findings of leading studies of the reliability of the energy infrastructure conducted over the past seven years and vulnerability assessments conducted after September 11,2001. The six focus areas are: 1) Energy Emergency Support and Management, 2) State and Local Government Support, 3) Criticality of Energy Assets, 4) Enabling Partnerships, 5) Technology Development and Application, and 6) Policy and Analysis Support. These are all critical elements of developing a balanced approach to our immediate energy protection needs and our longer term energy assurance needs.

The Nation's energy infrastructure is vast, complex, and highly interconnected. It encompasses a multitude of power plants, electric transmission and distribution lines, oil and gas production sites, pipelines, storage facilities, port facilities, information and control systems, and other assets that are integrated into our national energy system. This energy infrastructure is also the backbone for other critical infrastructures such as telecommunications, transportation, and banking and finance. In addition, there are a large number of entities that own, operate, finance, supply, control, build, regulate, monitor, and oversee our energy infrastructure. Eighty-five percent of the Nation's infrastructure is owned by the private sector. Regulation and oversight of energy production, generation, transportation, transmission, and use is governed by a host of federal agencies and states. As a result, a successful program in energy assurance must involve a collaborative approach that includes public-private partnerships to coordinate the various players and activities.

Coordination and collaboration are central principles of our approach to energy assurance. President Bush stated that homeland security is a shared responsibility that requires a national strategy and compatible, mutually supporting state, local and private sector strategies. This approach was embodied in the National Strategy for Homeland Security. The Department of Energy has lead federal responsibility for working with the energy sector in protecting critical infrastructures and key assets, in collaboration with the Department of Homeland Security. Two additional strategies, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace, expound on this responsibility and direct the Department of Energy to develop and maintain collaborative relationships with state and local governments and energy industry participants.

We work closely with the Department of Homeland Security, which leads, integrates, and coordinates critical infrastructure protection activities across the federal government. To aid this effort, DOE and DHS are in the process of developing a Memorandum of Agreement between the two agencies that will outline specific areas of collaboration and responsibilities. This encompasses critical infrastructure protection of physical and cyber assets, science and technology, and emergency response. We are also beginning to work with key parts of DHS, such as the Coast

Guard and the Federal Emergency Management Agency (FEMA), to determine how best to coordinate our efforts. For example, in July we attended a meeting which included representatives of DOE, DHS, the Defense Intelligence Agency, and the National Institute of Standards and Technology to consider options for developing a collaborative National SCADA Program. This program would help improve the physical and cyber security of supervisory control and data acquisition (SCADA) systems, which are used in the energy sector to remotely control and manage the flow of electric power and fuels throughout the energy infrastructure.

We also work with other federal agencies that have energy-related responsibilities. We work closely with the Department of Transportation's Office of Pipeline Safety to coordinate our respective efforts and identify areas for collaboration. We also coordinate with the Environmental Protection Agency (EPA) to avoid redundant efforts with petrochemical facilities. During the recent blackout, we assisted EPA in their review of Michigan's fuel waiver, which was ultimately granted. The waiver allowed the sale of 9 RVP gasoline in lieu of 7.8 RVP gasoline, which created more available resources for the State of Michigan and thereby prevented a possible gasoline shortage. We also partnered with several federal agencies (including the Federal Energy Regulatory Commission (FERC)), state regulators, and industry to assess the implications of a loss of natural gas supply to certain regions of the country. This study will help government policymakers and the natural gas industry to reduce the industry's vulnerability to terrorism, operational disruptions, and natural disasters.

Within the Department of Energy, we coordinate across a variety of offices:

- DOE's new Office of Electric Transmission and Distribution on issues related to the electric grid, most notably the recent blackout, which I will expand upon later;
- The Office of Security to improve the operations of DOE's Emergency Operation Center.
- The Chief Information Officer on the development of a joint facility to support continuity of operations;
- The Office of Energy Efficiency and Renewable Energy's regional offices to support our meetings With state energy offices;
- The Office of Fossil Energy on new technologies to harden oil and gas pipelines;
- The Office of Science on visualization techniques through their Advanced Scientific Computing Research Program; and
- The Office of Independent Oversight and Performance Assurance on cyber security protection.

Collaboration with the private sector is critical to improving energy assurance. As part of the President's strategy, we have designated "sector liaisons" to work with the electricity and oil and gas sectors. These liaisons in turn employ "sector coordinators" who function as DOE's primary interfaces on energy infrastructure security issues. DOE's sector liaisons share information and discuss coordination mechanisms with the American Petroleum Institute (API), the American Gas Association (AGA), the Interstate Natural Gas Association of America (INGAA), the Gas Technology Institute (GTI), the National Propane Gas Association (NPRA), the Edison Electric Institute (EEl), the Electric Power Research Institute (EPRI), the National Rural Electric Cooperative Association (NRECA), the American Public Power Association (APPA), and the North American Electric Reliability Council (NERC). For example, we are participating in NERC's Critical Infrastructure Protection Advisory Group and have briefed them on our activities related to electric reliability and cyber protection. We have had similar discussions on our oil and gas activities with API, which serves as the sector coordinator for oil and gas. To help create a strong business case for security investment, we are also collaborating on potential studies with the Council on Competitiveness.

States and local governments are also essential parts of energy assurance. They are responsible for emergency planning and response, and are the organizations that citizens turn to in times of crisis. We support a variety of state efforts to plan for, respond to, and mitigate actions that adversely affect the energy infrastructure and disrupt energy supplies. In the short time our program has been in existence, we have held several meetings with the National Association of State Energy Officials (NASEO), the National Governors Association (NGA), the National Association of Regulatory Utility Commissioners (NARUC), and the National Conference of State Legislatures (NCSL) to better understand how we can assist the states with emergency planning, emergency response tools, training and education, and elevating public awareness. We funded an NCSL study of energy security guidelines and options for state legislatures which was published in April 2003. We have addi-

tional efforts underway to develop model state guidelines for energy assurance plans and improved systems and procedures for multi-state coordination.

There are several other types of coordination underway which deserve mention. First and foremost, we tap the excellent scientific and technical resources of our national laboratories to address energy assurance issues. DOE has already identified over 500 ongoing activities in the national laboratories related to the protection of our Nation's critical infrastructures. We have also initiated a Laboratory Coordinating Council, representing all our major laboratories, to coordinate capabilities and activities related to infrastructure protection that can help meet our energy assurance challenges. We are also working with several universities on physical and cyber security issues. As part of our technology assessment efforts, we engaged Carnegie Mellon University to characterize needs related to vulnerabilities in the electricity sector. We are also exploring opportunities with George Mason University's Critical Infrastructure Protection Project. Our program is utilizing the greatest repository of physical structure engineering expertise—the International Union of Operating Engineers (IUOE). DOE and IUOE have begun development of energy assurance training curricula for energy infrastructure stakeholder groups, with initial courses offered by the International Union of Operating Engineers.

As the recent blackout demonstrated, our energy systems are interconnected with our North American neighbors. We cannot ignore the importance of coordinating energy assurance across our borders. Canada's electric grid is interconnected with the U.S. grid across our northern border and nearly all of Canada is an integral part of three of the ten NERC regions. As you know, we are currently working with Canada on the Task Force to investigate the cause of the blackout, which I will discuss in a moment. Although there are fewer electricity interconnections with Mexico, there are two small portions of Mexico that are also part of NERC regions. However, the United States also has bilateral agreements with Mexico under the Mexico-United States Critical Infrastructure Protection (CIP) Framework for Cooperation and the Smart Borders Initiative. In these, we agree to develop mechanisms for exchanging information on threats, sabotage and terrorist actions and provide coordination and cooperation in actions and measures to address detected vulnerabilities

The present concern of this Committee is how coordination works when a critical infrastructure fails, such as in the August 2003 blackout. I mention all these coordination efforts because I believe they provide the foundation for an effective national response for energy assurance.

Our process for helping others prepare for emergencies includes several elements. First, each electric energy provider is required to file an Emergency Incident and Disturbance Report when a system disruption occurs that meets certain criteria. An initial report must be filed within one hour and a final report within 48 hours. This allows DOE to be aware of potential major electric energy problems. Second, we provide active support for two Information Sharing and Analysis Centers (ISACs): the Energy ISAC (for oil and gas) and the Electricity Sector ISAC (for electricity). These ISACs provide a mechanism by which the industry can share important information about vulnerabilities, threats, intrusions, and anomalies among energy companies and provides a mechanism to communicate with the government The energy ISACs also coordinates with other ISACs. For example, during the blackout the Electricity Sector ISAC was in communication with the Telecom ISAC to monitor how electric problems might affect telecommunications. Our Office is coordinating with the energy ISACs and providing some financial support for their operation. Third, DOE participates in the Federal Response Plan through Emergency Support Function #12, Energy Annex. In the Plan, which is prepared by DHS/FEMA, DOE is the lead organization to gather, assess, and share information on energy system damage and impacts during an emergency.

Let me now review the events that took place immediately after the blackout occurred and explain how we coordinated within the Department, with other federal agencies, with the energy sector, and state and local governments.

On August 14, the Department's Emergency Operations Center (EOC) was activated with all relevant staff gathering there. Assignments were made regarding monitoring, analysis and mitigation of impacts of the event. Schedules were developed for convening status briefings. Federal Energy Regulatory Commission, Nuclear Regulatory Commission and Department of Homeland Security had a continual presence with their staff, too. DOE had representatives at the DHS Watch Office and FEMA Control Center, too.

The security of DOE's facilities was assessed, and it was determined that only the Brookhaven National Laboratory in New York was affected. For that facility, backup emergency power was available and increased security police personnel were called up and deployed. DOE's security activities were coordinated with the FBI, the National Joint Terrorist Task Force, and DHS.

With respect to monitoring of the event unfolding, an open phone line was connected to NERC. Market impact assessments were made continually. Determinations were made on availability of diesel fuel for backup generators. Availability of additional backup generators was researched, and commitments for delivery if needed were obtained. Pipeline outages were assessed to determine if remedial actions were required. Production availability of refineries was determined, as were associated cascading impacts of disruptions. These monitoring and assessment activities led to DOE intervening to encourage more direct support by electric utilities for bringing petroleum refineries in Ohio back into production, and ultimately coordinating drive hour extension and fuel waivers for Michigan.

On August 14, 2003, and only hours after the blackout occurred, the Secretary issued an order pursuant to his authority under section 202(c) of the Federal Power Act, directing the New England and New York Independent System Operators to energize and operate the Cross-Sound Cable. The Secretary issued the order because he determined that an emergency existed and that issuance of the order would alleviate the emergency and serve the public interest. Before issuing the order, the Secretary had received the unanimous recommendation of the North American Electric Reliability Council, the New York Independent System Operator (NYISO), ISO New England, Inc. (NEISO), and electric utilities in both New York and Connecticut supporting issuance of an emergency order.

The Cable was energized a short time after his order was issued. Within hours, it was delivering 300 MW of energy from Connecticut to Long Island and also providing valuable voltage support and stabilization services for the electric transmission systems in both New England and New York. It has been reported that operation of the Cable prevented rolling blackouts from occurring in New York in the hours immediately after electric service was restored.

On August 28, the Secretary issued another order that extended indefinitely the period that the Cross-Sound Cable could be operated. The August 28 order also directs Cross-Sound to continue providing voltage support and stabilization services, which benefit the transmission systems of both New York and New England. The August 28 order stated that ″it has not yet been authoritatively determined what happened on August 14 to cause the transmission system to fail resulting in the power outage, or why the system was not able to stop the spread of the outage.″ Because these questions have not yet been answered, the appropriate responses obviously have not yet been identified or taken. Therefore, the Secretary determined that an emergency continues to exist and operation of the cable should continue to be authorized.

With respect to State coordination, affected State Governors were contacted and an open communication process was established. Direct communications were established with State Energy Offices.

Letters to Members of Congress were written with the most current status information, and staff within the Office of Congressional and Intergovernmental Affairs were made available for inquiries from 8 AM to 8 PM each day. DOE staff was available for visits to Members' offices on request.

As part of the Department of Energy's response to the blackout of August 14, there were a number of public communications items. The Department issued a statement on August 14, coordinated by Deputy Secretary Kyle McSlarrow, noting that DOE had initiated its protocol for contingency situations. The statement noted that DOE was working with appropriate agencies including FERC, the Nuclear Regulatory Commission (NRC), FEMA, and DHS, as well as entities such as the North American Electric Reliability Council to assess the situation.

The Department immediately updated its website by adding a special section on its homepage with information related to the blackout. For example, all statements released from the Department were highlighted, as was general information on transmission grids and frequently asked questions on electricity. Reporters and the public often found answers to their questions. More than one reporter who called DOE's Office of Public Affairs noted the usefulness of the website information.

DOE's Office of Public Affairs answered hundreds of media calls and interview requests on August 14 and in the days following. An impromptu "blackout" media e-mail list was created for quick access to these reporters. In addition, the Secretary of Energy conducted multiple TV interviews from August 15 to 18 to communicate with the public on progress being made to resolve the blackout.

As power began to be restored, the Secretary of Energy issued a statement urging citizens of the areas affected by the blackout to use caution in energy use while the system was coming back on line. DOE worked with state and local officials on getting the message out that appliance use should be cut back until systems stabilized.

Following the blackout on August 14, President Bush and Prime Minister Chretien established a Joint US-Canada Task Force to investigate the cause of the

blackout, discover why it spread to such a large area, and determine ways to prevent any recurrence. Secretary Abraham and Canadian Minister of Natural Resources Herb Dhaliwal serve as Co-Chairs of that Task Force.

In addition to Secretary Abraham, the U.S. members of the Task Force are Tom Ridge, Secretary of Homeland Security; Pat Wood, Chairman of the Federal Energy Regulatory Commission; and Nils Diaz, Chairman of the Nuclear Regulatory Commission. In addition to Minister Dhaliwal, the Canadian members are Deputy Prime Minister John Manley; Kenneth Vollman, Chairman of the National Energy Board; and Linda J. Keen, President and CEO of the Canadian Nuclear Safety Commission.

The Task Force has an enormous job. From the first day, they've been in the field collecting and verifying vast amounts of detailed data from power generating plants, control facilities, utilities, and grid operators. In essence, they are busy gathering and analyzing information on tens of thousands of individual events that occurred over 34,000 miles of voltage transmission lines and involved hundreds of power generating units and thousands of substations, switching facilities, and circuit protection devices. The teams have been interviewing and collecting records on the numerous people, policies, and procedures that play a part in our complex power infrastructure.

The investigation is being conducted through three separate yet coordinated working groups focused on the Electric System, Nuclear Power, and Security.

The Electric System Working Group, led by experts at the Energy Department and the Federal Energy Regulatory Commission along with Natural Resources Canada, is focusing on the transmission infrastructure, its management, and its functioning.

The Nuclear Power Working Group, managed by the Nuclear Regulatory Commission and the Canadian Nuclear Safety Commission, is examining the performance of nuclear plants in the affected area during the blackout.

The Security Working Group, which is managed by the Department of Homeland Security and the Canadian government's Privy Council Office, is assessing the security aspects of the incident, including cyber security.

The good news is that these groups are making real headway. On September 12, the Task Force released a detailed timeline of events that led up to the blackout. This timeline is an essential tool for reconstructing the events of August 14 so that we can successfully understand exactly what caused the blackout.

The Electric System Working Group's assignment is challenging due to the sheer size and complexity of interrelationships among the diverse components of the electricity infrastructure. Recognizing the scope of this challenge, the Electric Systems Group has enlisted additional expert assistance. Technical experts with the Independent System Operators in the affected regions and with NERC are working with members of this group to determine how all the events are interrelated. They are also examining the procedures and control mechanisms that were designed to prevent a blackout from spreading from one area to another.

The Consortium for Electric Reliability Technology Solutions (CERTS), which has broad expertise in transmission and power delivery issues, is also assisting with Working Group. This team includes some of the world's top authorities on power system dynamics, transmission engineering and reliability, grid configuration, wholesale power markets, and outage recovery.

This group led the study of the 1996 blackout in the West and also helped DOE produce the comprehensive National Transmission Grid Study that recommended grid upgrades to meet transmission demands in the 2151 century. Transmission experts from the Bonneville Power Administration are also providing technical assistance.

The Security Working Group includes members from DHS, DOE, the National Security Agency, the United States Secret Service, the Federal Bureau of Investigation, and NERC. This group is examining whether a physical or cyber security breach contributed to the cause of the blackout.

The Security Working Group is working with the other Task Force Working Groups; developing an inquiry plan that articulates a detailed timeline for review of data including forensics, and interviews of company representatives to better understand each company's cyber topology; and working to obtain the detailed supporting data that will allow the team to better understand what caused, did not cause, or may have contributed to the events of August 14.

In summary, our vast energy infrastructure is built, managed, operated, regulated, and overseen by a large number of entities. Coordination among these stakeholders is essential to help prevent energy outages and ensure quick response and recovery if one occurs. The Department of Energy's planning and coordination efforts prior to the August 2003 blackout laid the groundwork for success coordination after the blackout occurred. The blackout time line released by the Joint US-Canada

Task Force will allow the working groups to move forward in uncovering the root causes of the blackout. We are putting the puzzle together and proceeding as quickly as possible without sacrificing accuracy.

Mr. CAMP. Thank you very much. Thank you both for your testimony.

Mr. Liscouski, I just have a couple of questions. I wondered what office or division played the lead role in responding to the events of August 2003, the blackout?

Mr. LISCOUSKI. Yes, sir. Within the context of DHS?

Mr. CAMP. Yes, within the context of DHS.

Mr. LISCOUSKI. The way the events unfolded, I would say the lead office was the IAIP office. We had the initial reports to our office about the blackout that enabled us to reach out to the private sector and to the sector at-large to get situational awareness around what was occurring. As soon as we were able to determine what did occur, we quickly coordinated with the other offices and directorates within DHS and the responsibility for that coordination moved over to the Homeland Security Operations Center.

Mr. CAMP. All right. Is that who also has the lead in assessing the causes of the outage and why? Or is that another part of the agency?

Mr. LISCOUSKI. No, sir. In the context of the Security Working Group, the Infrastructure Protection Office has the lead responsibility for that.

Mr. CAMP. I am interested in your thoughts on what would have happened if the power outage lasted longer. As you testified, there were a lot of other areas that were impacted. Clearly, airports had shut down, and even when some reopened with their generators, the Customs computers were down and flights were diverted to other cities. Water systems shut down and restaurants that were not even in the power outage area could not open because their water supply was not safe. Can you talk a little bit about what might have happened had it gone longer in terms of the impact on infrastructure and public health?

Mr. LISCOUSKI. Sure. In fact, we are in the process of doing the analysis right now. So at the top level, the assessment that I can provide to you is really based upon ongoing work. But I think it is fair to say that we had anticipated it. These types of events obviously occurred before, and we have a number of redundant systems in place, particularly in some of the critical areas such as telecommunications in which we are able to have redundancies that mitigate the effects of these longer-term types of outages.

I think you correctly point out the implications on immediate food supply and the potential there of what the implications might be. Fortunately, with the modeling we are doing we saw nothing catastrophic. Clearly, there were elements that were impacted. As we saw, the exchanges opened up shortly thereafter. So I think the positive result of our analysis so far is that many of the systems worked the way they were intended to do, providing more redundant capabilities and power with generation capabilities that allowed the systems to come back on fairly quickly.

Mr. CAMP. The Homeland Security Act of 2002 transferred the Department of Energy's energy security and assurance functions to DHS. How well has that integration proceeded?

Mr. LISCOUSKI. The integration has been working very well. The capabilities that were transferred over to DHS from the Office of Energy Assurance really provided us a baseline capability off of which we have leveraged significantly our ability to conduct vulnerability assessments across all the critical infrastructure. So it has really allowed us to build the capability within DHS that, as I indicated, we have leveraged across all those infrastructures. We continue to build our partnership with the Department of Energy's Energy Assurance Office.

Mr. CAMP. So with respect to the blackout of August 2003, how is your assessment on how that integration worked with regard to that incident?

Mr. LISCOUSKI. Very well. I think our internal skill sets that came to us from the Energy Assurance Office worked very well in understanding exactly how we had to respond to it and what types of questions and expectations we had as we outage continued to unfold. But I would say it is important to recognize that the real strength of what we have done is really the combination of other resources that came to DHS as well. So I would argue that if we did not have the elements from NIPC come to DHS, the elements of the NCS that came to DHS and the cyber components that we would have had as a stand-alone effort, they would have probably been within the same range of capabilities that they had if they remained at DOE.

But the combination of the resources we had among all of those elements between cyber and our ability to reach out to the sectors across sectors, really amplified our ability to respond and understand what was going on in those sectors and really put a plan forward. That was really the critical point here that I think in the past historically had not been within the capability. We didn't look at the event in a slice in time of the event occurring and that was all we were concerned about. The real advantage we had within DHS was the ability to keep one eye on that event and situational awareness to understand what was going on, but quickly also extrapolate from that event to how things may have progressed if in fact it were a terrorist event or how it might have been exploited if terrorists decided to take this as a target of opportunity, because we had people precisely looking at that going forward. That was a tremendous advantage which I would say did not exist before DHS came to be.

Mr. CAMP. Thank you very much.

Mr. Sessions, you may inquire.

Mr. SESSIONS. Thank you, Mr. Chairman.

I appreciate both of you being here today. I would like to direct my question, if I could, to Director Swink.

I know that the Energy and Commerce Committee has held any number of hearings concerning the blackout and what occurred. Today you are before the Homeland Security Select Committee. Are there lessons that we learned from this that you believe that together with the Department of Energy and Homeland Security that you believe we should learn as a recommendation from you that don't have to go through the processes of lawmaking and perhaps change things?

In other words, do you see something that we need to know perhaps today or will you be issuing a report that will say, "Here is something that happened, we need to change this rather quickly, and here are our recommendations"? Are you prepared at all today to address that?

Ms. SWINK. Yes, if I could make some comment. Actually, our table top, lessons learned, hardcore evaluation was set in our emergency operations center for tomorrow morning, but we have activated it to respond to the issues with the hurricane, so we will have to postpone it some. But I can just say that, one, clearly a couple of the areas that I know, and I believe it is the same thing with DHS, one of them is that we have to get much better at having monitoring information readily available to government agencies, not intrusive, but the information so we are not always on the phone calling people to find out what is happening. We actually have some very good monitoring data available to us. And there are capabilities out there, and we will be exploring those. In addition to that the ability to, as Bob was talking about, run some scenario analyses based on that. We were very concerned about the refineries being down, especially the two in Ohio, and being able to have a capability that accurately helps us understand the product movement from those refineries, what their feedstock concerns are. I think we have a ways to go to develop that set of databases as well as the level of knowledge to do those scenarios. By the way, our notion is to make those tools available throughout the United States, available to state organizations and nonprofit organizations also.

Mr. SESSIONS. Did part of your planning involve being notified by someone perhaps in Ohio, or on the actual site, to call someone to say, "We have problems; we want you to know this is not a terrorist attack; we think we know what it is," or did you have to initiate that call? In other words, was this part of the scenario, where they provided information to you from their basis, or did you have to seek that information to find out what had occurred?

Ms. SWINK. It was actually a combination. In some cases, we received calls. In other cases, we needed to call. But one of the things in working with state organizations that we have over the past several months, the state energy offices, the regulatory utility commissions, the state legislators, we are all working on developing a nationwide system that is a communications system that can aid the states, but also aid federal agencies in the energy area.

Mr. SESSIONS. From this member's perspective, I was very pleased. While I was not exactly aware of what was happening until probably they were in the midst of it, it looked organized. I believe that people came out very quickly and clearly and enunciated what we were looking at. I was very pleased to see up and down the line governors and other people who appeared to be working together, instead of pointing fingers, and were concerned about solving the problem. I must say that I felt like from the perspective of homeland security, I felt very good that Homeland Security, Department of Energy, as well as the White House at least were involved and active and seemed to have a handle on it.

I yield back my time.

Mr. CAMP. Thank you.

Ms. Sanchez may inquire.

Ms. Loretta SANCHEZ of California. Thank you, Mr. Chairman.

Mr. Secretary, on April 29 you briefed our subcommittee with respect to infrastructure and border security. In that slide, a PowerPoint presentation that you had, you outlined the department's goal to assess and compile a list of critical infrastructure vulnerabilities and to address 60 percent of the vulnerabilities in the list within 180 days. It has been four-and-a-half months since that date. Can you tell me, does there exist a single document that comprehensively assesses the nation's critical infrastructure risks and serves as a guide for us and for you in our efforts and as far as the spending program? And if not, when do you think that document is going to be ready? And in light of the 180-day time frame you discussed in the briefing, what progress have you made in assessing and addressing the 60 percent of the vulnerabilities?

Mr. LISCOUSKI. Thank you for the question. Actually, it is a good news story from my point of view. We really have made a significant amount of progress in addressing a lot of those vulnerabilities. I just want to clarify one point about that briefing. We really focused on some of the more critical ones that were first categorized during the Operation Liberty Shield, if you recall correctly. When the Iraq war started, we created a list, and this was just before I started with DHS, to identify some of those things that we thought were most critical to protect during the course of the war. That was the list that we referred to during the course of that briefing.

We have made some significant progress. I would be happy to share that with you in a written response downstream. But what we focused on were really a number of things during the course of that 180-day effort. As you recall, we were really focusing on how do we create DHS, you know, the IAIP director, the primary focus that I have been on all of a month, and we had to figure out what kind of business we were in. We were at war. We had a number of threats we had to respond to, and we had to build an organization. That was the primary focus, organizing ourselves around that war to really understand how we had to create an organization. And we have been moving out smartly on that.

We have looked at a variety of the critical infrastructure sectors to determine what practices had to be put in place. We did the vulnerability assessments. So, madam, I would say we are on track with the goals we set in that document.

Ms. Loretta SANCHEZ of California. So you are telling me that in a month and a half, we are going to have a list with all of the very critical infrastructure sectors and where that infrastructure is, and what type of protection we need to do for it, or how we are going to protect and what it is going to cost us, and a prioritization of that list so that we on this committee can figure out where we get the dollars and how we are going to do this over time?

Mr. LISCOUSKI. And I will shortly retire right after that, too. [Laughter.]

No. In fact, I was really referring to the Liberty Shield list. The other work in progress, and this is really an continuous work in progress, is the assessment of all the critical infrastructure throughout the United States. I did not mean to mislead you to think that we would have all that categorized in the next month

and a half. I would be surprised, frankly, if we had that done in the next 5 years. It is going to be an ongoing process. That is sort of peeling away the layers of the onion. The more you learn, the more you realize you do not know. Identifying the interdependencies among those critical infrastructures is also a body of work.

So no, ma'am, I am sorry to say we are not going to have that list in that period of time, but clearly we will have our processes in place so we can begin to move. We are doing that work now, but that will be an ongoing process. I do not think that will ever end.

Ms. Loretta SANCHEZ of California. What do you think are the most vulnerable infrastructure sectors and how do you make that determination? Do you do it asset by asset, regionally? Are you looking at it sector by sector? Can you give us some indication? I am sure you probably have this in writing somewhere and you will let us take a look at it.

Mr. LISCOUSKI. I think it is probably not fair to categorize one critical sector more vulnerable than another or more important than another. I think really there is a variety of contextual pieces here that have to be applied. The first is, what is the nature of the threat? The vulnerabilities really are contingent on the threat and your ability to negate those risks.

So rather than getting into a discussion about what I believe is the most vulnerable, I think we look at those and all the priorities, and we have work around identifying all those critical infrastructures. From our point of view, the nexus of what we do is constantly looking at threat information and then mapping those threats into the vulnerabilities we have identified.

At this point, we really are threat-driven. We are constantly turning over information we receive from the information analysis component and through the intelligence community. We are mapping those threats against what we have identified as those vulnerabilities. I think the end-state of where we would like to go is multi-pronged, from our point of view. We are trying to raise the bar across all the critical infrastructures and we want to get out of the threat-response mode and much more into the programmatic approach of saying we want to bake in good security processes across all critical infrastructure, irrespective of the threat so we really lower vulnerabilities across the board.

Ms. Loretta SANCHEZ of California. I know my time is up, but I am a little concerned about the fact that you said you are really threat-driven, because I hope this committee is not threat-driven and therefore we are really looking for less critical infrastructure, less vulnerabilities and a risk analysis so that we can decide where to put investment. I hope it is not because today they told us they were going to hit us in New York and tomorrow they are going to hit us in Alabama.

Mr. LISCOUSKI. If I may respond, I think it is worth clarification, and that is, again I will just remind the committee of the obvious here, that we have only been in business for 6 months. We have to respond to those things which we really do understand are being driven by factors outside of our control. But where we want to go at an end- state is really have a full understanding of all our vulnerabilities, and be much more focused on the vulnerabilities

and responding to the right remediation practices and best practices and not be threat-driven at this point.

Mr. CAMP. Thank you.

Ms. Dunn may inquire.

Ms. DUNN. Thank you very much, Mr. Chairman.

Welcome back, Mr. Liscouski. I had one question for you, actually two questions for you.

How effective were your interactions, do you believe, during this crisis in the Northeast? How effective was Department of Homeland Security in communicating with other agencies? What were your frustrations? What would you like to be able to do better and more quickly and more effectively?

Mr. LISCOUSKI. I think DHS responded very well and I think, you know, pridefully, because I was part of the process. I am not going to self-criticize too much, but I will be candid with you. I think we did a very good job communicating across federal sectors. I know our partners with DOE, as Ms. Swink pointed out, we had their members on our CAT team, on our Crisis Action Team. There were also at the Homeland Security Operations Center. So the benefit we have had was we did not have to establish communications with our federal partners during the event because we had ongoing communications with our federal partners prior to the event.

So that is the type of success story that I think DHS can tell very well. It is a continuous process. I would just emphasize the fact that we think about these things all the time, irrespective of whether there is an event or not. We are always in the mode of identifying what do we have to worry about. Because of that, we are in constant contact. So whether it is with DOE or EPA or whoever it might be, we are constantly engaged.

In terms of what we can improve better, there is always room for improvement. A continuous improvement process is what we are all about, particularly in a nascent organization such as DHS. So I think our own abilities to coordinate our processes, incorporating better technologies, as Denise pointed out, better visualization models, those things are process-oriented, but I think they are opportunities for fixes for us.

Ms. DUNN. This whole thing took place, and I had just given a speech a couple of days before on cybersecurity, cyberterrorism. One of the examples I used was how our power grid was linked into the Internet, and how it would be a target of vulnerability for terrorists. So 2 days later it happened, and I was watching with great interest as things happened on CNN. Very quickly, CNN came out and said that it was determined not to be a terrorist act. I am wondering, if you were involved in making that decision, how that decision was made and whether that is something that is still in flux and to be determined, or were we very quickly able to realize that it was not a terrorist act?

Mr. LISCOUSKI. I was a part of that process, but we relied heavily upon other partners in that process as well. The FBI, as you well know, and I think Larry Mefford testified last week about their involvement in that. So the combination between looking at the active investigation the FBI had ongoing, we did a very deep reach back as quickly as we could through our information analysis component, and through the intelligence community, to identify any

previous or existing threats that may have been out there. We looked at that. But the combination of the lack of intelligence about this, which from the world we come from that is not the final say, but the lack of physical evidence and any other attributes that we could identify as being related to criminal activity or terrorist activity allowed us to conclude at the initial outset that there was no nexus of terrorism or criminal activity. But to your follow-on question, clearly the ongoing analysis of the cyber-data and other information is what we are still in the process of collecting and analyzing to determine that conclusively.

Ms. DUNN. Dr. Swink, did you have any comment on that?

Ms. SWINK. The one comment on assessing the cyber area is that if you want to describe an area that has been working very well in a partnership, the DOE National Laboratory System has a lot of expertise in the cyber area, and we have been working very well under Bob's leadership of that working group.

Ms. DUNN. Good to hear. Let me ask you another question, Ms. Swink. All of us realize that there are interdependencies within the energy sector, as well as across infrastructure sectors. I am especially interested and concerned in how an attack on one center, such as on the power grid, could have serious effects on other critical infrastructure, such as our transportation system and communications systems.

Which interdependencies are the most vulnerable in your opinion? Are there hidden interdependencies that have not yet been focused on?

Ms. SWINK. The answer to the first question is that I don't think there is one that is most important. And to give you an example of answering the second part of your question, for the Olympics we did a table-top exercise in Salt Lake City for all of the infrastructures involved there, if there was a disruption there. And one of the things that came out that the telecommunications people had no understanding of was that they use a lot of water to cool their server stations. If the power went out in Salt Lake City, the availability of water pumped to their facilities to cool their facility would bring their server stations down.

So I think what is important is for us to continue to work on these scenario analyses and work on regional exercises and table-top exercises, because that is where you become more intelligent and more understanding of what these interdependency and cascading effects can be.

Ms. DUNN. Thank you very much.

Thank you, Mr. Chairman.

Mr. CAMP. Thank you.

Mr. Meek may inquire.

Mr. MEEK. Thank you, Mr. Chairman.

It is good to be here at this committee today. I had some of the same questions as it relates to this, and we had a hearing just the other day in another subcommittee talking about power outage and what actually happened. I noticed, Mr. Secretary, in your testimony as it relates to the phone service was limited. I wanted to ask where did that come from? Where did that evidence come from as it relates to phone service being limited?

Mr. LISCOUSKI. I am sorry. I am not so sure if I understand the question.

Mr. MEEK. I am sorry. I was reading your written testimony when you also stated here today that it was power outages. Television was at a limited basis, and also the telecommunications services were limited. How were they limited?

Mr. LISCOUSKI. If I recall correctly, and I can give you a more accurate answer in a written statement because we have done a lot of work on this. I recall the telecommunications system limitations really, Mr. Meek, I have to apologize. My sense is that some of the cell towers were out, and if I recall correctly, and again, I have a lot of data on this. I am just drawing a blank on the specific answer.

The things that we do in terms of assuring these services is what I can focus on with an immediate response in terms of the national communications system is particularly adept in working with the telecommunications industry to assure those services and assure that, as Ms. Swink pointed out earlier, that we have the appropriate fuel supplies going to the telecommunications providers for backup generators and things like that.

The initial outage I believe was related to that coming online. Again, I have to apologize. I will get back to you with a written answer.

Mr. MEEK. No problem. It is just one statement that you made. It goes to my question when we had our hearing the other day talking about telecommunications, and how it relates to communicating with the public when these things happen. I did make you aware of a piece of legislation that myself and many other members of the Congress are pushing as it relates to the ready-call bill, to make sure that individuals know what is going on when it is happening.

I can tell you, Ms. Dunn asked a question about how quickly we were able to excuse the issue of terrorist attack or an attack on our Internet capabilities or infrastructure, but I think it is important that we continue to push the private sector and also the public sector on the urgency. I am just kind of repeating myself yesterday, but since you are here today we have both agencies here. I think it is important that we remember that that is important while we are in somewhat calm waters. I know that there are going to be some task forces put together to make sure that that communicates from the private sector, and what homeland security has to do, what your agency has to do also towards moving us north. I look forward to working with you to that end.

I am very, very interested as it relates to our telecommunication capability in the time of homeland attack or what could be a potential attack in any geographical area to be able to communicate with Americans as expeditiously as possible and to be able to give good information and good intelligence that can be shared commonly with the private sector.

Mr. Chair, that completed my questions. Thank you.

Mr. CAMP. Thank you very much. The chairman of the full committee, Mr. Cox, may inquire.

Mr. COX. Thank you. I would like to welcome our witnesses again and add my gratitude to what you have heard from other members

for your time and the help that you are providing this committee in our oversight.

Mr. Liscouski, the Security Working Group is looking into a possible cyber-connection to the blackout. I take it that we use the words "cyber-connection" advisedly because we still want to include the small chance that there might be a bad actor, as well as simply mechanical or computer failure. Is that right?

Mr. LISCOUSKI. That is correct, sir.

Mr. COX. When do you expect that we will have an answer on that part of the investigation?

Mr. LISCOUSKI. I would like to report that it would be soon, but my fear is that it is going to take us quite sometime before we can come a conclusion.

Mr. COX. What does that mean? Ballpark?

Mr. LISCOUSKI. Probably several months. We are talking about 3 or 4 months, based upon the amount of data, which is really going to be dependent upon how focused we become on the initial root cause. Just at a top level, our process is really going to be geared at working with the electrical working group to identify root cause. Once we can identify the root cause of the issue, then we can begin to quickly look around at the surrounding causes that might be cyber- related.

In a classic investigation, if we are capable of doing that, we can potentially reduce our timeframe for the analysis. But if we have to look across all different platforms outside just a specific root cause area, then we are talking about terabytes of data through which we have to do analysis. That Is extremely time consuming.

Mr. COX. In addition to the cyber aspects, is this Security Working Group also looking at other means of bad actor, for example detonation of explosions, causes for the accidents or causes for the blackout?

Mr. LISCOUSKI. Yes, sir, we are looking at that as a component of it. Fortunately, those are more visible signs, but there are other potential causes that might be more physically oriented that we are examining as well.

Mr. COX. At the time that the country was assured that this was not a terrorist attack, my understanding is that it was the Department of Homeland Security that for the United States Government shared that information through the media. Is that correct?

Mr. LISCOUSKI. I believe that is correct, sir. Yes.

Mr. COX. And was that by prearrangement, or was that just how it happened?

Mr. LISCOUSKI. I don't recall exactly how that transpired. I can certainly get back to you with the sequence of events.

Mr. COX. I raise it because, first, it seems to have worked. Second, if it was just serendipity as opposed to a plan, then we can probably add this the list of lessons learned and make it part of the plan for next time.

Mr. LISCOUSKI. Yes.

Mr. COX. I suspect that there probably was some, if not total, fore-ordination of this because otherwise everybody would be trying to elbow their way to the front. And obviously, the Department of Homeland Security was created for this purpose. But as you can imagine, on the public side it is vitally important that people have

a clear answer from the USG. When we conducted TOPOFF II, we learned in an analogous way what happens when the Department of Energy was competing with the EPA about data concerning when the mayor can tell the public that the radiation is blowing your way or somebody else's way. We have to have somebody in charge. That was the lesson learned there. So from this real-life activity, it is very important that we recognize this seems to have worked. DHS took the lead role, and that should be institutionalized, if it isn't already.

Mr. LISCOUSKI. Yes, sir, if I may respond. The lack of conclusion I can provide you is my role during that course of the process was actively engaged and working with Secretary Ridge, and we were involved in the secure video teleconference with the FBI and CIA and State and the White House. During that discussion, we came to consensus on the determination. Unfortunately, I just wasn't present when the actual announcement was made.

Mr. COX. I understand, and I appreciate your undertaking to get that detail back to us. The two of you, or at least the departments that you represent, are working on an MOU. Is it the case that it is also you personally that are both working on this, or is it other people in the departments?

Mr. LISCOUSKI. No sir. It is our offices, I believe, in addition to our policy staff who are also working on agreements with DOE.

Ms. SWINK. We will cover the arrangements with the Science and Technology Office and the Emergency Response Office, too, but I believe that for this memorandum of agreement on critical infrastructure, the point will be Bob's office.

Mr. COX. And when do you expect the MOU will be completed?

Mr. LISCOUSKI. I would say it is ongoing, sir. I am not quite sure exactly what the time frame is going to be. What we are looking to do is looking at similar agreements we have to make with other agencies. Rather than just make one that we will have to make continuous adjustments for, our goal is to look at the commonalities for this agreement that would be applicable across all of the sectors.

Mr. COX. Ms. Swink, you testified that in real time you are also talking, for example, to NIST and DIA. Are you looking to execute parallel MOUs with them, or are you trying to roll that into the same agreement with the Department of Homeland Security?

Ms. SWINK. I know that our priority right now is to sort out the agreement with the Department of Homeland Security, and as Bob says, as much as possible create some model frameworks that all departments can look at with respect to developing that relationship. We have been sharing information actually for months on what should go into that type of agreement. As soon as that framework is there, there should be no reason at all that the other agencies don't become part of it.

Mr. COX. Thank you. My red light has gone on. I will just leave you with the question which is, Mr. Liscouski, the crisis action team that you set up in order to respond to the blackouts, which incorporated the infrastructure coordination division, national cyber-security division, protective security division and certain IA entities, was this ad hoc-ery or was this pre-planned? And to the

extent that it worked, which you testified that it did, is it something that we are going to institutionalize?

Mr. LISCOUSKI. Yes, sir. It is an institutionalized capability. The Homeland Security Operations Center is the focal point for coordination for incidents. All of the elements of DHS are represented on the HSOC, as well as the are components of our sister agencies who have response capabilities and proactive responsibilities as well. This is already institutionalized.

If I may, sir, just make one clarification with respect to MOUs. DHS, DOE, the other agencies with whom we work do not require an MOU to work going forward. There are all sorts of responsibilities for things that we have a very good understanding in terms of how we do work together. That is why the only clarification in terms of needing an MOU, our concern is, not concern, but working forward with other federal agencies. We believe we have a very good role and understanding based upon the Homeland Security Act and how DHS was formulated in the first place.

Mr. COX. Thank you.

Thank you, Mr. Chairman.

Mr. CAMP. Thank you very much.

Mr. Lucas may inquire.

Mr. LUCAS. Thank you, Mr. Chairman.

Mr. Secretary, in my district in Kentucky it has been ascertained that about 85 percent of our potential targets are in the private sector, like chemical plants and materials handling companies and things like that. Of course, they are in business to make a profit. They look to the bottom line. In your view, do you think that DHS relies too heavily on the voluntary private sector action to improve their infrastructure protection?

Mr. LISCOUSKI. No, sir, I don't. I believe appropriately the private sector needs guidance and needs to understand what the best practices are in the context of the threats that they face today. I do not believe the voluntary approach in the private sector is the inappropriate approach. Coming out of the private sector, I can tell you that it is something was always in the front of the minds of the corporations that I worked for. We did not need to be told necessarily how to do our work, but in the context of understanding the behaviors we needed to apply about what our responsibility was, was something we would engage with, and we consistently engaged with with the federal government. No, I believe the voluntary approach is the right approach.

Mr. LUCAS. Thank you. I relinquish the balance of my time.

Mr. CAMP. Thank you.

Mr. Weldon may inquire.

Mr. WELDON. Thank you, Mr. Chairman.

As my colleagues know, I come at these issues from the security standpoint of the Armed Services Committee and threats to our security.

Mr. Liscouski, you mention in your testimony that we are focusing on the issue to ensure that we can anticipate effects and prioritize our efforts based on the bigger picture, not just reacting to what is easily and immediately observed. Apparently, this blackout that we just experienced was caused by accidental incidents. We are putting into place processes to protect us from additional

accidental incidents. But a terrorist is not going to rely on that kind of capability, and my own feeling is that we are, if not totally, just about totally vulnerable to what I think is the biggest threat to both our power grid and to our information technology capability and our way of life.

I do not think we are prepared, and I am going to ask each of you to respond very specifically, in your agency, who has the responsibility to develop plans for us against what other nations have been planning to deliberately do if a nuclear war were to start? I am familiar with Russian nuclear doctrine. Their first attempt at attacking us would be to lay down an EMP burst off of our coast with a nuclear weapon that would not hurt one person, but would fry all of our electronic components, including our electrical grid system. It would shut down America, including our vehicles, that have chips in them that would stop on the roads.

Now, we tested this capability in 1962 when we did four tests at the Kwajalein Atoll in the Pacific. We were startled that within 800 miles everything was shut down, streetlights. We stopped cars dead in their tracks, and we fried the major electronic components of our telephone system. We did those tests in 1962. That is not classified. That has been reported in the media, and in fact it was just in a book put out by Dan Verton called "The Black Ice."

In 1999, we in the House held hearings on this phenomenon, not because of 9–11, but because we knew of the implications. Directed energy has become the weapon of choice for the future for nations that want to bring us down or harm us. We are doing research ourselves, and so are other countries on directed energy, let alone the EMP phenomenon. Who specifically and what department of both of your agencies has assessed and is responsible for protecting America from the standpoint of electromagnetic pulse lay-down and directed energy threats? Each of you.

Ms. SWINK. I will have to supply a more expanded answer for the record to get the level of detail that you are requesting. I will say that the DOE national laboratory system has been doing evaluations over the past year or more on the implications of EMP on SCADA systems themselves, supervisory control analysis data acquisition systems. At this point in time, there is a high concern for vulnerabilities, serious vulnerabilities. But with respect to exactly where in the department the leadership is for it, I will have to find that out for you.

Mr. WELDON. Mr. Liscouski?

Mr. LISCOUSKI. Mr. Weldon, in the context of Homeland Security, we have been studying this effort. I know there is an EMP commission. Our NCS, national communication system, has been working with the commission to study the effects. I am looking at some of the notes with respect to that. Modeling has been done with lightning strikes as a small- scale in understanding the implications of that. I know this is a big threat. We are taking it seriously. We are working with the commission to understand the effects of it. Our S&T organization is one that we have working with as well. So, no question, sir, it is a big problem.

Mr. WELDON. My problem is, Mr. Chairman, it is not mentioned in any of the testimony. The EMP Commission to which I assume

you are referring is actually a congressional commission that we created.

Mr. LISCOUSKI. Yes, sir.

Mr. WELDON. It is not a commission established by Homeland Security or the Energy Department.

Mr. LISCOUSKI. Yes, sir.

Mr. WELDON. The executive director of the commission is sitting in the room and he has had no contact with either of your agencies. To me, that is an indictment if we are supposedly preparing this country for what we call not just what is easily and immediately observed, but the bigger picture.

There is no more, no more threat to our security and our quality of life than a terrorist using electro-magnetic pulse, which we now have 10 countries that have nuclear capability. We are talking about low-yield weapons that would not harm one person. We detonate it in the atmosphere and we know 70 countries have missiles that could launch such a capability off of our coast.

We have tested this capability. We know what it does. My own feeling, Mr. Chairman and members of the full committee, is that we are not taking this issue seriously. We have no hardening of any of our systems in the country except for our ICBM system. That is the only hardening we have. I just think we have to start to raise the awareness. I congratulate the Congress, both sides, for establishing the EMP Commission. I introduced the executive director, Peter Prye, former CIA agent who is in the room. I would just say that I would think this distinguished panel ought to have more involvement with the agencies that are responsible for protecting us against the worst threats to our security.

Thank you.

Mr. CAMP. Thank you.

Mr. Dicks may inquire.

Mr. DICKS. Thank you, Mr. Chairman. I want to go back to this question about how we are doing our threat assessment, how we are cataloguing critical infrastructure. What is the responsibility of the states? Are the states asked to do a plan of critical infrastructure in their state, on a state-by-state basis? It seems to me, if we haven't approached this problem yet, which I think we should, that that might not be a bad way to do it. I mean, to come up with some criteria—here is what is important—and have the states fill it out, so they can give you their perspective of what is critical infrastructure in their states.

What is wrong with that? Or is it being done?

Mr. LISCOUSKI. Sir, in fact we are working very closely with the states. To your point earlier, or actually to Mr. Lucas's point, with respect to critical infrastructure being owned 85 percent within the private sector, 100 percent of it is in at the local level. The state and local governments with whom we work very closely are obviously responsible for helping us protect that and taking the lead in many ways in protecting that.

So we work very closely with them, and we have set up ways to begin. Again, this is a beginning effort. We recognize that this is clearly the beginning stages of DHS to develop this capability. But we are working with state and locals to develop training capabilities and to build their capacity to conduct vulnerability assess-

ments at the local level. This is not about DHS conducting vulnerability assessments for every single piece of critical infrastructure across the United States. We need our state and local partners. So to your point, sir, we are aggressively moving out on that.

Mr. DICKS. Well, it seems to me, and maybe we will have to legislate this, but somehow getting the states to do a plan which would include the assessment seems to be a very fundamental way to start, and the states have the joint terrorism task forces. They have the heads of the National Guard. The governors have their people who are working on these issues. It just seems to me that if we gave them a modest amount of resources and said do a plan for how you are going to handle critical infrastructure, and then work with your department, we might make some real progress and it would not take nearly as long. I think the state people know what is critical in their state, maybe even a little bit better that the feds do.

Mr. LISCOUSKI. Sir, I may not have been clear. I wanted to articulate we are exactly doing that.

Mr. DICKS. Okay, you are doing it?

Mr. LISCOUSKI. Yes, sir.

Mr. DICKS. Okay. Well, that is good. When do you think you will have these plans in place?

Mr. LISCOUSKI. Yes, sir, as I indicated, with our nascent effort. We are doing a couple of things, with building our organization and staffing up, as well as providing the capabilities out to the field. We are training state and local police agencies, law enforcement entities, on how to conduct vulnerability assessments, what the expectations are, basic standards and methods and how to do these things. This is an ongoing process.

Mr. DICKS. As you think about this, we have had hurricanes. We have had blackouts. These almost became like an exercise for DHS, for the department, the federal government, and FEMA. These things come along from time to time. In some cases, the catastrophic events are in some ways what would be very similar to what would happen in a terrorist attack. So it seems to me that maybe you take these events as they come along and it gives you a good chance to train your people, to really be prepared and to lay out your game plan for how you are going to deal with any catastrophic event. Obviously, we hope we will not have terrorist events, but at least it gives you some ability to train. Would you agree with that?

Mr. LISCOUSKI. Absolutely, sir. I do.

Mr. DICKS. We know we are going to have these kind of events. There is no way around it.

My staff tells me that California and New York have already done their plans, but DHS has not asked for them. Is that accurate?

Mr. LISCOUSKI. I don't believe so, sir. In fact, we are working closely with them.

Mr. DICKS. Why don't you check that out.

Mr. LISCOUSKI. I would be happy to.

Mr. DICKS. Ms. Swink, I have a question for you. This is a parochial matter. I hope my colleagues will forgive me just for a moment. I have been working for a number of years in the State of

Washington on a project called HAMMER. This is not named after the majority leader, by the way.

[Laughter.]

This is called the Hazardous Materials Management and Emergency Response Training and Education Center. This is a place where we do a lot of training. I understand that you are getting this turned over to you. Is that right?

Ms. SWINK. That is correct.

Mr. DICKS. I just hope you will take a very close look at this facility. I think for training first responders, National Guard, homeland security, this is an ideal facility. I just hope you will take a good close look at it.

Ms. SWINK. Mr. Dicks, I have been out and spent a couple of days at the HAMMER facility. It is an incredible asset, certainly, for what the Department of Energy sees needs to be done in the energy assurance area, but across the board. DHS actually has a border station there now. It is a major large prop training facility for which I think is going to be a tremendous asset.

Mr. DICKS. My time has run out, but I will do like the chairman did and leave you with one parting thought. I do not think that voluntarism is going to work. I think you are going to have to have some guidelines and some direction to the private sector.

Thank you.

Mr. CAMP. Thank you.

Ms. Jackson-Lee may inquire.

Ms. JACKSON-LEE of Texas. I would like to pursue a line of questioning with the Assistant Secretary for Infrastructure Protection. We had this line of questioning the day before yesterday about the assessments being made on the blackout. Is this the time for the report or are we still embargoed?

I think the question I was pursuing is what we have been able to determine by study and research on what happened and how you determined that it was not certainly a terrorist act, but it certainly was an infrastructure problem which can be equally disconcerting in light of the fact that out of that, horrible incidences can occur. So you delayed me in your response, and I am trying to find out now if this is the time or are we still doing the research?

Mr. LISCOUSKI. No, ma'am. In fact, I mentioned earlier we are in the process still of doing the analysis. This report is not going to be provided by the task force for a couple more months yet. I am afraid I cannot share the conclusions with you. We just don't have conclusions at this point.

Ms. JACKSON-LEE of Texas. When you say a couple of months, why don't you just project for me a basic timeframe on that.

Mr. LISCOUSKI. Ma'am, I am afraid I am not in charge of the time line for the publication of the report. I am contributing to the report to the task force. I would have to defer that to the task force leadership.

Ms. JACKSON-LEE of Texas. So you think, however, it is a couple of months?

Mr. LISCOUSKI. Yes, ma'am. I can tell you earlier Chairman Cox asked me about the analysis we are doing. The analysis we are conducting for the cyber investigation is quite involved and potentially may be even longer than that.

Ms. JACKSON-LEE of Texas. Let me try to find out the status of the DHS developing a comprehensive CIP risk assessment. Can you let us know where you are in doing that? And in your opinion, which of our critical infrastructure sectors pose the greatest national security concern?

Mr. LISCOUSKI. Yes, ma'am. In fact, since we started this effort with DHS back in March, as you know, we have been building the organization and simultaneously responding to threats posed to us by the Iraq war as our first order of business. The team did a great job in preparing protection plans to respond to the threats that were posed to us by the Iraq war, and then subsequently went on to the next effort of categorizing and identifying the critical sectors and the critical assets as part of our infrastructure protection plan.

That is an ongoing body of work. If we do this right, we will never be completed with it because if we are successful we will continue to identify the interdependencies of the critical infrastructure to uncover additional vulnerabilities. We are going to refine it. We have begun. As I have indicated, I have developed the capability to comprehensively begin this effort. We have begun the effort in earnest. I just will caution you that this is a very complex issue, one which DHS will be engaged with as federal partners and state and local and territorial partners for quite some time. So there will be no time line in which we will say we are finished. And in responding to the question concerning which are the most critical, I think you asked?

Ms. JACKSON-LEE of Texas. Yes.

Mr. LISCOUSKI. Again, it is in the context of we look at all 13 critical infrastructure components in the five key asset areas as they have been identified by the Homeland Security Act as just that, as critical. And really, we really look at them in the context of right now which are the most threatened, and we have a perspective on that, and we are continually culling the intelligence community for current threat information to identify those which require particular attention right now, as we are building capabilities. As you know, this critical infrastructure has been in the United States for quite some time, and we have never had a comprehensive look at protection of critical infrastructure as we have today with DHS.

So if the expectation is we will do this quickly, then we will not do it well. But I argue that we are really trying to take a very comprehensive look to put as many good security practices out there that are cost-effective, that are measurable and implementable by all aspects, not just the private sector, but by state and local governments as well.

This is an extremely complex issue. As DHS matures in its organization, when we are fully staffed over the next couple of years and develop our capabilities, I would be happy to get back to you with that answer. We are peeling this onion back and it is becoming more complex.

Ms. JACKSON-LEE of Texas. I do understand that. Let me just say, it looks like the light went from green to red. Is there a problem there? Let me just say, if you would, Mr. Chairman, because I was looking for the middle light there, and it did not light up, so I would ask you indulgence.

Mr. CAMP. Why don't you just proceed? Thank you.

Ms. JACKSON-LEE of Texas. I would appreciate it very much, Mr. Chairman.

Let me just say, there are a number of colleagues on this panel that are from New York, and I do want to express my admiration for New Yorkers in the tragedy of 9–11, and certainly they were very fortunate in the instance of the blackout. The television showed us tens of thousands of New Yorkers who had to walk across the Brooklyn Bridge to end their workday, and many other places and cities on that grid were experiencing the same. We can congratulate the people and the leadership of that area, but I would just emphasize the urgency of being able to respond more quickly than it seems that there might be an effort to do. I think this hearing is to emphasize the urgency. We have some serious concerns.

I end on the question of whether or not you are even looking at the individuals who can contribute to the vulnerabilities. I mentioned this yesterday. The young people, individuals at home can contribute to the vulnerabilities of cybersecurity. Because of that, because there is so much access to the cyberworld, to the Internet, it is I think imperative that we have sense of urgency and that we realize that any day something could happen that could be a catastrophe. I would hope that we would be able to have you before our committee again responding to the sense of urgency that I have just enunciated.

Mr. LISCOUSKI. May I respond? I would like to articulate that DHS clearly does have a sense of urgency about what we are doing. And if I have given you any indication that we don't, I apologize, because we are acting in an urgent way all of the time. We are continuously working at the most urgent requirements that we have. As I indicated yesterday, outreach and awareness program at all levels of government and the private sector and the civilian sector are clearly within our focus. I agree with you 100 percent that we have to educate all citizens of this country to what they can contribute to the effort to protect our homeland. Everyone here does have a responsibility for that. That is exactly the message we are trying to put out there. So I appreciate your support in that.

Mr. CAMP. Thank you.

Ms. Slaughter may inquire.

Ms. SLAUGHTER. Thank you, Chairman Camp.

One of the question, if I heard you respond correctly to Ms. Lee, was that you are not yet fully staffed in order to get the CIP finished. Is that correct?

Mr. LISCOUSKI. Ma'am, we are staffing as we speak. We are in the process of recruiting the best talent that we can. Part of that effort requires reaching out to the private sector where we can do that, and that requires us to get security clearances.

Ms. SLAUGHTER. How many professionals do you have now?

Mr. LISCOUSKI. To give you a ball park, in my office alone I believe we are probably in the number of around 200 and some-odd folks.

Ms. SLAUGHTER. How many do you need?

Mr. LISCOUSKI. Correct me if I am wrong. I would have to go back to an exact number, I think what we are staffing up for in

fiscal year 2004 is, within the Infrastructure Protection Office, approximately roughly 450 to 500 people.

Ms. SLAUGHTER. So you are only about half way there?

Mr. LISCOUSKI. For fiscal year 2003 we are pretty much on target. We are moving right along.

Ms. SLAUGHTER. Do the people that you hire already understand their own sectors and have the technical expertise in exactly what you need?

Mr. LISCOUSKI. That is precisely what we are hiring. It is technical expertise in those sectors, ma'am, yes.

Ms. SLAUGHTER. That is really disconcerting. I am disappointed that more than a month later we still don't know what happened on the power failure, just as I am disappointed that 2 years later we still don't know who mailed the anthrax. But let me just say something about pre-blackout. I was at Niagara Falls when this occurred. The first thing that we heard was that there had been a lightning strike at Niagara Falls. It was the most beautiful day we had all summer. But most of the events I would bet that contributed to it, occurred from noon to about 4:13 p.m. I think that is about the time our cell phones all went out, in any case. The generation and the transmission and the operating events all went down effective later in the day. The investigators I think are looking at what happened from 8 a.m. on that day, but we have not yet gotten any information on that. Is your office at all interested in that? Are you looking at that?

Mr. LISCOUSKI. Ma'am, as part of the Security Working Group we are looking at all aspects. We are working very closely with our other working group partners, sharing information. So we are interested in all aspects of the power outage.

Ms. SLAUGHTER. What concerns me is what Sheila Jackson-Lee had said. It could happen again any day, and the fact that we don't know why it happened on August 14 is very troubling to this point. Since the country seems to be willing to spend anything, do anything, go anywhere, the fact that we are still at this point, so to speak, in the dark I think is really quite troubling. We all understand that the grid had probably been neglected.

As a matter of fact, according to the Brookings Institution, the Bush administration ignores the major critical infrastructure in the private sector. In testimony before the committees on September 4, 2003, a witness from Brookings gave DHS "not a passing grade" on critical infrastructure protection. That was September 4, right after the blackout. At a recent Council on Foreign Relations homeland security event, former senior national security officials and senior state-level homeland security officials were asked to grade DHS on critical infrastructure protection, and the grades ranged from a D to a gentleman's C to another D to absent.

I wonder if you would care to respond to what appears to be a very negative assessment of what is going on at DHS and if you feel that part of that is because you are not yet staffed up or what are the problems.

Mr. LISCOUSKI. Yes, I would be happy to respond to it. Without knowing the specifics of those criticisms, I will just respond in a general way as well. I think perhaps there may be a lack of understanding of how complex this problem really is. I don't think any-

body has ever done this before in the context of the federal government, or anywhere, frankly, at the magnitude that DHS is doing that.

So we accept if there are valid, and there clearly are I am sure valid criticisms out there. We would like to learn how to do this better and we welcome those opportunities to learn how to do that better. You will find my management style is not one of arrogance or suggesting we know how to do it. In fact, if anything, we are looking to steal the best ideas from anybody that wants to tell us how to do these things so we can get the job done a lot better, and we are moving aggressively to do that.

And if we are at a C or a D right now, well, I am not suggesting I agree with that, but I would also suggest that we are doing a lot of work and we do need to do a lot more. I don't deny that for a moment.

Ms. SLAUGHTER. I have a lot of friends in the utility business who would like to give you some ideas on what they think.

Mr. LISCOUSKI. I would be happy to hear from them.

Ms. SLAUGHTER. They believe very strongly that the deregulation of electricity which required them to go out of generation of energy, and the fact that the people who were responsible for transmission lines did not keep them up and there was no incentive for them to do so, or actually were not told to do it specifically, which means to me that if we had it once, we are very likely to have it again.

Mr. LISCOUSKI. If I could just respond to that. That really sounds like a regulation issue and DHS is not a regulatory authority.

Ms. SLAUGHTER. I understand that, but nonetheless if you said you want to learn all aspects of it and find out what you think happened, that might be something that you might also have to look into.

Mr. LISCOUSKI. Thank you.

Ms. SLAUGHTER. Thank you.

Mr. CAMP. Thank you.

Ms. Christian-Christensen may inquire.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

Welcome back, Mr. Assistant Secretary. Welcome, Ms. Swink. I thank you, Mr. Liscouski, for remembering not only the states, but the territorial people in your comments.

Sorry for being late, but I did have a chance to look through your written testimonies. Assistant Secretary, I was impressed with the part of your testimony that talks about the DHS's responses that you described to the August 14 blackout. How much of that response happened just because the people on the ground knew what they were doing, or the people involved knew what they were doing from past experience? And how much do you think happened because there is a Department of Homeland Security? In other words, could we have done just as well in responding without the department being there? Do you understand the question?

Mr. LISCOUSKI. Yes, ma'am.

Mrs. CHRISTENSEN. How much of the response was really because we have an IAIP and a DHS?

Mr. LISCOUSKI. I would say it is all because we have IAIP. But practically speaking, and without being too glib, I do attribute our ability to respond well is because DHS does exist. The function that

IAIP represented was a good coordination point, as I described earlier in how events unfolded and what role IAIP played in that. Initially, as the blackout was becoming known to the community at large and came to our attention, IAIP coordinated with the sectors, the private sector, our federal partners, DOE, to determine exactly what was going on. We were able to do that fairly quickly, within an hour and actually even less, to understand what events were occurring and provide that information to the Secretary and subsequently to the White House very quickly to understand situational awareness.

The real discriminator in terms of what IAIP has provided to this effort that would not have existed if DHS not around was really the ability to look forward to the next step. I think clearly the capacity that DOE has and the experience that the folks have there, I readily admit that they would be able to adequately and ably handle this type of event. They are a tremendously experienced and talented group of professionals. But the distinction there is the fact that looking at the next event, in the context of without knowing if this was a terrorist event, and even with knowing that it was a terrorist event, DHS's responsibility was to look at what the next steps might be and how this event, how the blackout might have been exploited by terrorists or those who might have used this as an opportunity to conduct some sort of act.

We immediately progressed to that next level of thinking. The staff that I have working for me get paid to do that. We have scenarios based upon cyber events and electrical events, and other types of outages that we would say, okay, how could these events be exploited by terrorist groups? What do we know about the intelligence function? We were able to answer those questions and quickly put plans in place to prepare in the event that those scenarios were carried out. I think that is an incredible unique opportunity that the federal government has and that the American public has available to them by the creation of the DHS.

Mrs. CHRISTENSEN. Okay. You partly answered my next question, so I will ask a question to Ms. Swink. Moving to more information, technology dependent, and I hope this question was not asked already, smart grid is among the leading proposals to improve the capacity and reliability of the power grid. This would include replacing electro-mechanical switches with digital ones, and introducing real-time computer monitoring of the power lines. Would such changes increase the cyber-vulnerabilities of the power grid? If so, how should we balance the increase vulnerability with increased power grid performance and reliability?

Ms. SWINK. With business as usual, I would say that it would increase the vulnerabilities. But because of a lot of good work being done in the government labs, as well as the private sector, a much better understanding of how those new systems and devices need to be designed with authentication procedures, cryptography, immediate recognition of assaults by viruses, et cetera, we are well on the way of having the tools and mechanisms to build that system so that it is responsive and not vulnerable.

Mrs. CHRISTENSEN. So you think that because we are much more aware of some of the vulnerabilities, we will be able to address some of what might have otherwise been increased vulnerabilities?

Ms. SWINK. Yes.

Mrs. CHRISTENSEN. Okay. I guess I could ask this to either one. Well, my time is up. I will wait for the next panel.

Thank you, Mr. Chairman.

Mr. CAMP. Thank you.

As this is a joint hearing held with the Cyber Subcommittee, I will turn the gavel over now to Congressman Sessions.

I want to thank both of you for your attendance here today and for your very insightful testimony, and I appreciate your being here. We will move to our second panel. I want to thank you again.

Again, I will turn the panel over to Congressman Sessions. This is a joint hearing with the cyber subcommittee, and he will chair this second panel in today's joint hearing.

Mr. SESSIONS. [Presiding.] I thank the gentleman.

Local governments are responsible for coordinating the states's response to a wide range of emergencies and disasters, both natural and manmade. Local law enforcement, fire, public works and emergency medical agencies and personnel are being trained in how to properly respond to potential terrorist incidents. The blackouts tested the training and response capabilities of our first responders.

Colonel McDaniel is here today before us and he will provide an overview of the events that occurred in Michigan during the blackout. Also today we have Mr. Robert Dacey, Director of Information Security Issues for the Government Accounting Office. GAO has made numerous recommendations over the last few years related to information-sharing functions that have been transferred to the Department of Homeland Security.

One significant area concerns the federal government's critical infrastructure protection efforts, which has been focused on the sharing of information on incidents, threats and vulnerabilities and the providing of warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector. Today, we are prepared to hear from Mr. Dacey, and he will offer recommendations for strengthening the information-sharing and other critical infrastructure protection capabilities.

At this time, I would like to begin with Colonel Michael McDaniel from the State of Michigan.

STATEMENT OF COLONEL MICHAEL McDANIEL, ASSISTANT ADJUTANT GENERAL, HOMELAND SECURITY, STATE OF MICHIGAN

CoLonel MCDANIEL. Thank you, Chairman Sessions, Chairman Camp, members of the committee, for this opportunity to testify before you here today.

My name is Colonel Michael MCDANIEL. I serve as the Assistant Adjutant General for Homeland Security for the Michigan National Guard, and as such I also serve as the governor's adviser on homeland security to Michigan's Governor Jennifer Granholm.

Based on my understanding of the focus of this committee's interest, my narrative of events of August 14 through 16, 2003 will focus on the interdependencies of the infrastructure, the responses thereto and the communications between state, local and federal

agencies. I will then briefly discuss some of the issues that surfaced during our response to the blackout and potential resolution of them.

As you all know, on Thursday August 14, 2003 in the late afternoon approximately at 4:15 p.m., a massive power outage struck the power grid in the Midwest and Northeast U.S., as well as the Province of Ontario, causing blackouts from New York to Michigan. Within minutes, much of southeast Michigan and mid–Michigan was without power, including the major metropolitan areas of Detroit, Ann Arbor and Lansing.

I will briefly outline some of the major complications from the blackout. In much of southeast and mid–Michigan, the lack of electrical power resulted in widespread traffic signals not functioning, and limited telephone communications. Radio and television stations reported broadcasting difficulties, with several small stations not operating at all. Gas stations were unable to supply people's needs for their cars and for their portable generators, as without electricity those gasoline pumps were inoperable. The auto industry in Michigan was also directly impacted by the loss of power, shutting down operations for the majority of 3 days.

The Ambassador Bridge in Detroit, the busiest commercial land port in the United States, with 16,000 tractor-trailer trucks crossing daily, was also affected. This resulted in approximately a 4-mile backup of traffic for almost 24 hours on the United States side. I would just emphasize that it was the IT systems for the Canadian Customs that was shut down and not functioning. The U.S. Customs system at the bridge was working.

Many other computer systems were not functioning, however, including the Law Enforcement Information Network, or LEIN system. The Detroit Board of Water and Sewer, which is the oversight board for the nation's second or third largest water system, reported its system was not functioning correctly. It had a boiled water advisory which was not lifted until late Monday, August 18. The state's response in brief. As of 6 p.m., Governor Granholm had reported to the state emergency operation center. I would note that the Governor spoke directly with Department of Homeland Security Secretary Tom Ridge approximately 1 hour after the blackout began. As the dimensions of the emergency became clear, the federal DHS called every hour for briefings. The FEMA representative was also present and working from the state's EOC from August 15, the next day, onward. The state of emergency was not rescinded until a few days later.

Briefly, the lessons learned. In Michigan, we are monitoring, investigating or resolving the following issues. First, the communications between federal and state agencies. I think it is safe to say there was full and robust communication between the appropriate federal and state agencies, but I would make a couple of suggestions for improvement. First, we were giving reports to the Department of Homeland Security directly, to FEMA or the EP&R directorate within DHS, and then to FEMA Region 5. To a large degree this was redundant information.

Secondly, all of those communications were being made by telephone or facsimile machine. And given the intermittent outages of commercial telephone service elsewhere in the state, as well as in

the Lansing area for the first 8 hours, a backup system needs to be instituted that is not reliant on commercial lines or on portable generators.

Secondly, the communications between state and local agencies worked very well. I would go so far as to brag a little bit and say they worked flawlessly. I think this was in large part because we had a substantial investment in the State of Michigan over the last 12 years of approximately $220 million to create a statewide 800 megahertz digital trunk radio system. As a result, there were no interruptions in the system anywhere as the control system in all 180 towers have their own independent generators.

I would note a couple of points, however. The state had to issue bonds to fund such a large expenditure. The IRS has ruled, however, that because these are state bonds, only 5 percent of the members of the system can be non-state agencies. We do have a number of federal agencies who have radios on the system, including FBI, Bureau of Alcohol, Tobacco and Firearms, and the U.S. Forest Service. However, because of that 5 percent, we are limited in the degree to which we can request and ask the federal agencies to come on that system. Consideration should be given to creation of an exception to the IRS bonding restriction to promote interoperability of communications between state, as well as non-state agencies.

I would also like to talk briefly about interdependent infrastructure. We had questions from Congressmen Dicks and Lucas about the critical infrastructure protection and coming up with systems and inventories of those. I would just say that everybody has their own list of critical infrastructure protection, but what we need to do is have a process whereby those lists are not just inventoried and compiled and harmonized, but we need to have a strategic assessment.

The Office of Domestic Preparedness has asked the states to do that, and we are in the process of doing that. A strategic needs assessment of the state is to be done no later than December 31. All states have to do the same process. At that time I think we will have the next step in a critical infrastructure protection that is truly a national plan, not just a federal plan or a state plan.

Lastly, I would just mention the sufficiency of funds for state emergency operations centers. In some regards, the Department of Homeland Security has done very well in getting us funds for equipment and getting those down to the state. However, I would note that there was a fiscal year 2002 supplemental appropriation for statewide emergency operation center upgrades and modifications and we have still not had an answer or received funding on that.

I thank the committee for this opportunity to testify. I welcome any questions you have after Mr. Dacey.

[The statement of Colonel McDaniel follows:]

PREPARED STATEMENT OF COLONEL MICHAEL C. MCDANIEL

Thank you, Chairman Thornberry, Chairman Camp, and Members of the Committee for the opportunity to testify today before your committee.

My name is Colonel Michael C. McDaniel, and I serve as the Assistant Adjutant General for Homeland Security for the Michigan National Guard. As such, I serve as the Homeland Security Advisor to Michigan's Governor, Jennifer M Granholm.

Based on my understanding of the focus of this committee's interests, my narrative of the events of 1416 August, 2003 will focus on the interdependencies of our infrastructure, and the communications between state, local, and federal agencies. I will then discuss some of the issues that surfaced during our response to the blackout, and potential resolution of them.

On Thursday, August 14,2003, at approximately 4:15 p.m., a massive power outage struck the Niagara-Mohawk power grid in the Northeast US and Ontario causing blackouts from New York to Michigan. Within minutes, much of southeast Michigan and mid-Michigan was without power, including the major metropolitan areas of Detroit, Ann Arbor, and Lansing.

Approximately 60 percent of Michigan's entire population, or more than 2.2 million households, was affected by the outage, requiring state agencies and local governments to utilize extensive emergency protective measures in order to insure their health, safety and welfare.

Collectively, the State of Michigan and local governments expended $20.4 million on emergency measures to save lives, protect public health, and prevent damage to public and private property.

The Emergency Management Division of the Michigan State Police began to immediately monitor conditions in Lansing and around the state, including the state's nuclear power plants. Within minutes, when it was clear that there was a widespread outage, the state's Emergency Operations Center (EOC) was formally activated, and state agencies began to monitor state and national conditions.

Below, I will briefly outline some of the major complications from the blackout:

- In much of southeast and mid-Michigan, the lack of electric power resulted in widespread traffic signals not functioning and limited telephone communications. Radio and television stations reported broadcasting difficulties, with several small stations not operating at all.
- Many facilities lacked sufficient alternative energy sources. Portable generators were needed at hospitals and other public facilities, including the state mental institution.
- The Fermi II nuclear plant in Monroe County was shut down as a precaution. It returned to full power production and was reconnected to the power grid late Thursday, 21 August.
- Marathon Refinery, Michigan's largest refining facility, lost power and had to shut down. One unit did not shut down properly and began venting partially processed hydrocarbons. Because of the tank's location, the city of Melvindale (with the assistance of the Michigan State Police) decided to evacuate 30,000 residents and shut down Interstate 75 for several hours until the situation was controlled. The Marathon Refinery was inoperable as a result of the loss of electricity and water, and out of production for approximately 10 days.
- Gas stations were unable to supply peoples' needs for their cars and portable generators, as without electricity the pumps were inoperable.
- The auto industry was also directly impacted by the loss of power, shutting down operations forthe majority of three days.
- The Ambassador Bridge in Detroit, the busiest commercial landport in the United States with 16,000 tractor-trailers crossing daily, was also affected. Interestingly, both the bridge and U.S. Customs had their computers interrupted only momentarily until their back-up systems activated. Canadian customs, however, lost their computer datalink, and thus their ability to verify trucking manifests electronically. As a result they were forced to visually and manually inspect the manifests and, if warranted, the freight itself. This resulted in an approximately four-mile backup of traffic for almost 24 hours on the U.S. side.
- Many computer systems were not functioning, including the Law Enforcement Information Network (LEIN).
- Metropolitan Detroit Airport was closed and all flights canceled until midnight on August 14.
- The Detroit Board of Water and Sewers, oversight board of the nation's second largest watersystem, reported that its system was not functioning correctly. It issued a boiled water advisory for its entire service area. A number of public water issues arose from the blackout. First, there is a need for generators and for an automatic activation switches for these generators. Second, much of the system's gauges and switches rely on telephone lines, or telemetry, which is used to receive information on the system's capabilities. Last, there was no system to notify all of the customers of the boiled water advisory, as notification was dependent on the public media. It became clear, on the morning of August 15, that the largest problem was the lack of potable water. Public and private entities delivered hundreds of thousands of gallons of water to those affected sites, but a boiled water advisory was not lifted until Monday, August 18.

The State's Response

As of 6:00 p.m., Governor Granholm and her senior staff had reported to the state Emergency Operations Center (EOC). The Governor had been briefed by the Emergency Management Division of the Michigan State Police (MSP), and all state agency representatives, and she first advised the citizens of conditions and our efforts via public media, at approximately 10:00 p.m. The MSP had positioned 50 state troopers on stand-by for mobilization, if needed to maintain order in blackout areas. Little to no looting was reported, and crime rates were at or below average. The Michigan National Guard also had troopers ready on stand-by.

I would note that the Governor spoke with Department of Homeland (DHS) Secretary Tom Ridge approximately one hour after the blackout began. As the dimensions of the emergency became clear, the federal DHS called every hour for briefings.

The State of Michigan has always had a great working relationship with FEMA Region V, and this working relationship was very evident during this emergency. Region V had activated their Regional Operating Center (ROC), and was in close and constant telephone contact. A FEMA representative was also present and working from the State EOC, from August 15 onward.

The state of emergency was not rescinded until August 22, 2003.

Emergency Protective Measures Reimbursement

On August 27,2003 the State applied to FEMA for federal reimbursement under the Stafford Act' for actions taken by local or state agencies to remove or reduce immediate threats to public health, safety, welfare, or private property when those measures are used in the public interest. As of September 15, we have not received any response from FEMA. This is not an inordinately long period of time, but Michigan and other states are watching to see if the placement of FEMA within the Emergency

Preparedness and Response Directorate (EP&R) of DHS will prolong the application process. I would note that the Undersecretary for EP&R has assured the state emergency management directors that it will not.

Lessons Learned

In Michigan, we are monitoring, investigating, or resolving the following issues:

(A) Communications between federal and state agencies. There was full and robust communication between the appropriate federal and state agencies. DHS and FEMA were in regular, consistent contact with the State EOC. The State Department of Environmental Quality, Public Service Commission and National Guard were communicating with the Environmental Protection Agency, the Department of Energy, and the National Guard Bureau, respectively. Two suggestions for improvement, however, can be made. First, the reports given to DHS and FEMA Region V were redundant information. While the "operations tempo" of the emergency response was such that this was not a hindrance, this redundancy should be eliminated as the reorganization of federal agencies within DHS is completed. Second, all communication was by telephone or facsimile machine. Given the intermittent outages of commercial telephone service elsewhere in the state, a backup system needs to be instituted that is not reliant on commercial lines. I would note that there is a wireless system between FEMA Region V and the State EOC. Perhaps this capability can be expanded.

(B) Communications between state agencies and between state and local agencies. Internal communications, both within a state agency and between employees of the state and a local agency, worked flawlessly. The State of Michigan, over the last 12 years has spent in excess of $220 million to create a statewide 800 Mhz digital trunk radio system. It is the believed to be the largest radio system, in terms of land mass covered, in the nation that meets APSCO 25 (Association of Public Safety Communications Officials) standards. This system provides full interoperability, of course, as all members are on the same system. There are at the present time 374 different public agencies which use the Michigan Public Safety Communication System as their primary radio communications, and another 90 agencies that use the system for emergency management purposes only. The member agencies include all state agencies, as well as counties, townships, tribes, and federal agencies (the FBI, U.S. Customs, Bureau of A TF and Forest Service). There are currently more than 11,000 radios on the system.

There were no interruptions to the system anywhere during the blackout because the control center and all antennae have independent generators. Four of the five counties as well as many municipalities within those counties in the declared emergency area are now considering joining the Michigan Public Safety Communications System.

During FY 2003 the DHS administered an equipment grant program to promote interoperable communications between local governmental agencies. The states expect to learn the grant recipients and amounts awarded in the near future. This program, by providing a specific financial incentive to pursue interoperability, has been well-received by the States. This program and its results should be monitored closely and considered for potential expansion.

Because the state had to issue bonds to fund such a large expenditure, the Internal Revenue Service (IRS) has ruled that with state bonds only 5 percent of the members of the system can be non-state entities, or, in this case, federal or tribal members. While far less than 5 percent of the radios on the system are used by federal agencies, true interoperability compels their participation on the system. We need to find means to encourage federal participation on the MPSCS, thus consideration should be given to creation of an exception to the IRS bonding restriction to promote interoperability of communications between state and non-state agencies.

(C) Interdependent Infrastructure. The above narrative illustrates the ripple effect of an impact on one sector for the rest of the nation's infrastructure. The facilities, systems, and functions that comprise our critical infrastructures are highly sophisticated and complex. We are only now beginning to study the degree that our systems work together in processes that are highly interdependent. In one oft-cited example, e-commerce depends on electricity as well as information and communications. Assuring electric service requires operational transportation and distribution systems to guarantee the delivery of fuel necessary to generate power. Such interdependencies have developed over time and are the product of operational processes that have fueled unprecedented efficiency and productivity.

Given the dynamic nature of the systems, we need not only to model but also a concerted, joint state/federal effort to identify and prioritize not just the systems, but their critical components, their interdependencies, and the state and federal agencies that both regulate and rely on them. In the past, different state and federal agencies have inventories and prioritized the critical infrastructure. This process is ongoing, it is a vital step for every operational plan for protection and security, and those priority lists are driving our efforts.

(D) Sufficiency of funds for state Emergency Operations Centers. Deficiencies in the state Emergency Operations Center become obvious after spending 36 straight hours there. The FY 2002 Supplemental Appropriation provided approximately $51 million nationwide specifically for Emergency Operation Center upgrades and modifications. This amount is insufficient to properly upgrade the Emergency Operations Center for every state and territory. For example the State of Michigan had requested $9.5 million for this purpose, which would include all design, engineering, construction, and project management costs for the State EOC, and an alternate EOC in the metro Detroit area. A decision on the grants is long overdue, particularly considering that some state, somewhere in the nation, is facing an emergency, albeit usually natural emergencies, such as floods, fires and hurricanes, almost every day.

I thank the Committee for the opportunity to testify, and I welcome any questions you may have.

Mr. SESSIONS. Colonel McDaniel, thank you so much. Your request to us concerning the tax implications will be not only acknowledged by this committee, but we will also provide you back in writing what we intend to do as far as referring that. We have several members, including the gentlewoman from Washington, who sit on the Ways and Means Committee and would be able to address that properly.

Thank you so much.

Director Dacey, you are recognized.

STATEMENT OF MR. ROBERT DACEY, DIRECTOR, INFORMATION SECURITY, GENERAL ACCOUNTING OFFICE

Mr. DACEY. Chairman Sessions, Chairman Camp, and members of the subcommittee, I am pleased to be here today to discuss the Department of Homeland Security's information- sharing responsibilities, particularly as they relate to critical infrastructure protection, or CIP, and the challenges and key management issues

that the department faces in implementing those responsibilities. As you requested, I will briefly summarize my written statement.

The Homeland Security Act of 2002 brought together 22 diverse organizations and created a new Cabinet-level department to help prevent terrorist attacks against the United States, reduce the vulnerability to terrorist attacks, and minimize damage and assist in recovery from attacks if they should occur. Achieving the complex mission of the department will require the ability to effectively share a variety of information among its own entities and with other federal agencies, state and local governments, the private sector and others.

For example, the department will need to be able to access, receive and analyze law enforcement information, intelligence information and other threat incident and vulnerability information from federal and non-federal sources; to administer the Homeland Security Advisory System and provide specific warning information and advice on appropriate protective measures and countermeasures; to share information both internally and externally with agencies in law enforcement on such things as goods and passengers in- bound to the United States and individuals who are known or suspected terrorists or criminals; and to share information among emergency responders in preparing for and responding to terrorist attacks and other emergencies.

GAO has made numerous recommendations over the last several years related to information-sharing functions that have been transferred to the Department of Homeland Security. A number of actions have been taken or are underway to improve information-sharing, such as the department's recent announcement of the creation of the U.S. Computer Emergency Response Team, or CERT, to provide in part a coordination center that links public and private response capabilities.

However, further efforts are needed to address several information-sharing challenges concerning the government's CIP efforts. These challenges include developing a comprehensive and coordinated national CIP plan to facilitate information-sharing that clearly delineates the roles and responsibilities of federal and non-federal entities, defines interim objectives and milestones, sets time frames for achieving them and establishes performance measures.

Two, developing fully productive information-sharing relationships within the federal government and between the federal government and the state and local governments, the private sector and others.

Three, improving the federal government's capabilities to analyze incident, threat and vulnerability information and share appropriate, timely and useful warnings and other information concerning cyber and physical threats.

And four, providing appropriate incentives for non- federal entities to increase information sharing with the federal government and to enhance other CIP efforts.

Success of homeland security also relies on establishing effective systems and processes within the department to facilitate information-sharing. Through our prior work we have identified several critical success factors and other key management issues that the department should consider as it establishes systems and processes

for information sharing. For example, the department should continue its efforts to develop and implement an enterprise architecture to integrate the many existing systems and processes required to support its mission and to guide the department's investments in new systems to effectively support homeland security in the coming years.

Two, to implement effective system acquisition and investment management processes to appropriately select, control and evaluate IT projects. And third, to implement effective information security to protect the sensitive information that the department maintains and to develop secure, available communication networks to safely transmit information.

Other key management issues include developing a performance focus, integrating staff from different organizations and ensuring the department has properly skilled staff.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you have.

[The statement of Mr. Dacey follows:]

PREPARED STATEMENT OF MR. ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY, GENERAL ACCOUNTING OFFICE

INFORMATION SHARING RESPONSIBILITIES, CHALLENGES, AND KEY MANANGEMENT ISSUES

Messrs. Chairmen and Members of the Subcommittees:

I am pleased to be here today to discuss the challenges that the Department of Homeland Security (DHS) faces in integrating its information gathering and sharing functions, particularly as they relate to fulfilling its critical infrastructure protection (CIP) responsibilities. CIP involves activities that enhance the security of the cyber and physical public and private infrastructures that are essential to our national security, national economic security, and/or national public health and safety. The Homeland Security Act of 2002 brought together 22 diverse organizations and created DHS to help prevent terrorist attacks in the United States, reduce the vulnerability of the United States to terrorist attacks, and minimize damage and assist in recovery from attacks that do occur. To accomplish this mission, the act established specific homeland security and CIP responsibilities for the department and directed it to coordinate its efforts and share information among its own entities and with other federal agencies, state and local governments, the private sector, and others.

In my testimony today, I will summarize our analysis of information sharing as an integral part of fulfilling DHS's mission and CIP responsibilities. I will then discuss our related prior analyses and recommendations for improving the federal government's information sharing efforts. Last, I will discuss the key management issues that DHS should consider in developing and implementing effective information sharing processes and systems.

In preparing this testimony, we relied on prior GAO reports and testimonies on combating terrorism, critical infrastructure protection (CIP), homeland security, information sharing, information technology (IT), and national preparedness, among others. These prior reports and testimonies included our review and analysis of the *National Strategy for Homeland Security, the National Strategy to Secure Cyberspace, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, the National Strategy for Combating Terrorism,*[1] the Homeland Security Act of 2002,[2] and other relevant federal policies. Our work for today's testimony was performed in September 2003 in accordance with generally accepted government auditing standards.

---

[1] The White House, *The National Strategy for Homeland Security* (Washington, D.C.: July 2002); *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003); *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: February 2003); and *The National Strategy for Combating Terrorism* (Washington, D.C.: February 2003).

[2] Public Law 107–296.

Results in Brief

The Homeland Security Act of 2002 and other federal policy, including the *National Strategy for Homeland Security,* assign responsibilities to DHS for coordinating and sharing information related to threats of domestic terrorism, within the department and with and between other federal agencies, state and local governments, the private sector, and other entities. For example, to accomplish its missions, the new department must (1) access, receive, and analyze law enforcement information, intelligence information, and other threat, incident, and vulnerability information from federal and nonfederal sources; (2) analyze this information to identify and assess the nature and scope of terrorist threats; and (3) administer the Homeland Security Advisory System and provide specific warning information and advice on appropriate protective measures and countermeasures. Further, DHS must share information both internally and externally with agencies and law enforcement on such things as goods and passengers inbound to the United States and individuals who are known or suspected terrorists and criminals. It also must share information among emergency responders in preparing for and responding to terrorist attacks and other emergencies.

We have made numerous recommendations over the last several years related to information sharing functions that have been transferred to DHS. One significant area concerns the federal government's CIP efforts, which is focused on the sharing of information on incidents, threats, and vulnerabilities, and the providing of warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector. Although improvements have been made, further efforts are needed to address the following critical CIP challenges:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;
- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector; and
- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other CIP efforts.

In addition, we recently identified challenges in consolidating and standardizing watch list structures and policies, which are essential to effectively sharing information on suspected terrorists and criminals.[3]

The success of homeland security also relies on establishing effective systems and processes to facilitate information sharing among and between government entities and the private sector. Through our prior work, we have identified critical success factors and other key management issues that DHS should consider as it establishes systems and processes to facilitate information sharing among and between government entities and the private sector. These success factors include establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents. As part of its information technology management, DHS should continue to develop and implement an enterprise architecture to integrate the many existing systems and processes required to support its mission and to guide the department's investments in new systems to effectively support homeland security in the coming years. Other key management issues include ensuring that sensitive information is secured, developing secure communications networks, integrating staff from different organizations, and ensuring that the department has properly skilled staff.

Information Sharing Is Integral to Fulfilling DHS's Mission

With the terrorist attacks of September 2001, the threat of terrorism rose to the top of the country's national security and law enforcement agendas. As stated by the President in his *National Strategy for Homeland Security* in July 2002, our nation's terrorist enemies are constantly seeking new tactics or unexpected ways to carry out

[3] Watch lists are automated databases that contain various types of data on individuals, from biographical data—such as a person's name and date of birth—to biometric data such as fingerprints.

their attacks and magnify their effects, such as working to obtain chemical, biological, radiological, and nuclear weapons. In addition, terrorists are gaining expertise in less traditional means, such as cyber attacks. In response to these growing threats, Congress passed and the President signed the Homeland Security Act of 2002 creating the DHS. The overall mission of this new cabinet-level department includes preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing damage and assisting in recovery from attacks that do occur. To accomplish this mission, the act established specific homeland security responsibilities for the department and directed it to coordinate its efforts and share information within DHS and with other federal agencies, state and local governments, the private sector, and other entities. This information sharing is critical to successfully addressing increasing threats and fulfilling the mission of DHS.

Threats, Incidents, and the Consequences of Potential Attacks Are Increasing

DHS's responsibilities include the protection of our nation's publicly and privately controlled resources essential to the minimal operations of the economy and government against the risks of physical as well as computer-based or cyber attacks. Over the last decade, physical and cyber events, as well as related analyses by various entities, have demonstrated the increasing threat to the United States.

With the coordinated terrorist attacks against the World Trade Center in New York City and the Pentagon in Washington, D.C., on September 11, 2001, the threat of terrorism rose to the top of the country's national security and law enforcement agendas. Even before these catastrophic incidents, the threat of attacks against people, property, and infrastructures had increased concerns about terrorism. The terrorist bombings in 1993 of the World Trade Center in New York City and in 1995 of the Alfred P. Murrah Federal Building in Oklahoma City, which killed 168 people and wounded hundreds of others, prompted increased emphasis on the need to strengthen and coordinate the federal government's ability to effectively combat terrorism domestically. The 1995 Aum Shinrikyo sarin nerve agent attack in the Tokyo subway system also raised new concerns about U.S. preparedness to combat terrorist incidents involving weapons of mass destruction.[4] However, as clearly demonstrated by the September 11, 2001, incidents, a terrorist attack would not have to fit the definition of weapons of mass destruction to result in mass casualties, destruction of critical infrastructures, economic losses, and disruption of daily life nationwide.

U.S. intelligence and law enforcement communities continuously assess both foreign and domestic terrorist threats to the United States. Table 1 summarizes key physical threats to homeland security.

Table 1: Physical Threats to Homeland Security

Threat	Description
Chemical weapons	Chemical weapons are extremely lethal and capable of producing tens of thousands of casualties. They are also relatively easy to manufacture, using basic equipment, trained personnel, and precursor materials that often have legitimate dual uses. As the 1995 Tokyo subway attack revealed, even sophisticated nerve agents are within the reach of terrorist groups.
Biological weapons	Biological weapons, which release large quantities of living, disease-causing microorganisms, have extraordinary lethal potential. Like chemical weapons, biological weapons are relatively easy to manufacture, requiring straightforward technical skills, basic equipment, and a seed stock of pathogenic microorganisms. Biological weapons are especially dangerous because we may not know immediately that we have been attacked, allowing an infectious agent time to spread. Moreover, biological agents can serve as a means of attack against humans as well as livestock and crops, inflicting casualties as well as economic damage.

[4] A weapon of mass destruction is a chemical, biological, radiological, or nuclear agent or weapon.

Table 1: Physical Threats to Homeland Security—Continued

Threat	Description
Radiological weapons	Radiological weapons, or ''dirty bombs,'' combine radioactive material with conventional explosives. The individuals and groups engaged in terrorist activity can cause widespread disruption and fear, particularly in heavily populated areas.
Nuclear weapons	Nuclear weapons have enormous destructive potential. Terrorists who seek to develop a nuclear weapon must overcome two formidable challenges. First, acquiring or refining a sufficient quantity of fissile material is very difficult—though not impossible. Second, manufacturing a workable weapon requires a very high degree of technical capability—though terrorists could feasibly assemble the simplest type of nuclear device. To get around these significant though not insurmountable challenges, terrorists could seek to steal or purchase a nuclear weapon.
Conventional means	Terrorists, both domestic and international, continue to use traditional methods of violence and destruction to inflict harm and spread fear. They have used knives, guns, and bombs to kill the innocent. They have taken hostages and spread propaganda. Given the low expense, ready availability of materials, and relatively high chance for successful execution, terrorists will continue to make use of conventional attacks.

Source: National Strategy for Homeland Security

In addition to these physical threats, terrorists and others with malicious intent, such as transnational criminals and intelligence services, pose a threat to our nation's computer systems. As dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way much of the world communicate and conducts business, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. If not properly controlled, the speed and accessibility that create the enormous benefits of the computer age also allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes.

Government officials are increasingly concerned about cyber attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and are using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.[5] In addition, the disgruntled organization insider is a significant threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available IT, the likelihood increases

[5] *Virus:* a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse:* a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. Worm: an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Logic bomb:* in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer:* synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

that cyber attacks will threaten vital national interests. Table 2 summarizes the key cyber threats to our infrastructure.

Table 2: Cyber Threats to Critical Infrastructure Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence,[a] can affect the daily lives of Americans across the country.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and ''worms'' have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation unless otherwise indicated.

[a] **Prepared Statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 2, 2000.**

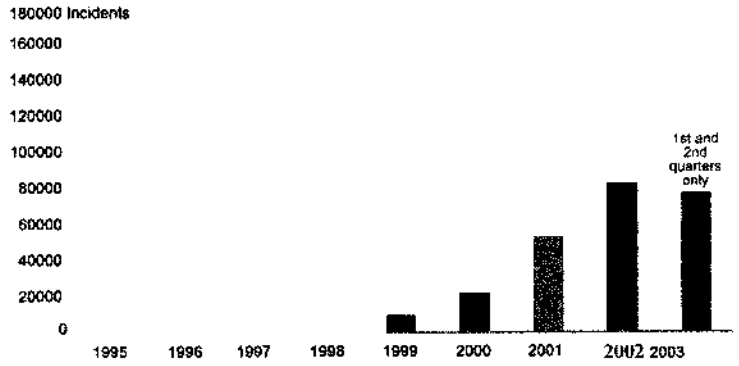
As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A hacker can literally download tools from the Internet and "point and click" to start an attack. Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

Along with these increasing threats, the number of computer security incidents reported to the CERT® Coordination Center[6] has also risen dramatically from just under 10,000 in 1999 to about 82,000 in 2002, and to over 76,000 for the first and second quarters of 2003. And these are only the reported attacks. The Director of CERT Centers stated that he estimates that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) the organization was un-

[6] The CERT® Coordination Center (CERT® CC) is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

able to recognize that its systems had been penetrated or there were no indications of penetration or attack or (2) the organization was reluctant to report. Figure 1 shows the number of incidents reported to the CERT Coordination Center from 1995 through the first half of 2003.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT Coordination Center from 1995 through the First Half of 2003



Source: GAO analysis based on Carnegie-Mellon University's CERT(r) Coordination Center data.

According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in February 2002, the threat to these infrastructures was highlighted by the Special Advisor to the President for Cyberspace Security in a Senate briefing when he stated that although to date none of the traditional terrorists groups, such as al Qaeda, have used the Internet to launch a known assault on the United States' infrastructure, information on water systems was discovered on computers found in al Qaeda camps in Afghanistan.[7] Also, in his February 2002 statement for the Senate Select Committee on Intelligence, the director of central intelligence discussed the possibility of cyber warfare attack by terrorists.[8] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

Since September 11, 2001, the critical link between cyberspace and physical space has also been increasingly recognized. In his November 2002 congressional testimony, the Director, CERT Centers at Carnegie-Mellon University, noted that supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems, and that these control systems are increasingly being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions.[9] These computer-controlled and network-connected systems are potential targets for individuals bent on causing massive disrup-

[7] "Administrative Oversight: Are We Ready for A Cyber Terror Attack?" Testimony before the Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, by Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the President's Critical Infrastructure Protection Board (Feb. 13, 2002).

[8] Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 6, 2002.

[9] Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Nov. 19, 2002.

tion and physical damage, and the use of commercial, off-the-shelf technologies for these systems without adequate security enhancements can significantly limit available approaches to protection and may increase the number of potential attackers. Not only is the cyber protection of our critical infrastructures important in and of itself, but a physical attack in conjunction with a cyber attack has also been highlighted as a major concern. In fact, the National Infrastructure Protection Center (NIPC) has stated that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure.[10] As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For example, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack.

Information Sharing is Critical to Meeting DHS's Mission

As our government and our nation has become ever more reliant on interconnected computer systems to support critical operations and infrastructures and as physical and cyber threats and potential attack consequences have increased, the importance of sharing information and coordinating the response to threats among stakeholders has increased. Information sharing and coordination among organizations are central to producing comprehensive and practical approaches and solutions to combating threats. For example, having information on threats and on actual incidents experienced by others can help an organization identify trends, better understand the risk it faces, and determine what preventive measures should be implemented. In addition, comprehensive, timely information on incidents can help federal and nonfederal analysis centers determine the nature of an attack, provide warnings, and advise on how to mitigate an imminent attack. Also, sharing information on terrorists and criminals can help to secure our nation's borders.

The Homeland Security Act of 2002 created DHS with the primary responsibility of preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing damage and assisting in recovery from attacks that do occur. To help DHS accomplish its mission, the act establishes, among other entities, five under secretaries with responsibility over directorates for management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness and response.

As part of DHS's responsibilities, the act includes several provisions specifically related to coordinating and sharing information within the department and among other federal agencies, state and local governments, the private sector, and other entities. It also includes provisions for protecting CIP information shared by the private sector and for sharing different types of information, such as grand jury and intelligence information. Other DHS responsibilities related to information sharing include

- requesting and receiving information from other federal agencies, state and local government agencies, and the private sector relating to threats of terrorism in the United States;
- distributing or, as appropriate, coordinating the distribution of warnings and information with other federal agencies, state and local governments and authorities, and the public;
- creating and fostering communications with the private sector;
- promoting existing public/private partnerships and developing new public/private partnerships to provide for collaboration and mutual support; and
- coordinating and, as appropriate, consolidating the federal government's communications and systems of communications relating to homeland security with state and local governments and authorities, the private sector, other entities, and the public.

Each DHS directorate is responsible for coordinating relevant efforts with other federal, state, and local governments. The act also established the Office for State and Local Government Coordination to, among other things, provide state and local governments with regular information, research, and technical support to assist them in securing the nation. Further, the act included provisions as the "Homeland Secu-

[10] National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption* (Washington, D.C.: July 2002).

rity Information Sharing Act" that requires the President to prescribe and implement procedures for facilitating homeland security information sharing and establishes authorities to share different types of information, such as grand jury information; electronic, wire, and oral interception information; and foreign intelligence information. In July 2003, the President assigned these functions to the Secretary of Homeland Security.[11]

The following sections illustrate how DHS will require successful information sharing within the department and between federal agencies, state and local governments, and the private sector to effectively carry out its mission.

INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION DIRECTORATE

The Information Analysis and Infrastructure Protection Directorate (IAIP) is responsible for accessing, receiving, and analyzing law enforcement information, intelligence information, and other threat and incident information from respective agencies of federal, state, and local governments and the private sector, and for combining and analyzing such information to identify and assess the nature and scope of terrorist threats. IAIP is also tasked with coordinating with other federal agencies to administer the Homeland Security Advisory System to provide specific warning information along with advice on appropriate protective measures and countermeasures.[12] Further, IAIP is responsible for disseminating, as appropriate, information analyzed by DHS within the department, to other federal agencies, to state and local government agencies, and to private-sector entities.

The Homeland Security Act of 2002 makes DHS and its IAIP directorate also responsible for key CIP functions for the federal government. CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are critical to national security, national economic security, and/or national public health and safety. Information sharing is a key element of these activities. Over 80 percent of our nation's critical infrastructures are controlled by the private sector. As part of its CIP responsibilities, IAIP is responsible for

(1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States and

(2) recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities.

Federal CIP policy has continued to evolve since the mid-1990s through a variety of working groups, special reports, executive orders, strategies, and organizations. In particular, Presidential Decision Directive 63 (PDD 63) issued in 1998 established CIP as a national goal and described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. To accomplish its goals, PDD 63 established and designated organizations to provide central coordination and support. These included the Critical Infrastructure Assurance Office (CIAO), an interagency office established to develop a national plan for CIP, and NIPC, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation/response. The Homeland Security Act of 2002 transferred these and certain other CIP entities and their functions (other than the Computer Investigations and Operations Section of NIPC) to DHS's IAIP directorate.

Federal CIP policy, beginning with PDD 63 and reinforced through other strategy documents, including the *National Strategy for Homeland Security* issued in July 2002, called for a range of activities intended to establish a partnership between the public and private sectors to ensure the security of our nation's critical infrastructures. To ensure coverage of critical infrastructure sectors, this policy identified infrastructure sectors that were essential to our national security, national economic security, and/or national public health and safety. For these sectors, which now total 14, federal government leads (sector liaisons) and private-sector leads (sector coordinators) were to work with each other to address problems related to CIP for their sector. In particular, they were to (1) develop and implement vulnerability awareness and education programs and (2) contribute to a sectoral plan by

- assessing the vulnerabilities of the sector to cyber or physical attacks;

---

[11] The White House, Executive Order 13311—Homeland Security Information Sharing (Washington, D.C.: Jul. 29, 2003).

[12] The Homeland Security Advisory System uses five levels (Severe, High, Elevated, Guarded, and Low) to inform federal, state, and local government agencies and authorities, the private sector, and the public of the nation's terrorist threat conditions.

• recommending a plan to eliminate significant vulnerabilities;
• proposing a system for identifying and preventing major attacks; and
• developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with the Federal Emergency Management Agency as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

CIP policy also called for sector liaisons to identify and assess economic incentives to encourage the desired sector behavior in CIP. Federal grant programs to assist state and local efforts, legislation to create incentives for the private sector and, in some cases, regulation are mentioned in CIP policy.

Federal CIP policy also encourages the voluntary creation of information sharing and analysis centers (ISACs) to serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. Their activities could improve the security posture of the individual sectors, as well as provide an improved level of communication within and across sectors and all levels of government. While PDD 63 encouraged the creation of ISACs, it left the actual design and functions of the ISACs, along with their relationship with NIPC, to be determined by the private sector in consultation with the federal government. PDD 63 did provide suggested activities, which the ISACs could undertake, including

• establishing baseline statistics and patterns on the various infrastructures;
• serving as a clearinghouse for information within and among the various sectors;
• providing a library for historical data for use by the private sector and government; and
• reporting private-sector incidents to NIPC.

As we reported in our April 8, 2003,[13] testimony, table 3 shows the sectors identified in federal CIP policy, the lead agencies for these sectors, and whether or not an ISAC has been established for the sector.

Table 3: Lead Agencies and ISAC Status by CIP Sector

Sectors Sectors identified by PDD 63	Designated lead agency	ISAC established
Information and telecommunications	Homeland Security*	
Information technology		x
Telecommunications		x
Research and education networks		x
Banking and finance	Treasury	x
Water	Environmental Protection Agency	x
Transportation	Homeland Security*	
Aviation		
Surface transportation		x
Maritime		prospective
Trucking		x
Emergency services**	Homeland Security*	
Emergency law enforcement		x
Emergency fire services		x
Government **	Homeland Security*	
Interstate		x
Energy	Energy	
Electric power		x
Oil and gas		x
Public health	Health and Human Services	

[13] U.S. General Accounting Office, *Information Security Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures,* GAO–03–564T (Washington, D.C.: Apr. 8, 2003).

Table 3: Lead Agencies and ISAC Status by CIP Sector—Continued

Sectors Sectors identified by PDD 63	Designated lead agency	ISAC established
Sectors identified by the National Strategy for Homeland Security		
Food		x
Meat and poultry	Agriculture	
All other food products	Health and Human Services	
Agriculture	Agriculture	
Chemical industry and hazardous materials	Environmental Protection Agency	
Chemicals		x
Defense industrial base	Defense	
Postal and shipping	Homeland Security	
National monuments and icons	Interior	
Other communities that have established ISACs		
Real estate		x

***The lead agencies previously designated by PDD 63 were (from top to bottom) the Department of Commerce, Department of Transportation, Department of Justice/Federal Bureau of Investigation, and the Federal Emergency Management Agency.**

****PDD 63 identified as critical sectors (1) emergency law enforcement and (2) emergency fire services and continuity of government. In the** *National Strategy for Homeland Security,* **emergency law enforcement and emergency fire services are both included in an emergency services sector. Also, continuity of government, along with continuity of operations, is listed as a subcomponent under the government sector.**

The Interstate ISAC shown in table 3 was established by the National Association of State Chief Information Officers (NASCIO) and is intended to provide a mechanism for informing state officials about DHS threat warnings, alerts, and other relevant information, and for state officials to report information to DHS. According to a NASCIO official, currently, there are limited resources available to provide suggested ISAC activities. For example, there is not a watch operation, although notifications can be sent out to members at any time and some states have their own watch centers. He also stated that NASCIO's efforts have focused on working with DHS to develop an intergovernmental approach, similar to other federal and state efforts such as law enforcement task forces, where state and federal agencies share resources and responsibilities.

As called for by the *National Strategy for Homeland Security,* on February 14, 2003, the President also released the *National Strategy to Secure Cyberspace* and the complementary *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* These two strategies identify priorities, actions, and responsibilities for the federal government (including lead agencies and DHS) as well as for state and local governments and the private sector. These two strategies also emphasize the importance of developing mechanisms for the public and private sectors to share information about vulnerabilities, incidents, threats, and other security data. For example, the *National Strategy to Secure Cyberspace* calls for the development of a National Cyberspace Security Response System. To be coordinated by DHS, this system is described as a public/private architecture for analyzing and warning, managing incidents of national significance, promoting continuity in government systems and private-sector infrastructures, and increasing information sharing across and between organizations to improve cyberspace security. The system is to include governmental and nongovernmental entities, such as private-sector ISACs. The strategies also encourage the continued establishment of ISACs and efforts to enhance the analytical capabilities of existing ISACs.

As we reported in April 2003, according to a DHS official, the department is continuing to carry out the CIP activities of the functions and organizations transferred

to it by the Homeland Security Act of 2002.[14] Further, this official stated that the department is taking actions to enhance those activities as it integrates them within the new department and is continuing previously established efforts to maintain and build relationships with other federal entities, including the FBI and other NIPC partners, and with the private sector.

To fulfill its mission, the IAIP directorate will need to ensure effective information sharing with other federal entities. For example, information sharing with the recently formed Terrorist Threat Integration Center (TTIC) is a central function of the directorate. TTIC was created to merge and analyze terrorist-related information collected domestically and abroad to enhance coordination, facilitate threat analysis, and enable more comprehensive threat assessments. DHS is providing staff to work at TTIC, and the center is to provide DHS with a comprehensive assessment of threat information that will guide the department's response to any potential attacks.

To help implement its cybersecurity responsibilities, in June 2003, DHS created the National Cyber Security Division within IAIP, and on September 15, 2003, DHS announced the appointment of the first director of the division. According to DHS, this division will identify, analyze, and reduce cyber threats and vulnerabilities; disseminate threat warning information; coordinate incident response; and provide technical assistance in continuity of operations and recovery planning. Building on capabilities transferred to DHS from the CIAO, the NIPC, the Federal Computer Incident Response Center (FedCIRC), and the National Communications System, the division is organized around three units designed to:

• identify risks and help reduce the vulnerabilities to government's cyber assets and coordinate with the private sector to identify and help protect America's critical cyber assets;

• oversee a consolidated Cyber Security Tracking, Analysis, & Response Center, which will detect and respond to Internet events; track potential threats and vulnerabilities to cyberspace; and coordinate cybersecurity and incident response with federal, state, local, private-sector and international partners; and

• create, in coordination with other appropriate agencies, cybersecurity awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities.

Also, on September 15, 2003, DHS announced the creation of the U.S. Computer Emergency Response Team (US—CERT)—a partnership between the National Cyber Security Division and CERT/CC. According to DHS, it will

• improve warning and response time to security incidents by fostering the development of detection tools and using common commercial incident and vulnerability reporting protocols—with the goal to reduce the response time to a security event to an average of 30 minutes by the end of 2004;

• increase the flow of critical security information throughout the Internet community;

• provide a coordination center that, for the first time, links public and private response capabilities to facilitate communication across all infrastructure sectors;

• collaborate with the private sector to develop and implement new tools and methods for detecting and responding to vulnerabilities; and

• work with infrastructure owners and operators and technology experts to foster the development of improved security technologies and methods to increase cybersecurity at all levels across the nation.

In its announcement, DHS also stated that the US—CERT is expected to grow to include other partnerships with private-sector security vendors and other domestic and international CERT organizations. These groups will work together to coordinate national and international efforts to prevent, protect, and respond to the effects of cyber attacks across the Internet.

The Directorate of Border and Transportation Security

According to the act, the Border and Transportation Security Directorate (BTS) is responsible for, among other things, (1) preventing the entry of terrorists and the instruments of terrorism into the United States; (2) securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems, including managing and coordinating those functions transferred to the department; (3) carrying out immigration enforcement functions; (4) establishing and administering rules for granting visas, and (5) administering customs laws. A number of federal entities are under its responsibility, such as the Transportation Security Administration, U.S. Customs Service, the border security functions of the Immigration

[14] GAO–03–564T.

and Naturalization Service (INS), Animal and Plant Health Inspection Service, and the Federal Law Enforcement Training Center.

To successfully protect the borders and transportation systems of the United States, BTS faces the challenge of sharing information across the various organizations under its responsibility. According to the *National Strategy for Homeland Security*, to successfully prevent the entry of contraband, unauthorized aliens, and potential terrorists, DHS will have to increase the level of information available on inbound goods and passengers to the border management component agencies under the BTS. For example, the strategy discusses the need to increase the security of international shipping containers—noting that 50 percent of the value of U.S. imports arrives via 16 million containers. To increase security, U.S. inspectors will need shared information so that they can identify high-risk containers. In addition, protecting our borders from the entry of unauthorized aliens and potential terrorists will require the sharing of information between various law enforcement and immigration services. For example, we recently reported on the use of watch lists as important tools to help secure our nation's borders.[15] These lists provide decision makers with information about individuals who are known or suspected terrorists and criminals so that these individuals can be prevented from entering the country, apprehended while in the country, or apprehended as they attempt to exit the country.

The Emergency Preparedness and Response Directorate

According to the act, the Emergency Preparedness and Response Directorate (EPR) ensures that the nation is prepared for, and able to recover from, terrorist attacks, major disasters, and other emergencies. In addition, EPR is responsible for building a comprehensive national incident management system with federal, state, and local governments and authorities to respond to such attacks and disasters. This project will require developing an extensive program of information sharing among federal, state, and local governments. Further, EPR is to develop comprehensive programs for developing interoperable communications technology and helping to ensure that emergency response providers acquire such technology. Among the functions transferred to EPR are the Federal Emergency Management Agency, the Integrated Hazard Information System of the National Oceanic and Atmospheric Administration, and the Metropolitan Medical Response System.

Information sharing is important to emergency responders to prepare for and respond to terrorist attacks and other emergencies. For example, if a biological attack were to occur, it would be important for health officials to quickly and effectively exchange information with relevant experts directly responding to the event in order to respond appropriately. To support this type of exchange, the Centers for Disease Control and Prevention (CDC) created the Epidemic Information Exchange (*Epi–X*), a secure, Web-based communications network that serves as an information exchange between CDC, state and local health departments, poison control centers, and other public health professionals. According to CDC, *Epi–X's* primary goals include informing health officials about important public health events, helping them respond to public health emergencies, and encouraging professional growth and the exchange of information. CDC has also created an emergency operations center to respond to public health emergencies and to allow for immediate secure communication between CDC, the Department of Health and Human Services, federal intelligence and emergency response officials, DHS, and state and local public health officials.

Information Sharing Challenges

We have made numerous recommendations over the last several years related to information sharing functions that have been transferred to DHS. One significant area of our work concerns the federal government's CIP efforts, which is focused on sharing information on incidents, threats, and vulnerabilities and providing warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector. Although improvements have been made in protecting our nation's critical infrastructures and continuing efforts are in progress, further efforts are needed to address the following critical CIP challenges that we have identified:

• developing a comprehensive and coordinated national plan to facilitate CIP information sharing, which clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;

---

[15] U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing,* GAO–03–322 (Washington, D.C: Apr. 15, 2003).

• developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;
• improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector; and
• providing appropriate incentives for nonfederal entities to increase information sharing with the federal government.

In addition, we recently identified challenges in consolidating and standardizing watch list structures and policies, which are essential to effectively sharing information on suspected criminals and terrorists.

A Complete and Coordinated National CIP Plan Needs to Be Developed

An underlying issue in the implementation of CIP is that no national plan to facilitate information sharing yet exists that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets time frames for achieving objectives, and establishes performance measures. Such a clearly defined plan is essential for defining the relationships among all CIP organizations to ensure that the approach is comprehensive and well coordinated. Since 1998, we have reported on the need for such a plan and made numerous related recommendations.

In September 1998, we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of federal entities was important to ensure governmentwide cooperation and support for PDD 63.[16] At that time, we recommended that the Office of Management and Budget (OMB) and the Assistant to the President for National Security Affairs ensure such coordination.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public/private partnership to defend our national infrastructures. However, this plan focused largely on federal cyber CIP efforts, saying little about the private-sector role.

In September 2001, we reported that agency questions had surfaced regarding specific roles and responsibilities of entities involved in cyber CIP and the timeframes within which CIP objectives were to be met, as well as guidelines for measuring progress.[17] Accordingly, we made several recommendations to supplement those we had made in the past. Specifically, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government's strategy to address computer-based threats define

• specific roles and responsibilities of organizations involved in CIP and related information security activities;
• interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementing vulnerability assessments and related remedial plans; and
• performance measures for which entities can be held accountable.

In July 2002, we issued a report identifying at least 50 organizations that were involved in national or multinational cyber CIP efforts, including 5 advisory committees; 6 Executive Office of the President organizations; 38 executive branch organizations associated with departments, agencies, or intelligence organizations; and 3 other organizations.18 Although our review did not cover organizations with national physical CIP responsibilities, the large number of organizations that we did identify as involved in CIP efforts presents a need to clarify how these entities coordinate their activities with each other. Our report also stated that PDD 63 did not specifically address other possible critical sectors and their respective federal agency counterparts. Accordingly, we recommended that the federal government's strategy also

• include all relevant sectors and define the key federal agencies' roles and responsibilities associated with each of these sectors, and
• define the relationships among the key CIP organizations.

---

[16] U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk,* GAO/AIMD–98–92 (Washington, D.C.: Sept. 23, 1998).

[17] U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations,* GAO–01–822 (Washington, D.C.: Sept. 20, 2001).18GAO–02–474.

In July 2002, the *National Strategy for Homeland Security* called for interim cyber and physical infrastructure protection plans that DHS would use to build a comprehensive national infrastructure plan. Implementing a well-developed plan is critical to effective coordination in times of crises. According to the strategy, the national plan is to provide a methodology for identifying and prioritizing critical assets, systems, and functions, and or sharing protection responsibility with state and local governments and the private sector. The plan is also to establish standards and benchmarks for infrastructure protection and provide a means to measure performance. The plan is expected to inform DHS on budgeting and planning for CIP activities and how to use policy instruments to coordinate between government and private entities to improve the security of our national infrastructures to appropriate levels. The strategy also states that DHS is to unify the currently divided responsibilities for cyber and physical security. According to the department's November 2002 reorganization plan, the Assistant Secretary for Infrastructure Protection is responsible for developing a comprehensive national infrastructure plan.

As discussed previously, in February 2003, the President issued the interim strategies—*The National Strategy to Secure Cyberspace and The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (hereafter referred to in this testimony as the cyberspace security strategy and the physical protection strategy). These strategies identify priorities, actions, and responsibilities for the federal government, including federal lead departments and agencies and the DHS, as well as for state and local governments and the private sector. Both define strategic objectives for protecting our nation's critical assets. The physical protection strategy discusses the goals and objectives for protecting our nation's critical infrastructure and key assets from physical attack. The cyberspace security strategy provides a framework for organizing and prioritizing the individual and concerted responsibilities of all levels of government to secure cyberspace.

According to the physical protection strategy, across government, there are inconsistent methodologies to prioritize efforts to enhance critical infrastructure protection. This problem is compounded with ineffective communication among the federal, state, and local governments that has resulted in untimely, disparate, and at times conflicting communication between those who need it most. DHS has been given a primary role in providing cross-sector coordination to improve communication and planning efforts and serves as the single point of coordination for state and local governments on homeland security issues. To fulfill its role as the cross-sector coordinator, DHS will partner with state and local governments and the private sector to institute processes that are transparent, comprehensive, and results-oriented. This effort will include creating mechanisms for collaborative national planning efforts between the private and public sectors and for consolidating the individual sector plans into a comprehensive plan that will define their respective roles, responsibilities, and expectations.

The cyberspace security strategy is the counterpart to the physical protection strategy and provides the framework for organizing and prioritizing the individual and concerted responsibilities of all levels of government to secure cyberspace. DHS serves as the focal point for managing cybersecurity incidents that could affect the federal government or the national information infrastructure and, thus, plays a central role in executing the initiatives assigned in this strategy. While the cyberspace security strategy mentions the responsibility of DHS in creating a comprehensive national plan for securing resources and key infrastructures, much of the strategy's emphasis remains on coordinating and integrating various plans with the private sector.

Neither strategy (1) clearly indicates how the physical and cyber efforts will be coordinated; (2) defines the roles, responsibilities, and relationships among the key CIP organizations, including state and local governments and the private sector; (3) indicates time frames or milestones for their overall implementation or for accomplishing specific actions or initiatives; nor (4) establishes performance measures for which entities can be held responsible. Until a comprehensive and coordinated plan is completed that unifies the responsibilities for cyber and physical infrastructures; identifies roles, responsibilities, and relationships for all CIP efforts; establishes time frames or milestones for implementation; and establishes performance measures, our nation risks not having a consistent and appropriate information sharing framework to deal with growing threats to its critical infrastructure.

Better Information Sharing on Threats and Vulnerabilities Must Be Implemented

Information sharing is a key element in developing comprehensive and practical approaches to defending against potential cyber and other attacks, which could threaten the national welfare. Information on threats, vulnerabilities, and incidents expe-

rienced by others can help identify trends, better understand the risks faced, and determine what preventive measures should be implemented. However, as we have reported in recent years, establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult. In addition, the private sector has expressed concerns about sharing information with the government and the difficulty of obtaining security clearances. Both the Congress and the administration have taken steps to address information sharing issues in law and recent policy guidance, but their effectiveness will largely depend on how DHS implements its information sharing responsibilities.

A number of activities have been undertaken to build information-sharing relationships between the federal government and the private sector, such as InfraGard, the Partnership for Critical Infrastructure Security, efforts by the CIAO, and efforts by lead agencies to establish ISACs. For example, the InfraGard Program, which provides the FBI and NIPC with a means of securely sharing information with individual companies, has expanded substantially. InfraGard membership has increased from 277 in October 2000 to almost 9,400 in September 2003. Members include representatives from private industry, other government agencies, state and local law enforcement, and the academic community.

As stated above, PDD 63 encouraged the voluntary creation of ISACs to serve as the mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information between the private sector and the federal government through NIPC. In April 2001, we reported that NIPC and other government entities had not developed fully productive information-sharing relationships but that NIPC had undertaken a range of initiatives to foster information-sharing relationships with ISACs, as well as with government and international entities. We recommended that NIPC formalize relationships with ISACs and develop a plan to foster a two-way exchange of information between them.

In response to our recommendations, NIPC officials told us in July 2002 that an ISAC development and support unit had been created, whose mission was to enhance private-sector cooperation and trust so that it would result in a two-way sharing of information. As shown previously in table 3, as of April 2003, DHS reported that there are 16 current ISACs, including ISACs established for sectors not identified as critical infrastructure sectors. DHS officials also stated that they have formal agreements with most of the current ISACs.

In spite of progress made in establishing ISACs, additional efforts are needed. All sectors do not have a fully established ISAC, and even for those sectors that do, our recent work showed that participation may be mixed, and the amount of information being shared between the federal government and private-sector organizations also varies. Specifically, as we reported in February 2003, the five ISACs we recently reviewed showed different levels of progress in implementing the PDD 63 suggested activities.[19] For example, four of the five reported that efforts were still in progress to establish baseline statistics, which includes developing a database on the normal levels of computer security incidents that would be used for analysis purposes. Also, while all five reported that they served as the clearinghouse of information (such as incident reports and warnings received from members) for their own sectors, only three of the five reported that they are also coordinating with other sectors. Only one of the five ISACs reported that it provides a library of incidents and historical data that was available to both the private sector and the federal government, and although three additional ISACs do maintain a library, it was available only to the private sector. Table 4 summarizes the reported status of the five ISACs in performing these and other activities suggested by PDD 63.

Table 4: ISACs' Progress in Performing Activities Suggested by PDD 63

Activity	Telecommunications	Electricity	ISAC Information Technology	Energy	Water
Establish baseline statistics	In progress	In progress	Yes	In progress	In progress

[19] U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors,* GA–03–233 (Washington, D.C.: Feb. 28, 2003).

Table 4: ISACs' Progress in Performing Activities Suggested by PDD 63—Continued

Activity	Telecommunications	Electricity	ISAC Information Technology	Energy	Water
Serve as clearinghouse within and among sectors	Yes	Yes	Yes	Only within own sector	Only within own sector
Provide library to private sector and government	In progress	Yes	Available only to private sector	Available only to private sector	Available only to private sector
Report incidents to NIPC	Yes	Yes	Yes	No	Yes

Source: ISACs.

As also noted in our February 2003 report, some in the private sector expressed concerns about voluntarily sharing information with the government. Specifically, concerns were raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith. For example, the IT, energy, and the water ISACs reported that they did not share their libraries with the federal government because of concerns that information could be released under FOIA. And, officials of the energy ISAC stated that they have not reported incidents to NIPC because of FOIA and antitrust concerns.

The recently established ISAC Council may help to address some of these concerns. According to its chairman, the mission of the ISAC Council is to advance the physical and cybersecurity of the critical infrastructures of North America by establishing and maintaining a framework for interaction between and among the ISACs. Activities of the council include establishing and maintaining a policy for inter-ISAC coordination, a dialog with governmental agencies that deal with ISACs, and a practical data and information sharing protocol (what to share and how to share). In addition, the council will develop analytical methods to assist the ISACs in supporting their own sectors and other sectors with which there are interdependencies and establish a policy to deal with matters of liability and anti-trust. The chairman also reported that the council held an initial meeting with DHS and the White House in June 2003 to, among other things, understand mutual DHS and ISAC expectations.

There will be continuing debate as to whether adequate protection is being provided to the private sector as these entities are encouraged to disclose and exchange information on both physical and cybersecurity problems and solutions that are essential to protecting our nation's critical infrastructures. The *National Strategy for Homeland Security* includes "enabling critical infrastructure information sharing" in its 12 major legislative initiatives. It states that the nation must meet this need by narrowly limiting public disclosure of information relevant to protecting our physical and cyber critical infrastructures in order to facilitate the voluntary submission of information. It further states that the Attorney General will convene a panel to propose any legal changes necessary to enable sharing of essential homeland security related information between the federal government and the private sector.

Actions have already been taken by the Congress and the administration to strengthen information sharing. For example, the USA PATRIOT Act promotes information sharing among federal agencies, and numerous terrorism task forces have been established to coordinate investigations and improve communications among federal and local law enforcement.[20] Moreover, the Homeland Security Act of 2002 includes provisions that restrict federal, state, and local government use and disclosure of critical infrastructure information that has been voluntarily submitted to DHS. These restrictions include exemption from disclosure under FOIA, a general limitation on use to CIP purposes, and limitations on use in civil actions and by state or local governments. The act also provides penalties for any federal employee

[20] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Public Law No. 107–56, October 26, 2001.

who improperly discloses any protected critical infrastructure information. In April 2003, DHS issued for comment its proposed rules for how critical infrastructure information volunteered by the public will be protected. At this time, it is too early to tell what impact the act will have on the willingness of the private sector to share critical infrastructure information.

Information sharing among federal, state and local governments also needs to be improved. In August 2003 we reported the results of our survey of federal, state, and city government officials' perceptions of the effectiveness of the current information-sharing process.[21] Performed primarily before DHS began its operations, our survey identified some notable information-sharing initiatives, but also highlighted coordination issues and other concerns that many of the surveyed entities had with the overall information-sharing process. For example, the FBI reported it had significantly increased the number of its Joint Terrorism Task Forces and, according to our survey, 34 of 40 states and 160 of 228 cities stated that they participated in information-sharing centers. However, although such initiatives may increase the sharing of information to fight terrorism, none of the three levels of government perceived the current information-sharing process as effective, particularly when sharing information with federal agencies. Respondents reported that information on threats, methods, and techniques of terrorists was not routinely shared; and the information that was shared was not perceived as timely, accurate, or relevant. Further, 30 of 40 states and 212 of 228 cities responded that they were not given the opportunity to participate in national policy making on information sharing. Federal agencies in our survey also identified several barriers to sharing threat information with state and city governments, including the inability of state and city officials to secure and protect classified information, the lack of federal security clearances, and a lack of integrated databases.

The private sector has also expressed its concerns about the value of information being provided by the government. For example, in July 2002 the President for the Partnership for Critical Infrastructure Security stated in congressional testimony that information sharing between the government and private sector needs work, specifically, in the quality and timeliness of cybersecurity information coming from the government.[22] In March 2003 we also reported that the officials from the chemical industry noted that they need better threat information from law enforcement agencies, as well as better coordination among agencies providing threat information.[23] They stated that chemical companies do not receive enough specific threat information and that it frequently comes from multiple government agencies. Similarly, in developing a vulnerability assessment methodology to assess the security of chemical facilities against terrorist and criminal attacks, the Department of Justice observed that chemical facilities need more specific information about potential threats in order to design their security systems and protocols. Chemical industry officials also noted that efforts to share threat information among industry and federal agencies will be effective only if government agencies provide specific and accurate threat information. Threat information also forms the foundation for some of the tools available to industry for assessing facility vulnerabilities. The Justice vulnerability assessment methodology requires threat information as the foundation for hypothesizing about threat scenarios, which form the basis for determining site vulnerabilities.

The Homeland Security Act, the *National Strategy for Homeland Security,* the *National Strategy to Secure Cyberspace,* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* all acknowledge the importance of information sharing and identify multiple responsibilities for DHS to share information on threats and vulnerabilities. In particular:

• The Homeland Security Act authorizes the IAIP Under Secretary to have access to all information in the federal government that concerns infrastructure or other vulnerabilities of the United States to terrorism and to use this information to fulfill its responsibilities to provide appropriate analysis and warnings related to threats to and vulnerabilities of critical information systems, crisis management support in response to threats or attacks on critical information systems, and technical assist-

---

[21] U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need toBe Strengthened,* GAO–03–760 (Washington, D.C.: Aug. 27, 2003).

[22] Testimony of Kenneth C. Watson, President, Partnership for Critical Infrastructure Security, beforethe Subcommittee on Oversight and Investigation of the Energy and Commerce Committee, U.S. House of Representatives, July 9, 2002.

[23] U. S. General Accounting Office, *Homeland Security: Voluntary Initiatives Are Under Way at ChemicalFacilities, but the Extent of Security Preparedness is Unknown,* GAO–03–439 (Washington D.C.: Mar.14, 2003).

ance upon request to private-sector and government entities to respond to major failures of critical information systems.

• The *National Strategy for Homeland Security* specifies the need for DHS to work with state and local governments to achieve "seamless communication" among all responders. This responsibility includes developing a national emergency communication plan to establish policies and procedures to improve the exchange of information. Ensuring improved communications also involves developing systems that help prevent attacks and minimize damage. Such systems, which would be accessed and used by all levels of government, would detect hostile intents and help locate individual terrorists as well as monitor and detect outbreaks.

• The cyberspace security strategy encourages DHS to work with the National Infrastructure Advisory Council and the private sector to develop an optimal approach and mechanism to disclose vulnerabilities in order to expedite the development of solutions without creating opportunities for exploitation by hackers. DHS is also expected to raise awareness about removing obstacles to sharing information concerning cybersecurity and infrastructure vulnerabilities between the public and private sectors and is encouraged to work closely with ISACs to ensure that they receive timely and actionable threat and vulnerability data and to coordinate voluntary contingency planning efforts.

• The physical protection strategy describes DHS's need to collaborate with the intelligence community and the Department of Justice to develop comprehensive threat collection, assessment, and dissemination processes that are distributed to the appropriate entity in a timely manner. It also enumerates several initiatives directed to DHS to accomplish to create a more effective information-sharing environment among the key stakeholders, including establishing requirements for sharing information; supporting state and local participation with ISACs to more effectively communicate threat and vulnerability information; protecting secure and proprietary information deemed sensitive by the private sector; implementing processes for collecting, analyzing, and disseminating threat data to integrate information from all sources; and developing interoperable systems to share sensitive information among government entities to facilitate meaningful information exchange.

• The *National Strategy for Homeland Security* also describes DHS's need to engage its partners around the world in cooperative efforts to improve security. It states that DHS will increase information sharing between the international law enforcement, intelligence, and military communities.

Analysis and Warning Capabilities Need to Be Improved

Analysis and warning capabilities should be developed to detect precursors to attacks on the nation so that advanced warnings can be issued and protective measures implemented. Since the 1990s, the national security community and the Congress have identified the need to establish analysis and warning capabilities to protect against strategic computer attacks against the nation's critical computer-dependent infrastructures. Such capabilities need to address both cyber and physical threats and involve (1) gathering and analyzing information for the purpose of detecting and reporting otherwise potentially damaging actions or intentions and (2) implementing a process for warning policymakers and allowing them time to determine the magnitude of the related risks.

In April 2001,[24] we reported on NIPC's progress and impediments in developing analysis and warning capabilities for computer-based attacks, which included the following:[25]

• Lack of a generally accepted methodology for analyzing strategic cyber-based threats. For example, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.

• Lack of industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. In September 2001, we reported that although outreach efforts had raised awareness and improved information sharing, substantive, comprehensive analysis of infrastructure sector interdependencies and vulnerabilities had been limited.

---

[24] GAO–01–323.

[25] Pursuant to the Homeland Security Act of 2002, the functions of NIPC (except for computerinvestigations and operations) were transferred over to DHS from the FBI.

Another challenge confronting the analysis and warning capabilities of our nation is that, historically, our national CIP attention and efforts have been focused on cyber threats. As we also reported in April 2001, although PDD 63 covers both physical and cyber threats, federal efforts to meet the directive's requirements have pertained primarily to cyber threats since this is an area that the leaders of the administration's CIP strategy view as needing attention. However, the terrorist attacks of September 11, 2001, have increased the emphasis of physical threats. In addition, in July 2002, NIPC reported that the potential for concurrent cyber and physical ("swarming") attacks is an emerging threat to the U.S. critical infrastructure. Further, in July 2002, the director of NIPC also told us that NIPC had begun to develop some capabilities for identifying physical CIP threats. For example, NIPC had developed thresholds with several ISACs for reporting physical incidents and, since January 2002, has issued several information bulletins concerning physical CIP threats. However, NIPC's director acknowledged that fully developing this capability would be a significant challenge. The physical protection strategy states that DHS will maintain a comprehensive, up-to-date assessment of vulnerabilities across sectors and improve processes for domestic threat data collection, analysis, and dissemination to state and local governments and private industry.

The administration and the Congress continue to emphasize the need for these analysis and warning capabilities. The *National Strategy for Homeland Security* identified intelligence and warning as one of six critical mission areas and called for major initiatives to improve our nation's analysis and warning capabilities. The strategy also stated that no government entity was then responsible for analyzing terrorist threats to the homeland, mapping these threats to our vulnerabilities, and taking protective action. The Homeland Security Act gives such responsibility to the new DHS. For example, the IAIP Under Secretary is responsible for administering the Homeland Security Advisory System, and is to coordinate with other federal agencies to provide specific warning information and advice to state and local agencies, the private sector, the public, and other entities about appropriate protective measures and countermeasures to homeland security threats.

An important aspect of improving our nation's analysis and warning capabilities is having comprehensive vulnerability assessments. The *National Strategy for Homeland Security* also states that comprehensive vulnerability assessments of all of our nation's critical infrastructures are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given sector and then invest accordingly to protect it. The strategy states that the U.S. government does not perform vulnerability assessments of the nation's entire critical infrastructure. The Homeland Security Act of 2002 states that the DHS's IAIP Under Secretary is to carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructures of the United States.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, is received from the intelligence and law enforcement communities. For example, there has been considerable public debate regarding the quality and timeliness of intelligence data shared between and among relevant intelligence, law enforcement, and other agencies. Also, as the transfer of NIPC to DHS organizationally separated it from the FBI's law enforcement activities (including the Counterterrorism Division and NIPC field agents), it will be critical to establish mechanisms for continued communication to occur. Further, it will be important that the relationships between the law enforcement and intelligence communities and the new DHS are effective and that appropriate information is exchanged on a timely basis. The act gives DHS broad statutory authority to access intelligence information, as well as other information relevant to the terrorist threat and to turn this information into useful warnings. For example, DHS is to be a key participant in the multiagency TTIC[26] that began operations on May 1, 2003. According to a White House fact sheet, DHS's IAIP is to receive and analyze terrorism-related information from the TTIC.[27] Although the purpose of TTIC and the authorities and responsibilities of the FBI and Central Intelligence Agency (CIA) counterterrorism organizations remain distinct, in July 2003, the TTIC Director reported that initiatives are under way to facilitate efforts within the intelligence community to ensure that DHS has access to all information required to execute its mission. He also reported other progress, such as updates to a TTIC-sponsored Web site that provides

[26] The center was formed from elements of the Department of Homeland Security, the FBI's Counterterrorism Division, the Director of Central Intelligence's Counterterrorist Center, and the Department of Defense.

[27] The White House, *Fact Sheet: Strengthening Intelligence to Better Protect America* (Washington, D.C.: Jan. 28, 2003).

terrorism-related information. For example, the Web site is to increasingly include products tailored to the needs of state and local officials, as well as private industry. In addition, according to NIPC's director, as of July 2002, a significant challenge in developing a robust analysis and warning function is the development of the technology and human capital capacities to collect and analyze substantial amounts of information. Similarly, the Director of the FBI testified in June 2002 that implementing a more proactive approach to preventing terrorist acts and denying terrorist groups the ability to operate and raise funds require a centralized and robust analytical capacity that did not then exist in the FBI's Counterterrorism Division.[28] He also stated that processing and exploiting information gathered domestically and abroad during the course of investigations require an enhanced analytical and data mining capacity that was not then available. According to DHS's reorganization plans, the IAIP Under Secretary and the chief information officer (CIO) of the department are to fulfill their responsibilities as laid out by the act to establish and uses a secure communications and IT infrastructure. This infrastructure is to include data-mining and other analytical tools in order to access, receive, analyze, and disseminate data and information.

Additional Incentives Are Needed to Encourage Increased Information Sharing Efforts

PDD 63 stated that sector liaisons should identify and assess economic incentives to encourage sector information sharing and other desired behavior. Consistent with the original intent of PDD 63, the *National Strategy for Homeland Security* states that, in many cases, sufficient incentives exist in the private market for addressing the problems of CIP. However, the strategy also discusses the need to use all available policy tools to protect the health, safety, or well-being of the American people. It mentions federal grant programs to assist state and local efforts, legislation to create incentives for the private sector, and, in some cases, regulation. The physical protection strategy reiterates that additional regulatory directives and mandates should only be necessary in instances where the market forces are insufficient to prompt the necessary investments to protect critical infrastructures and key assets. The cyberspace security strategy also states that the market is to provide the major impetus to improve cybersecurity and that regulation will not become a primary means of securing cyberspace.

Last year, the Comptroller General testified on the need for strong partnerships with those outside the federal government and that the new department would need to design and manage tools of public policy to engage and work constructively with third parties.[29] We have also previously testified on the choice and design of public policy tools that are available to governments.[30] These public policy tools include grants, regulations, tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address security concerns. Some of these tools are already being used, such as in the water and chemical sectors.

Without appropriate consideration of public policy tools, private-sector participation in sector-related information sharing and other CIP efforts may not reach its full potential. For example, we reported in January 2003 [31] on the efforts of the financial services sector to address cyber threats, including industry efforts to share information and to better foster and facilitate sectorwide efforts. We also reported on the efforts of federal entities and regulators to partner with the financial services industry to protect critical infrastructures and to address information security. We found that although federal entities had a number of efforts ongoing, Treasury, in its role as sector liaison, had not undertaken a comprehensive assessment of the potential public policy tools to encourage the financial services sector in implementing information sharing and other CIP-related efforts. Because of the importance of considering public policy tools to encourage private-sector participation, we recommended that Treasury assess the need for public policy tools to assist the industry in meeting the sector's goals. In addition, in February 2003, we reported on the mixed progress five ISACs had made in accomplishing the activities suggested by PDD 63.

---

[28] Testimony of Robert S. Mueller, III, Director Federal Bureau of Investigation, before theSubcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, Committee on Appropriations, U.S. House of Representatives, June 21, 2002.

[29] U.S. General Accounting Office, Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will Be Pivotal to Success, GAO–01–886T (Washington, D.C.: June 25, 2002).

[30] U.S. General Accounting Office, *Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy,* GAO–02–549T (Washington, D.C.: Mar. 28, 2002).

[31] U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats,* GAO–03–173 (Washington, DC,: Jan. 30, 2003).

We recommended that the responsible lead agencies assess the need for public policy tools to encourage increased private-sector CIP activities and greater sharing of intelligence and incident information between the sectors and the federal government.

The President's fiscal year 2004 budget request for the new DHS includes $829 million for information analysis and infrastructure protection, a significant increase from the estimated $177 million for fiscal year 2003. In particular, the requested funding for protection includes about $500 million to identify key critical infrastructure vulnerabilities and support the necessary steps to ensure that security is improved at these sites. Although the funding also includes almost $300 million for warning advisories, threat assessments, a communications system, and outreach efforts to state and local governments and the private sector, additional incentives may still be needed to encourage nonfederal entities to increase their CIP efforts.

Consolidating and Standardizing Watch List Structures and Policies

We recently reported on the terrorist and criminal watch list systems maintained by different federal agencies.[32] These watch lists are important information-sharing tools for securing our nation's borders against terrorists. Simply stated, watch lists can be viewed as automated databases that are supported by certain analytical capabilities. These lists contain various types of data, from biographical data—such as a person's name and date of birth—to biometric data such as fingerprints. Nine federal agencies,[33] which before the establishment of DHS spanned five different cabinet-level departments,[34] currently maintain 12 terrorist and criminal watch lists. These lists are also used by at least 50 federal, state, and local agencies.

According to the *National Strategy for Homeland Security,* in the aftermath of the September 11th attacks, it became clear that vital watch list information stored in numerous and disparate databases was not available to the right people at the right time. In particular, federal agencies that maintained information about terrorists and other criminals had not consistently shared it. The strategy attributed these information-sharing limitations to legal, cultural, and technical barriers that resulted in the watch lists being developed in different ways, for different purposes, and in isolation from one another. To address these limitations, the strategy provides for developing a consolidated watch list that would bring together the information on known or suspected terrorists contained in federal agencies' respective lists.

As we reported, we found that the watch lists include overlapping but not identical sets of data, and that different policies and procedures govern whether and how these data are shared with others. As a general rule, we found that this information sharing is more likely to occur among federal agencies than between federal agencies and either state and local governments agencies or private entities. Among other things, we also found that the extent to which such information sharing is accomplished electronically is constrained by fundamental differences in the watch lists' systems architecture. Also, differences in agencies' cultures have been and remain one of the principal impediments to integrating and sharing information from watch lists and other information. We recommended that the Secretary of DHS, in collaboration with the heads of other departments and agencies that have or use watch lists, lead an effort to consolidate and standardize the federal government's watch list structures and policies to promote better integration and information sharing. DHS generally agreed with our findings and recommendations.

Effective Systems and Processes Need to Be Established to Facilitate Information Sharing

The success of homeland security relies on establishing effective systems and processes to facilitate information sharing among government entities and the private sector. In May 2003, the CIO of DHS stated that a key goal to protecting our nation is to put in place mechanisms that provide the right information to the right people in a timely manner. He further stated that with the use of IT, homeland security officials throughout the United States will have a more complete awareness of threats and vulnerabilities, as well as knowledge of the personnel and resources

---

[32] GA–03–322.

[33] The nine agencies are the State Department's Bureau of Intelligence and Research and Bureau of Consular Affairs; the Justice Department's Federal Bureau of Investigation, Immigration and Naturalization Service, U.S. Marshals Service, and the U.S. National Central Bureau for Interpol; the Department of Defense's Air Force Office of Special Investigations; the Transportation Department's Transportation Security Administration; and the Treasury Department's U.S. Customs Service. Of these, the Immigration and Naturalization Service, the Transportation Security Administration, and the U.S. Customs Service have been incorporated into the new DHS.

[34] These departments are the Departments of State, Treasury, Transportation, Justice, and Defense.

available to conquer those threats. We have identified critical success factors to information sharing that DHS should consider. Also, in addition to the need to develop technological solutions, key management issues that DHS must overcome to achieve success include

- integrating existing IT resources of 22 different agencies,
- making new IT investments,
- ensuring that sensitive information is secured,
- developing secure communications networks,
- developing a performance focus,
- integrating staff from different organizations and ensuring that the department has properly skilled staff, and
- ensuring effective oversight.

Addressing these issues will be critical to establishing the effective systems and processes required to facilitate information sharing within the new department.

Success Factors for Sharing Information

In October 2001, we reported on information sharing practices of organizations that successfully share sensitive or time-critical information.[35] We found that these practices include:

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- developing standards and agreements on how shared information will be used and protected;
- establishing effective and appropriately secure communications mechanisms; and
- taking steps to ensure that sensitive information is not inappropriately disseminated.

Among the organizations we studied, we found some very good models to learn from and build on. For example, CERT/CC is charged with establishing a capability to quickly and effectively coordinate communication between experts in order to limit damage, responding to incidents, and building awareness of security issues across the Internet community. In this role, CERT/CC receives Internet security-related information from system and network administrators, technology managers, and policymakers and provides them with this information along with guidance and coordination to major security events. Further, the Agora is a Seattle-based regional network that at the time of our study had over 600 professionals representing various fields, including information systems security; law enforcement; local, state, and federal governments; engineering; IT; academics; and other specialties. Members work to establish confidential ways for organizations to share sensitive information about common problems and best practices for dealing with security threats. They develop and share knowledge about how to protect electronic infrastructures, and they prompt more research specific to electronic information systems security.

In addition, we have previously reported on several other key considerations in establishing effective information sharing, including:

- identifying and agreeing on the types of information to be collected and shared between parties,
- developing standard terms and reporting thresholds,
- balancing varying interests and expectations, and
- determining the right format and standards for collecting data so that disparate agencies can aggregate and integrate data sets.

Some efforts have already taken place in these areas. For example, NIPC obtained information-sharing agreements with most ISACs, which included specific reporting thresholds for physical and cyber incidents. Also, incident reporting thresholds have been publicly issued. It will be important for DHS to incorporate these considerations into its information-sharing efforts.

Developing Technological Solutions

Developing and implementing appropriate technological solutions can improve the effectiveness and efficiency of information sharing. We have previously reported on the lack of connectivity and interoperability between databases and technologies important to the homeland security effort.[36] Databases belonging to federal law enforcement agencies and INS, for example, are not connected, and databases between state, local, and federal governments are not always connected. The technological constraints caused by different system architectures that impede the sharing of dif-

[35] U.S. General Accounting Office, Information Sharing: Practices That Can Benefit Critical Infrastructure Protection, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

[36] GAO–02–811T

ferent agencies' watch lists illustrate the widespread lack of interoperability of many federal government information systems.

New technologies for data integration and interoperability could enable agencies to share information without the need for radical structural changes. This would allow the component agencies of DHS to work together yet retain a measure of autonomy, thus removing some barriers hindering agencies from embracing change. In August 2002, we reported on various existing technologies that could be more widely implemented to facilitate information sharing.[37] We reported that Extensible Markup Language (XML) is useful for better information sharing. XML is a flexible, nonproprietary set of standards for annotating or "tagging" information so that it can be transmitted over a network such as the Internet and readily interpreted by disparate computer systems. If implemented broadly with consistent data definitions and structures, XML offers the promise of making it significantly easier for organizations and individuals to identify, integrate, and process information that may be widely dispersed among systems and organizations. For example, law enforcement agencies could potentially better identify and retrieve information about criminal suspects from any number of federal, state, and local databases.

We also reported that various technologies could be used to protect information in shared databases. For example, data could be protected through electronically secured entry technology (ESET). ESET would allow users of separate databases to cross check or "mine" data securely without directly disclosing their information to others, thus allowing agencies to collaborate as well as address their needs for confidentiality or privacy. Such technology could, for example, allow an airline to cross check a passenger or employee against data held by government agencies in a single-step process without actually disclosing the data to the airline. In checking an individual, the airline would not receive any data from the agencies' databases; rather, it would receive a "yes or no" type of response and/or a referral for further action. Additionally, appropriate authorities could automatically be notified.

We noted that intrusion detection systems could be used to prevent unauthorized users from accessing shared information. Intrusion detection uses normal system and network activity data as well as known attack patterns. Deviations from normal traffic patterns can help to identify potential intruders.

We also observed the need to simplify the process of analyzing information to more efficiently and effectively identify information of consequence that must be shared. Great emphasis has been placed upon data mining and data integration, but the third and perhaps most crucial component may be data visualization. The vast amount of information potentially available to be mined and integrated must be intelligently analyzed, and the results effectively presented, so that the right people have the right information necessary to act effectively upon such information. This may involve pinpointing the relevant anomalies.

Before DHS was established, the Office of Homeland Security had already begun several technological initiatives to integrate terrorist-related information from databases from different agencies responsible for homeland security. These included (1) adopting meta-data standards for electronic information so that homeland security officials understood what information was available and where it could be found and (2) developing data-mining tools to assist in identifying patterns of criminal behavior so that suspected terrorists could be detained before they could act.

To address these technological challenges, the Homeland Security Act emphasized investments in new and emerging technologies to meet some of these challenges and established the Science and Technology Directorate, making it responsible for establishing and administering research and development efforts and priorities to support DHS missions.

Improving Information Technology Management

Improving IT management will be critical to transforming the new department. DHS should develop and implement an enterprise architecture, or corporate blueprint, to integrate the many existing systems and processes required to support its mission. This architecture will also guide the department's investments in new systems to effectively support homeland security in the coming years. Other key IT management capacities that DHS will need to establish include investment and acquisition management processes, effective IT security, and secure communications networks.

An Enterprise Architecture

Effectively managing a large and complex endeavor requires, among other things, a well-defined and enforced blueprint for operational and technological change, com-

[37] U.S. General Accounting Office, *National Preparedness: Technology and Information Sharing Challenges,* GAO–02–1048R (Washington, D.C.: Aug. 30, 2002).

monly referred to as an enterprise architecture. Developing, maintaining, and using enterprise architectures is a leading practice in engineering both individual systems and entire enterprises. Enterprise architectures include several components, including a (1) current or "as is" environment, (2) target or "to be" environment, and (3) transition plan or strategy to move from the current to the target environment. Governmentwide requirements for having and using architectures to guide and constrain IT investment decision making are also addressed in federal law and guidance.[38] Our experience with federal agencies has shown that attempts to transform IT environments without enterprise architectures often result in unconstrained investment and systems that are duplicative and ineffective. Moreover, our February 2002 report on the federal agencies' use of enterprise architectures found that their use of enterprise architectures was a work in progress, with much to be accomplished.[39]

DHS faces tremendous IT challenges because programs and agencies have been brought together in the new department from throughout the government, each with their own information systems. It will be a major undertaking to integrate these diverse systems to enable effective information sharing among themselves, as well as with those outside the department.

The Office of Homeland Security has acknowledged that an enterprise architecture is an important next step because it can help identify shortcomings and opportunities in current homeland-security-related operations and systems, such as duplicative, inconsistent, or missing information. Furthermore, the President's homeland security strategy identifies, among other things, the lack of an enterprise architecture as an impediment to DHS's systems interoperating effectively and efficiently. Finally, the CIO of DHS has stated that the most important function of his office will be to design and help implement a national enterprise architecture that will guide the department's investment in and use of IT. As part of its enterprise development efforts, the department has established working groups comprising state and local CIOs to ensure that it understands and represents their business processes and strategies relevant to homeland security. In addition, OMB, in its current review of DHS's redundant IT for consolidation and integration, has taken an initial first step to evaluate DHS's component systems.[40] According to an official in the office of the CIO, DHS has compiled an inventory of systems that represents its current enterprise architecture and will soon have a draft of its future enterprise architecture. In addition, this official anticipates having a preliminary road map of the plan to transition to the future enterprise architecture in September 2003 and estimates that DHS will have the plan itself by next winter.

In June 2002, we recommended that the federal government develop an architecture that defined the homeland security mission and the information, technologies, and approaches necessary to perform the mission in a way that was divorced from organizational parochialism and cultural differences.[41] Specifically, we recommended that the architecture describe homeland security operations in both (1) logical terms, such as interrelated processes and activities, information needs and flows, and work locations and users; and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. We observed that a particularly critical function of a homeland security architecture would be to establish protocols and standards for data collection to ensure that data being collected were usable and interoperable and to tell people what they needed to collect and monitor.

The CIO Council, OMB, and GAO have collaborated to produce guidance on the content, development, maintenance, and implementation of architectures that could be used in developing an architecture for DHS.[42] In April, we issued an executive guide on assessing and improving enterprise architecture management that extends this guidance.[43]

---

[38] U.S. General Accounting Office, *Business Systems Modernization: Longstanding Management and Oversight Weaknesses Continue to Put Investments at Risk,* GAO–03–553T (Washington, D.C.: Mar. 31, 2003).

[39] U.S, General Accounting Office, *Information Technology: Enterprise Architecture Use across theFederal Government Can Be Improved,* GAO–02–6 (Washington, D.C.: Feb. 19, 2002).

[40] Office of Management and Budget, *Reducing Redundant IT Infrastructure Related to HomelandSecurity, Memorandum for the Heads of Selected Departments and Agencies,* July 19, 2002, M–02–12.

[41] GAO–02–811T.

[42] See Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture, Version* 1.0, (Washington, D.C.: Feb. 2001).

[43] U.S. General Accounting Office, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1),* GAO–03–584G (Washington, D.C.: April 2003).

Investment and Acquisition Management Processes

The Clinger-Cohen Act, federal guidance, and recognized best practices provide a framework for organizations to follow to effectively manage their IT investments. This involves having a single, corporate approach governing how an organization's IT investment portfolio is selected, controlled, and evaluated across its various components, including assuring that each investment is aligned with the organization's enterprise architecture. The lack of effective processes can lead to cost, schedule, and performance shortfalls, and in some cases, to failed system development efforts. We have issued numerous reports on investment and acquisition management challenges at agencies now transferred into DHS, including INS.

INS has had long-standing difficulty developing and fielding information systems to support its program operations. Since 1990, we have reported that INS managers and field officials did not have adequate, reliable, and timely information to effectively carry out the agency's mission. For example, INS's benefit fraud investigations have been hampered by a lack of integrated information systems.[44] Also, INS's alien address information could not be fully relied on to locate many aliens who were believed to be in the country and who might have knowledge that would assist the nation in its antiterrorism efforts.[45] Contributing to this situation was INS's lack of written procedures and automated controls to help ensure that reported changes of address by aliens are recorded in all of INS's automated databases. Our work has identified weaknesses in INS's IT management capacities as the root cause of its system problems, and we have made recommendations to correct the weaknesses. INS has made progress in addressing our recommendations.

In his written statement for a May 2003 hearing before the House Government Reform Committee, the DHS CIO stated that IT investments, including mission-specific investments, are receiving a departmentwide review. Benefits envisioned from this capital investment and control process include integrating information and identify and eliminating duplicate applications, gaps in information, and misalignments with business goals and objectives.

Sound acquisition management is also central to accomplishing the department's mission. One of the largest federal departments, DHS will potentially have one of the most extensive acquisition requirements in government. The new department is expected to acquire a broad range of technologies and services from private-sector companies.

Moreover, DHS is faced with the challenge of integrating the procurement functions of many of its constituent programs and missions. Inherited challenges exist in several of the incoming agencies. For example, Customs has major procurement programs under way that must be closely managed to ensure that it achieves expectations. Despite some progress, we reported that Customs still lacks important acquisition management controls.[46] For its new import processing system, Customs has not begun to establish process controls for determining whether acquired software products and services satisfy contract requirements before acceptance, nor to establish related controls for effective and efficient transfer of acquired software products to the support organization responsible for software maintenance. Agreeing with one of our recommendations, Customs continues to make progress and plans to establish effective acquisition process controls.

Getting the most from its IT investment will depend on how well the department manages its acquisition activities. High-level attention to strong system and service acquisition management practices is critical to ensuring success.

Information Security Challenges

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency, and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[47] Further,

---

[44] U.S. General Accounting Office, *Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems,* GAO–02–66 (Washington, D.C.: Jan. 31, 2002).

[45] U.S. General Accounting Office, *Homeland Security: INS Cannot Locate Many Aliens Because It Lacks Reliable Address Information,* GAO–03–188 (Washington, D.C.: Nov. 21, 2002).

[46] U.S. General Accounting Office, *Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project,* GAO–02–545 (Washington, D.C.: May 13, 2002).

[47] *Title III—Federal Information Security Management Act of 2002,* E-Government Act of 2002, P.L. 107—347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.

the Homeland Security Act specifically requires DHS to establish procedures to ensure the authorized use and the security and confidentiality of information shared with the department, including information on threats of terrorism against the United States; infrastructure or other vulnerabilities to terrorism; and threatened interference with, attack on, compromise of, or incapacitation of critical infrastructures or protected systems by either physical or computer-based attack. However, establishing an effective information security program may present significant challenges for DHS, which must bring together programs and agencies from throughout the government and integrate their diverse communications and information systems to enable effective communication and information sharing both within and outside the department.

Since 1996, we have reported that poor information security is a widespread problem for the federal government, with potentially devastating consequences.[48] Further, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2003.[49] Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. For the past several years, we have analyzed audit results for 24 of the largest federal agencies,[50] and our latest analyses, of audit reports issued from October 2001 through October 2002, continued to show significant weaknesses in federal computer systems that put critical operations and assets at risk.[51] In particular, we found that all 24 agencies had weaknesses in security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls and covers a range of activities related to understanding information security risks, selecting and implementing controls commensurate with risk, and ensuring that the controls implemented continue to operate effectively. In addition, we found that 22 of the 24 agencies had weaknesses in access controls—weaknesses that can make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage, or in today's increasingly interconnected computing environment, can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise. In April 2003,[52] we also reported that many agencies still had not established information security programs consistent with requirements originally prescribed by government information security reform legislation[53] and now permanently authorized by FISMA.

Considering the sensitive and classified information to be maintained and shared by DHS, it is critical that the department implement federal information security requirements to ensure that its systems are appropriately assessed for risk and that adequate controls are implemented and working properly. Federal information security guidance, such as that issued by the National Institute of Standards and Technology (NIST), can aid DHS in this process. For example, NIST has issued guidance to help agencies perform self-assessments of their information security programs, conduct risk assessments, and use metrics to determine the adequacy of in-place security controls, policies, and procedures.[54] In addition, as we have previously re-

---

[48] U.S. General Accounting Office, Information Security: Opportunities for Improved OMB Oversight of Agency Practices, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

[49] U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures,* GAO–03–121 (Washington, D.C.: January 2003).

[50] U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical FederalOperations and Assets at Risk,* GAO/AIMD–98–92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies,* GAO/AIMD–00–295 (Washington, D.C.: Sept. 6, 2000); *Computer Security: Improvements Needed to Reduce Risk to CriticalFederal Operations and Assets,* GAO–02–231T (Washington, D.C.: Nov. 9, 2001), and *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk,* GAO–02–303T (Washington,D.C.: Nov. 19, 2002).

[51] GAO–03–303T.

[52] GAO–03–564T.

[53] *Title X, Subtitle G—Government Information Security Reform,* Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L.106–398, October 30, 2000.

[54] National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology Systems,* NIST Special Publication 800–26, November 2001; *Risk Management Guide for Information Technology Systems—Recommendations of the National Institute of Standards and Technology, Special Publication* 800–30, January 2002; *Security Metrics Guide for Information Technology Systems,* NIST Draft Special Publication 800–55 (October 2002).

ported, agencies need more specific guidance on the controls that they need to implement to help ensure adequate protection.[55] Currently, agencies have wide discretion in deciding which computer security controls to implement and the level of rigor with which to enforce these controls. Although one set of specific controls will not be appropriate for all types of systems and data, our studies of best practices at leading organizations have shown that more specific guidance is important.[56] In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. Responding to this need, FISMA requires NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

DHS has identified implementing its information security program as a year-one objective. In continuing these efforts, it is important that DHS consider establishing processes to annually review its information security program and to collect and report data on the program, as required by FISMA and OMB.

Secure Communications Networks

The Homeland Security Information Sharing Act, included in the Homeland Security Act of 2002, provides for the President to prescribe and implement procedures for federal agencies to share homeland security and classified information with others, such as state and local governments, through information sharing systems. Provisions of the act depict the type of information to be shared as that which reveals a threat of actual or potential attack or other hostile acts. Grand jury information; electronic, wire, or oral information; and foreign intelligence information are all included in these provisions. The *National Strategy for Homeland Security* also refers to the need for states to use a secure intranet to increase the flow of classified federal information to state and local entities. According to the strategy, this network would provide a more effective way to share information about terrorists. The strategy also refers to putting into place a "collaborative classified enterprise environment" to allow agencies to share information in their existing databases.

To ensure the safe transmittal of sensitive, and, in some cases, classified, information vertically among everyone from intelligence entities, including the CIA, to local entities, such as those involved in emergency response and law enforcement, as well as horizontally across the same levels of government, requires developing and implementing communications networks with adequate security to protect the confidentiality, integrity, and availability of the transmitted information. Furthermore, these communications networks must be accessible to a variety of parties, from federal agencies to state and local government entities and some private entities.

Secure networks for sharing sensitive information between state and federal entities have been implemented and are being used. For example, the National Law Enforcement Telecommunication System (NLETS) links all states and many federal agencies to the FBI's National Crime Information Center (NCIC) network for the exchange of criminal justice information. Another law enforcement system called the Regional Information Sharing System (RISS) links thousands of local, state, and federal agencies to Regional Organized Crime Information Centers. Information sharing networks for the purpose of sharing sensitive information with some federal agencies also exist within the intelligence community. Other agencies are also engaged in efforts to provide homeland security networking and information management support for crisis management activities. Department of Defense officials have also stated that the Army National Guard's network GuardNet, which was used to communicate among the states and the District of Columbia during the September 11 terrorist attacks, is being considered for homeland security mission support. For several years, the states have also been working on efforts to establish an information architecture framework for government information systems integration.

There also appear to be many new efforts under way to implement secure networks. In addition, according to the recently published the cyberspace security strategy, DHS intends to develop a national cyberspace security response system, the Cyber Warning Information Network (CWIN), to provide crisis management support to

[55] GAO–03–121.

[56] U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations,* GAO/AIMD–98–68 (Washington, D.C.: May 1998).

government and nongovernment network operation centers. CWIN is envisioned as providing private and secure network communications for both government and industry for the purpose of sharing cyber alert and warning information. Moreover, the National Communications System, one of the 22 entities that were merged into the DHS, has implemented a pilot system, the Global Early Warning Information System (GEWIS), which will measure how critical areas of the Internet are performing worldwide and then use that data to notify government, industry, and allies of impending cyber attacks or possible disturbances.

It was also recently reported that the Justice Department and the FBI are expanding two existing sensitive but unclassified law enforcement networks to share homeland security information across all levels of government. When fully deployed, their Antiterrorism Information Exchange (ATIX) will provide law enforcement agencies at all levels access to information. Law enforcement agencies also can use ATIX to distribute security alerts to private-sector organizations and public officials who lack security clearances. Users, who will have different access levels on a need-to-know basis, will include a broad range of public safety and infrastructure organizations, including businesses that have homeland security concerns and duties. They will have access to a secure E-mail system via a secure Intranet, which the FBI and DHS will use to deliver alerts to ATIX users. The FBI and other federal agencies, including DHS, will link to ATIX via Law Enforcement Online, the bureau's system for sensitive-but-unclassified law enforcement data that provides an encrypted communications service for law enforcement agencies on a virtual private network. The second Department of Justice and FBI network, the Multistate Antiterrorism Regional Information Exchange System, will enable crime analysts working on terrorism investigations to quickly check a broad range of criminal databases maintained by federal, state, and local agencies.

DHS reportedly is establishing secure videoconferencing links with emergency operations centers in all 50 states, as well as two territories and the District of Columbia. Also, the DHS CIO has stated that a major initiative in implementing the department's IT strategy for providing the right information to the right people at all times is establishing the DHS Information Sharing Network Pilot project. Moreover, he sets 2005 as a milestone for DHS to build a "network of networks." However, at this time, we do not have information on these projects or the extent to which they will rely on existing networks. It is also not clear how the DHS "network of networks" architecture will work with the state architecture being developed by the National Association of State CIOs.

Managing Performance

As we have previously reported,[57] the new department has the challenge of developing a national homeland security performance focus, which relies on related national and agency strategic and performance planning efforts of the Office of Homeland Security, OMB, and the other departments and agencies. Indeed, the individual planning activities of the various component departments and agencies represent a good start in the development of this focus. However, our past work on implementation of the Government Performance and Results Act (GPRA) has highlighted ongoing difficulty with many federal departments and agencies setting adequate performance goals, objectives, and targets. Accordingly, attention is needed to developing and achieving appropriate performance expectations and measures for information sharing and in ensuring that there is linkage between DHS's plans, other agencies' plans, and the national strategies regarding information sharing. Ensuring these capabilities and linkages will be vital in establishing comprehensive planning and accountability mechanisms that will not only guide DHS's efforts but also help assess how well they are really working.

As we previously reported,[58] one of the barriers that the new department faces in establishing effective homeland security is interagency cooperation, which is largely attributed to "turf" issues among the 22 component agencies subsumed by the new department. Strong and sustained commitment of agency leaders would provide performance incentives to managers and staff to break down cultural resistance and encourage more effective information sharing pertaining to homeland security. Moreover, agency leaders have a wide range of tools at their disposal for enforcing and rewarding cooperative efforts, including performance bonuses for senior executives and incentive award programs for staff.

Our studies of other cross-cutting federal services with similar "turf" problems have also shown that agency performance plans, which are required by GPRA, offer a

[57] U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security,* GAO–03–102 (Washington, D.C.: January 2003).

[58] GAO–02–1048R.

good avenue for developing incentives to cooperate. Specifically, agencies can set up goals in their performance plans for participation in cross-cutting programs and report on their progress in meeting these goals to the Congress. The Congress could also build similar incentives into budget resolutions.

Shared programmatic goals and metrics would also encourage cooperation and coordination. Agencies subsumed by DHS should all participate in the development of goals, milestones, and metrics to measure progress and success, and such indicators should be clearly articulated and endorsed by senior management. Such goals and metrics must be carefully chosen since how performance is measured greatly influences the nature of the performance itself; poorly chosen metrics may lead to unintended or counterproductive results. However, visible, clearly articulated and carefully chosen shared goals and metrics can effectively overcome "turf" issues. Developing metrics to measure the success of these activities is critical to ensuring a successful effort. Similar indicators more directly related to information sharing could be developed.

Emphasizing Human Capital

Human capital is another critical ingredient required for ensuring successful information sharing for homeland security. The cornerstones to effective human capital planning include leadership; strategic human capital planning; acquiring, developing, and retaining talent; and building results-oriented organizational cultures. The homeland security and intelligence communities must include these factors in their management approach in order to benefit from effective collaboration in this critical time.

As we have previously reported, the governmentwide increase in homeland security activities has created a demand for personnel with skills in areas such as IT, foreign language proficiencies, and law enforcement, without whom critical information has less chance of being shared, analyzed, integrated, and disseminated in a timely, effective manner.[59] We specifically reported that shortages in staffing at some agencies had exacerbated backlogs in intelligence and other information, adversely affecting agency operations and hindering U.S. military, law enforcement, intelligence, counterterrorism, and diplomatic efforts.[60]

We have also previously reported that some of the agencies that moved into DHS have long-standing human capital problems that will need to be addressed. One of these challenges has been the ability to hire and retain a talented and motivated staff. For example, we reported that INS has been unable to reach its program goals in large part because of such staffing problems as hiring shortfalls and agent attrition.[61] We also reported that several INS functions have been affected by the lack of a staff resource allocation model to identify staffing needs.[62] We concluded then that it was likely that increased attention to the enforcement of immigration laws and border control would test the capacity of DHS to hire large numbers of inspectors for work at our nation's border entry points. Moreover, we reported that other agencies being integrated into DHS were also expected to experience challenges in hiring security workers and inspectors. For example, we reported that the Agriculture Department, the Customs Service, INS, and other agencies were all simultaneously seeking to increase the size of their inspections staffs.[63]

To overcome its significant human capital shortfalls, DHS must develop a comprehensive strategy capable of ensuring that the new department can acquire, develop, and retain the skills and talents needed to prevent and protect against terrorism. This requires identifying skill needs; attracting people with scarce skills into government jobs; melding diverse compensation systems to support the new department's many needs; and establishing a performance-oriented, accountable culture that promotes employee involvement and empowerment. In February, the DHS CIO acknowledged the lack of properly skilled IT staff within the component agencies. Challenges facing DHS in this area, he stated, include overcoming political and cultural barriers, leveraging cultural beliefs and diversity to achieve collaborative change, and recruiting and retaining skilled IT workers. He acknowledged that the department would have to evaluate the talent and skills of its IT workforce to identify existing skill gaps. He further stated that a critical component of DHS's IT strategic plan would address the actions needed to train, reskill, or acquire the nec-

---

[59] GAO–02–1122T.

[60] U.S. General Accounting Office, *Foreign Languages: Human Capital Approach Needed to Correct Staffing and Proficiency Shortfalls,* GAO–02–375 (Washington, D.C.: January 2002).

[61] U.S. General Accounting Office, *Immigration Enforcement: Challenges to Implementing the INSInterior Enforcement Strategy,* GAO–02–861T (Washington, D.C.: June 19, 2002).

[62] U.S. General Accounting Office, Immigration and Naturalization Service: Overview of RecurringManagement Challenges, GAO–02–168T (Washington, D.C.: Oct. 17, 2001).

[63] GAO–03–260.

essary skills to achieve a world-class workforce. He committed to working closely with the department's Chief Human Capital Officer and with the Office of Personnel Management to achieve this goal. He set July 2003 as a milestone for developing a current inventory of IT skills, resources, and positions and September 2003 as the targeted date for developing an action plan.

Ensuring Institutional Oversight

It is important to note that accountability is also a critical factor in ensuring the success of the new department. The oversight entities of the executive branch—including the inspectors general, OMB, and the Office of Homeland Security—have a vital role to play in ensuring expected performance and accountability. Likewise, congressional committees and GAO, as the investigative arm of the legislative branch, with their long-term and broad institutional roles, also have roles to play in overseeing that the new department meets the demands of its homeland security mission.

In summary, information sharing with and between all levels of government and the private sector must become an integral part of everyday operations if we are to be able to identify terrorist threats and protect against attack. As such, information sharing is an essential part of DHS's responsibilities and is critical to achieving its mission. To implement these responsibilities, DHS will need to develop effective information sharing systems and other information sharing mechanisms. The department will also need to develop strategies to address other challenges in establishing its organization and information architecture and in developing effective working relationships, cooperation, and trust with other federal agencies, state and local governments, and the private sector.

Messrs. Chairmen, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittees may have at this time.

Contacts and Acknowledgements

For information about this statement, please contact Robert Dacey, Director, Information Security Issues, at (202) 512–3317, or William Ritt, Assistant Director, at (202) 512–6443. You may also reach them by E-mail at daceyr@gao.gov or rittw@gao.gov. Individuals who made key contributions to this testimony include Mark Fostek, Sophia Harrison, and Barbarol James.

August 14, 2003 Outage
Sequence of Events
U.S./Canada Power Outage Task Force
September 12, 2003

This is an outline of significant physical and electrical events that occurred in a narrow window of time, before and during the cascade that led to the blackout of August 14, 2003. This outline reviews events beginning at approximately noon on that day, to provide a ″picture″ of the sequence of events and how the grid situation evolved over the afternoon. It focuses chiefly on events that occurred on major transmission facilities (230 kilovolts and greater) and at large power plants.

This outline does not attempt to present or explain the linkages between the sequences of events that are described. Determining those linkages will require additional intensive analysis over the weeks to come. In the coming weeks, our experts will continue to analyze data from:

- the thousands of transmission line events that occurred on the 138 kV system and on lower voltage lines over the severnl hours before and during the grid's collapse
- the hundreds of events related to power plant internctions with the grid during this period
- the conditions and operntions on the grid before noon. Many things happened well before noon—including reactive power and voltage problems and flow patterns across several states—that may be relevant in a causal sense to the blackout.
- any actions taken, or not taken, by system operators prior to or during the outage.

The U.S. Canada Power Outage Task Force investigation is looking at all of the above factors and more in order to refine these data and dig deeper into what happened and why.

This timeline is not intended to indicate and should not be assumed to explain why the blackout happened, only to provide an early picture of what happened. It is not intended to indicate and should not be assumed to assign fault or culpability for the blackout. Determining the specific causes of these failures requires a thorough and professional investigation, which the bi-national investigative team has undertaken. The above concerns and explanations will be addressed in future reports prepared by the investigative team and issued by the Joint U.S.lCanada Task Force.

Note: The information in this report is based on what is known about the August 14, 2003 blackout as of September 11, 2003, and is subject to change based on further investigation of this event.

August 14, 2003 Outage
Sequence of Events

This report provides the sequence of some of the significant events that led to the blackout of the electric systems in the Mid-west and Northeast United States and eastern Canada on August 14, 2003. This explanation is intended to provide a general understanding of how the blackout evolved; it does not include every detail that is relevant and necessary to fully understand the root causes of the blackout. Such details are within the thousands of records of data that need further analysis. Those data records include circuit breaker operations, power plant startups and shutdowns, voltage changes, power flow shifts, and load shedding. A joint team from the United States and Canada is conducting a thorough investigation of the blackout and will provide appropriate details in a future report.

Event Times

The times listed in this summary were derived from the "time stamp" that accompanied each data record. Whenever a circuit breaker opens to disconnect a transmission line or closes to reconnect a line, or generating unit is brought on line or off, or voltage exceeds a specified limit, the time that event occurred is recorded to the nearest second (and sometimes to the fraction of a second).

In some cases, the investigators discovered that these time stamps were not accurate because the computers that recorded the information became backlogged, or the clocks from which the time stamps were derived had not been calibrated to the national time standard. Investigators must determine which events are accurately time-stamped, and build from those events to cross-check other system events from multiple sources to verify the precise time for each event. Some of these events are still not known to the exact second.

All times in the chronology are in Eastern Daylight Time.

Voltage Collapse

One of the characteristics of the August 14 blackout was an apparent "voltage collapse" that occurred on portions of the transmission system surrounding and within the northern Ohio and eastern Michigan load centers. Transmission system voltage is needed to transfer electric power from the generation stations to the load centers, and is somewhat similar in function to water main pressure. Reactive power is the component of total power that assists in maintaining proper voltages across the power system. Sufficient voltage is maintained by supplying the transmission system with reactive power from generating stations and static devices called capacitors. Lightly-loaded transmission lines also provide reactive power and help sustain system voltage. Conversely, customer loads such as motors and other electromagnetic devices consume reactive power, as do heavily loaded transmission lines. Therefore, as transmission lines become more heavily loaded, they consume more of the reactive power needed to maintain proper transmission voltage.

Reactive power cannot travel long distances because it meets considerable resistance over the transmission lines. Therefore, reactive power sources need to be close to the point of reactive power demand — for example, near the load centers. When heavily loaded transmission lines disconnect, the lines that remain in service automatically pick up portions of flow from the disconnected line, which increases the reactive power consumed by these lines. When reactive supply is limited, the increased loading will cause a voltage drop along the line. If reactive supply is not provided at the end of the line, the voltage could fall precipitously. At that point, the transmission system can no longer transfer electric power from distant generation to energy users in load centers.

In some instances, the reactive power demand within an area is too great for the local generating units to supply. In those cases, the units can trip off line (automatic separation or shut-down), either from reactive power overload, or because the system voltage has become too low to provide power to the generators' own auxiliary equipment, such as fans, coal pulverizers, and pumps.

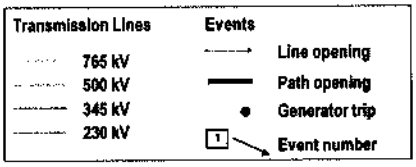
The power system is designed to ensure that if conditions on the grid (excessive or inadequate voltage, apparent impedance or frequency) threaten the safe operation of the transmission lines or power plants, the threatened equipment automatically separates from the network to protect itself from physical damage. Physical damage, if allowed to occur, would make restoration more difficult and much more expensive.

Pre-blackout Conditions

Most of the events that appear to have contributed to the blackout occurred during the period from about noon EDT until 4:13 p.m. EDT. Generation and transmission operating events plus scheduled interchange through the systems in the region may have affected events later in the day. The investigators are studying these events beginning at 8 a.m. on August 14 to determine whether they were significant to the blackout.

Map Key

The key on the right explains the lines and symbols on the maps that accompany this description of events. An "open path" or "open line" means that one or more transmission lines can no longer carry electricity between two areas; a "generator trip" means the generator separates from the grid and stops producing electricity.

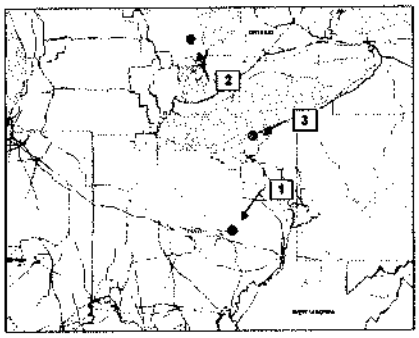


Events Leading to the Blackout

12:05:44 – 1:31:34 PM – Generator trips

1. 12:05:44 – Conesville Unit 5 (rating 375 MW)
2. 1:14:04 – Greenwood Unit 1 (rating 785 MW)
3. 1:31:34 – Eastlake Unit 5 (rating: 597 MW)

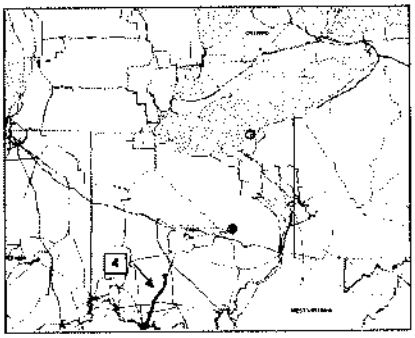
Conesville plant is in central Ohio and Greenwood plant is north of the Detroit area. Greenwood Unit 1 tripped at 1:14:04 and returned to service at 1:57. Eastlake Unit 5 is in northern Ohio along the southern shore of Lake Erie and is connected to the 345 kV transmission system. These generating unit trips (shutdowns) caused the electric power flow pattern to change over the transmission system.



2:02 PM – Transmission line disconnects in southwestern Ohio

4. Stuart – Atlanta 345 kV

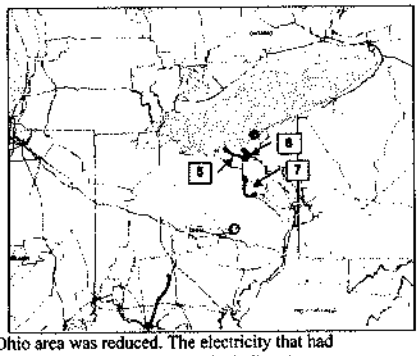
This line is part of the transmission pathway from southwestern Ohio into northern Ohio. It disconnected from the system due to a brush fire under a portion of the line. Hot gases from a fire can ionize the air above a transmission line, causing the air to conduct electricity and short-circuit the conductors.



3:05:41 – 3:41:33 PM – Transmission lines disconnect between eastern Ohio and northern Ohio

5. 3:05:41 – Harding-Chamberlain 345 kV
6. 3:32:03 – Hanna-Juniper 345 kV
7. 3:41:33 – Star-South Canton 345 kV

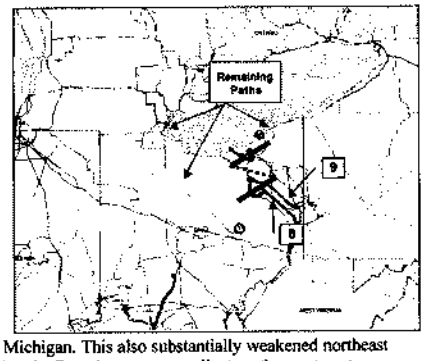
These three transmission lines are part of the pathway into northern Ohio from eastern Ohio. At this time, the reason for the Harding-Chamberlain line going out of service is unknown. The Hanna-Juniper line contacted a tree, creating a short-circuit to ground that caused the line to disconnect itself. The Star-South Canton line had disconnected and reclosed twice earlier in the day, but the significance of those events is not yet clear.



With these lines disconnected, the effectiveness of the transmission path from eastern Ohio into the northern Ohio area was reduced. The electricity that had been flowing over these lines instantly began flowing over other transmission lines, including the underlying 138 kV systems, that connect northern Ohio to the grid. However, this new power flow pattern began to overload those other lines as well. As voltage was dropping, demand of about 600 MW disconnected in the northern Ohio area from industrial customers (whose motors dropped off line due to low voltage) and distribution-level customers who were disconnected automatically from the 138 and 69 kV transmission system.

3:45:33 – 4:08:58 PM – Remaining transmission lines disconnect from eastern into northern Ohio

8. 3:45:33 – Canton Central-Tidd 345 kV
9. 4:06:03 – Sammis-Star 345 kV

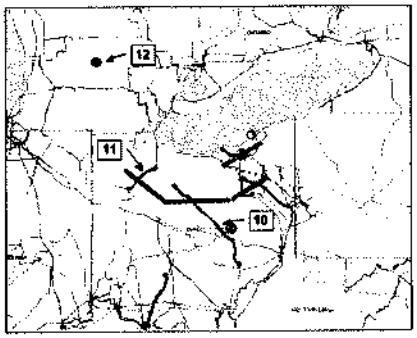


Canton Central-Tidd disconnected at 3:45:33 and reconnected 58 seconds later. However, the Canton Central 345/138 kV transformers disconnected and did not reconnect, isolating the 138 kV system from the 345 kV support at the Canton Central substation. The Sammis-Star 345 kV line then disconnected at 4:06:03, which completely blocked the 345 kV path into northern Ohio from eastern Ohio. This left only three paths for power to flow into northern Ohio: 1) from northeastern Ohio and Pennsylvania around the southern shore of Lake Erie, 2) from southern Ohio (recall, however, that part of that pathway was severed following the Stuart-Atlanta line trip at 2:02), and 3) from eastern Michigan. This also substantially weakened northeast Ohio as a source of power to eastern Michigan, making the Detroit area more reliant on the west-east Michigan lines and the same southern and western Ohio transmission lines.

During the period 3:42:49-4:08:58, multiple 138 kV lines across northern Ohio disconnected themselves. This blacked out Akron and the areas west and south.

4:08:58 – 4:10:27 PM – Transmission lines into northwestern Ohio disconnect, and generation trips in central Michigan

10. 4:08:58 – Galion-Ohio Central-Muskingum 345 kV
11. 4:09:06 – East Lima-Fostoria Central 345 kV
12. 4:09:23-4:10:27 – Kinder Morgan (rating: 500 MW; loaded to 200 MW)



When the Galion-Ohio Central-Muskingum and East Lima-Fostoria Central transmission lines disconnected, this blocked the transmission paths from southern and western Ohio into northern Ohio and eastern Michigan. Thus the combined northern Ohio and eastern Michigan load centers were connected only by the transmission lines from: 1) northeastern Ohio and Pennsylvania along the southern shore of Lake Erie; 2) western Michigan via the west-east lines that cross the state; and 3) Ontario. Eastern Michigan was connected to northern Ohio only by three 345 kV transmission lines near the southwestern bend of Lake Erie.

The Kinder Morgan generating unit tripped (shut down) in central Michigan (loaded to 200 MW).

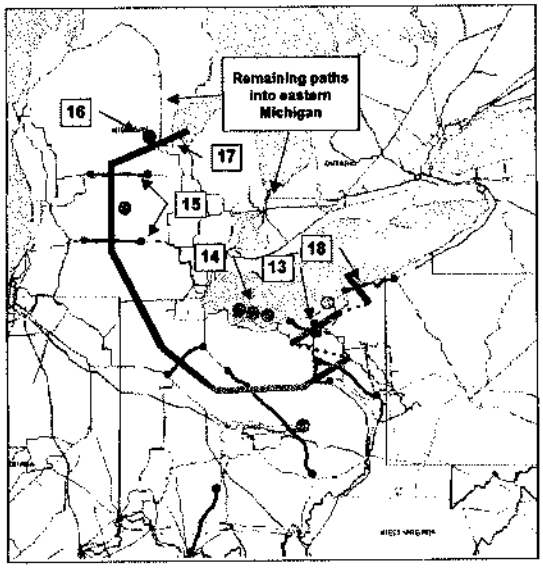
Power flows became heavy from Indiana and over the west-east Michigan transmission lines to serve loads in eastern Michigan and northern Ohio.

The reduced transmission capacity serving the northern Ohio load centers resulted in the transmission voltage becoming depressed in that area as load exceeded the rapidly declining power delivery capability.

At about 4:09, the Eastern Interconnection frequency rose by 0.020 – 0.027 Hz, which represents a demand loss in the range of 700 – 950 MW.

4:10:00 – 4:10:38 PM – Transmission lines disconnect across Michigan and northern Ohio, generation trips off line in northern Michigan and northern Ohio, and northern Ohio separates from Pennsylvania

13. 4:10 – Harding-Fox 345 kV
14. 4:10:04 – 4:10:45 – Twenty generators along Lake Erie in northern Ohio (loaded to 2174 MW total)
15. 4:10:37 – West-East Michigan 345 kV
16. 4:10:38 – Midland Cogeneration Venture (loaded to 1265 MW)
17. 4:10:38 – Transmission system separates northwest of Detroit
18. 4:10:38 – Perry-Ashtabula-Erie West 345 kV



Twenty generators (loaded to 2174 MW) tripped off line along Lake Erie during the period 4:10:04 – 4:10:45. The loss of this generation increased the power flows into the northern Ohio and eastern Michigan load centers on the remaining paths, which included the west-east transmission lines that cross Michigan.

The west-east Michigan 345 kV paths then disconnected at 4:10:37, leaving eastern Michigan connected by only a circuitous path around northern Michigan that disconnected one second later, and the connections to Ontario and northern Ohio. Investigators are still studying the power flows that resulted.

At 4:10:38, the Midland Cogeneration Venture (MCV), loaded to 1265 MW, tripped off line.

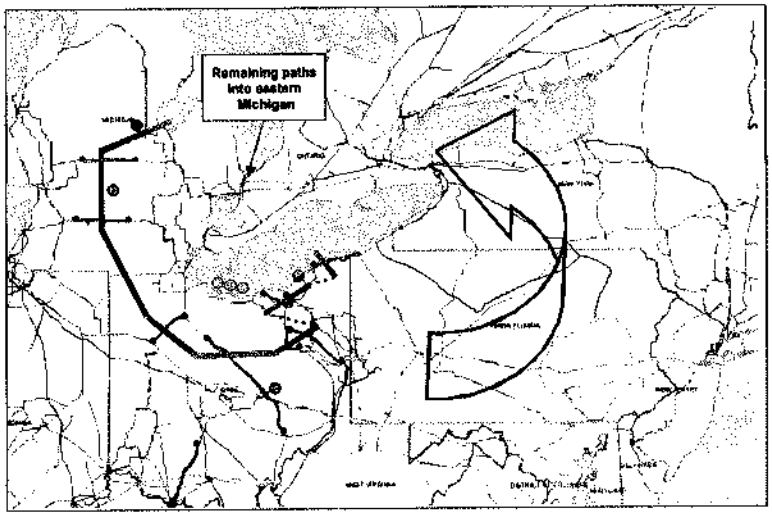
The MCV generation trip imposed heavier flows on the remaining transmission system, and left eastern Michigan and northern Ohio with very depressed voltages. The remaining transmission paths into the Detroit area from the northwest separated.

At 4:10:38, the Perry-Ashtabula-Erie West 345 kV transmission line tripped, severing the path into the northern Ohio area from Pennsylvania along the southern shore of Lake Erie.

Summary of the Situation at 4:10:38

When the Perry-Ashtabula-Erie West 345 kV transmission line disconnected at 4:10:38, the entire eastern Michigan and northern Ohio load centers had little generation left available to them and the voltage was declining. The only connection between those load centers and the rest of the Eastern Interconnection was at the interface between the Michigan and Ontario systems. Also, the frequency was declining in northern Ohio in those areas that had separated from the Interconnection.

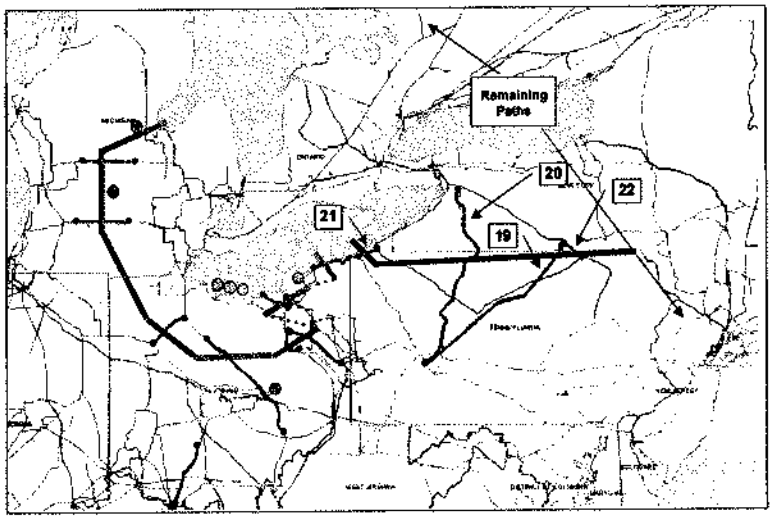
When the transmission lines along the southern shore of Lake Erie disconnected, the power that had been flowing along that path immediately reversed direction and began flowing in a giant loop counterclockwise from Pennsylvania to New York to Ontario and into Michigan.



We now turn our attention to the Pennsylvania, New York, Ontario, Québec, and Maritimes areas.

4:10:40 – 4:10:44 PM – Four transmission lines disconnect between Pennsylvania and New York

19. 4:10:40 – Homer City-Watercure Road 345 kV
20. 4:10:40 – Homer City-Stolle Road 345 kV
21. 4:10:41 – South Ripley-Dunkirk 230 kV
22. 4:10:44 – East Towanda-Hillside 230 kV



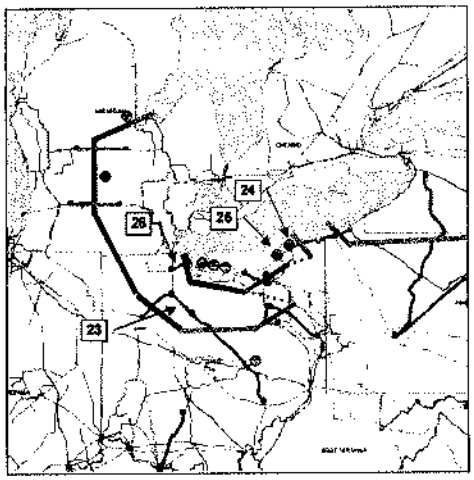
Responding to the surge of energy flowing north out of Pennsylvania through New York and Ontario into Michigan, these four lines disconnected within four seconds of one another and separated Pennsylvania from New York.

At this point, the northern part of the Eastern Interconnection (which still included the rapidly dwindling load in eastern Michigan and northern Ohio) remained connected to the rest of the interconnection at only two locations: 1) in the east through the ties between New York and New Jersey, and 2) in the west through the 230 kV transmission line between Ontario, Manitoba, and Minnesota.

Heavy power flows were moving northward over the New York-New Jersey ties.

4:10:41 PM – Transmission line disconnects and generation trips in northern Ohio

23. Fostoria Central-Galion 345 kV
24. Perry 1 nuclear unit (rated 1252 MW)
25. Avon Lake 9 unit (rated 616 MW)
26. Beaver-Davis Besse 345 kV



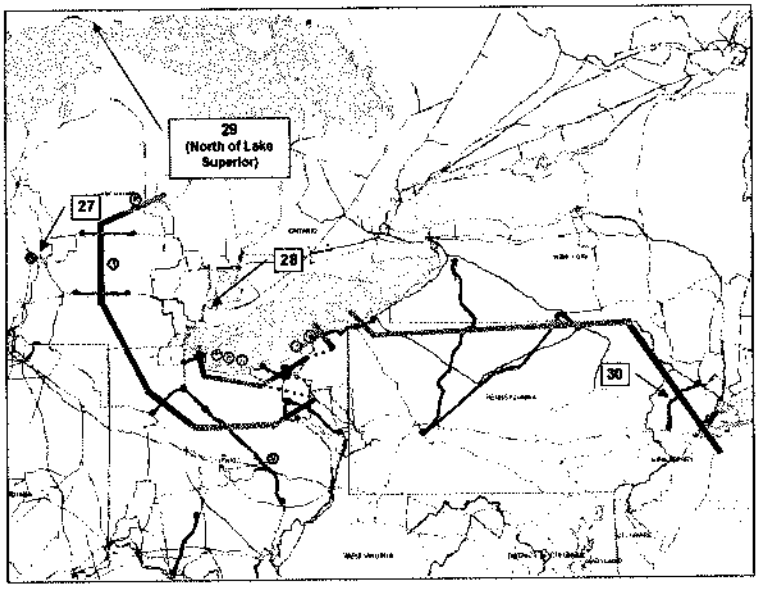
The Fostoria Central-Galion line forms part of the pathway from central to northern Ohio. That path was already blocked by the combination of the Galion-Muskingum-Ohio Central line disconnecting at 4:08:58, and the East Lima-Fostoria Central line disconnecting at 4:09:06.

Perry 1 nuclear unit, located on the southern shore of Lake Erie near the border with Pennsylvania, and Avon Lake 9, located near Cleveland, tripped off line at virtually the same time.

When the Beaver-Davis Besse 345 kV line, which connects the Cleveland and Toledo areas, disconnected, it left the Cleveland area isolated from the Eastern Interconnection. Cleveland area load was disconnected first by automatic underfrequency load shedding, and finally by the disconnection of the transmission lines.

4:10:42 – 4:10:45 PM – Transmission paths disconnect in northern Ontario and New Jersey, isolating the northeast portion of the Eastern Interconnection

27. 4:10:42 – Campbell unit 3 (rated 820 MW) trips
28. 4:10:43 – Keith-Waterman 230 kV
29. 4:10:45 – Wawa-Marathon 230 kV
30. 4:10:45 – Branchburg-Ramapo 500 kV



At 4:10:43, eastern Michigan was still connected to Ontario, but the Keith-Waterman 230 kV line that forms part of that interface disconnected.

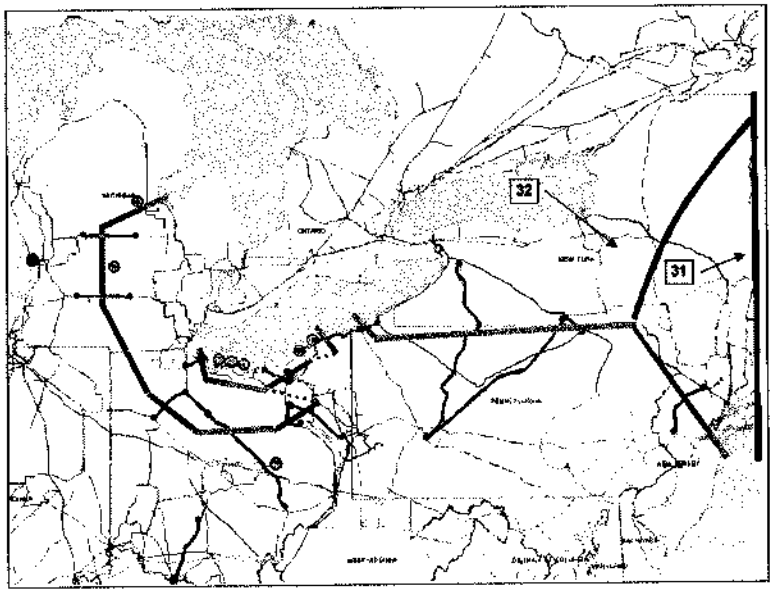
At 4:10:45, the Ontario system separated when the Wawa-Marathon 230 kV line disconnected along the northern shore of Lake Superior. The portion of Ontario to the west of Wawa remained connected to Manitoba and Minnesota.

At the same time, the Branchburg-Ramapo 500 kV line was now the remaining link between the Eastern Interconnection and the area ultimately affected by the blackout, and that line disconnected at 4:10:45 along with the underlying 230 and 138 kV ties in New Jersey. This left the northern part of New Jersey connected to New York. Pennsylvania and the remainder of New Jersey remained connected to the Eastern Interconnection.

At this point, the Eastern Interconnection was split into two sections separated by an east-to-west line. To the north of that line was New York City, northern New Jersey, New York, New England, the Maritime

provinces, eastern Michigan, the majority of Ontario, plus the Québec system. To the south of that line was the rest of the Eastern Interconnection, which was not affected by the blackout.

4:10:46 – 4:10:55 PM – New York splits east-to-west. New England (except southwestern Connecticut) and the Maritimes separate from New York and remain intact.



During the next nine seconds, several separations occurred between the areas in the northern section of the Eastern Interconnection.

31. 4:10:46– 4:10:55 – New York-New England transmission lines disconnect

The ties between New York and New England disconnected during this period, and most of the New England area became an island with generation and demand balanced close enough that it could remain operational. However, southwestern Connecticut was separated from New England and remained tied to the New York system for about one minute.

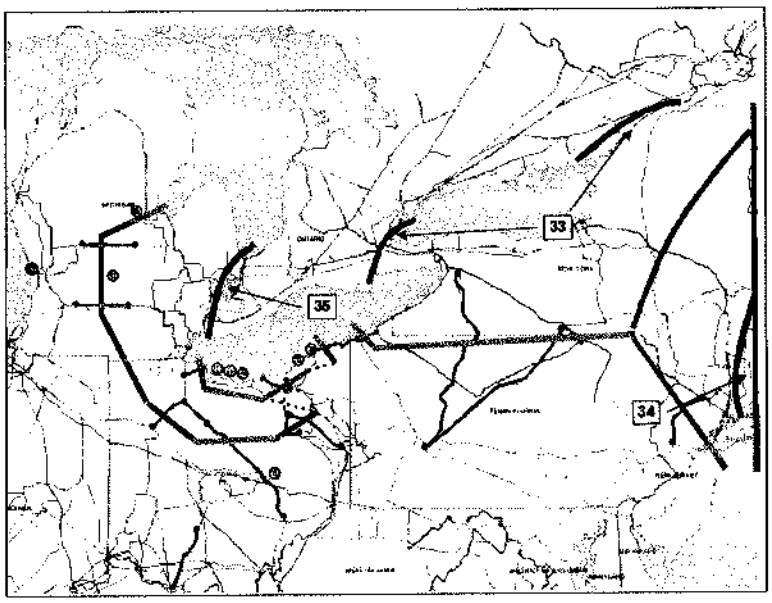
32. 4:10:48 – New York transmission splits east-west.

The transmission system in New York split along an east-west line, with northern New Jersey and southwestern Connecticut connected to the eastern part of the New York system, and Ontario and eastern Michigan connected to the western part. During the next second, Ontario and New York would separate,

with 15% of the demand across New York state disconnected automatically. About 2500 MW of Ontario demand automatically disconnected as Ontario attempted to rebalance its system.

4:10:50 – 4:11:57 PM – Ontario separates from New York west of Niagara Falls and west of St. Lawrence. Southwestern Connecticut separates from New York and blacks out.

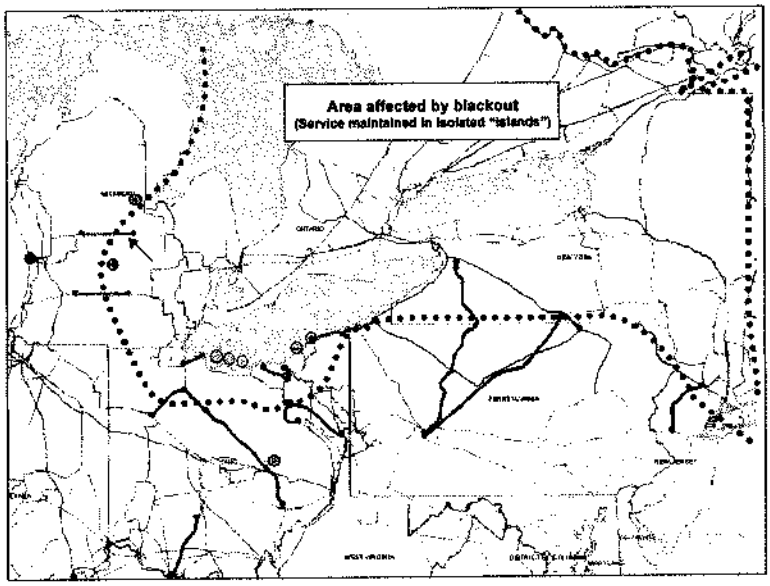
33. 4:10:50– The Ontario system just west of Niagara Falls and west of St. Lawrence separates from New York.
34. 4:11:22 – Long Mountain – Plum Tree 345 kV
35. 4:11:57 – Remaining transmission lines between Ontario and eastern Michigan separate



The Ontario-New York separation at 4:10:50 left New York's and Ontario's large hydro and some thermal generators at Niagara and St. Lawrence, as well as the 765 kV and direct current interties with Québec, connected to the New York system, supporting the demand in upstate New York just south of Lake Ontario. Three of the transmission circuits near Niagara automatically reconnected Ontario to New York at 4:10:56. Another 4500 MW of Ontario demand automatically disconnected. At 4:11:10, the Niagara lines disconnected again, and New York and Ontario again separated. Most of Ontario blacked out after this separation, leaving 22,500 MW of demand disconnected out of a total demand of about 24,000 MW. The eastern New York island blacked out with only scattered small pockets of service remaining. The western New York island continued to serve about 50% of the demand in that island.

When Long Mountain-Plum Tree (connected to Pleasant Valley substation in New York) disconnected, it left southwestern Connecticut connected to New York only through the 138 kV cable that crosses Long Island Sound. About 500 MW of southwest Connecticut demand was disconnected by automatic grid operations. Twenty-two seconds later the Long Island Sound cable disconnected, islanding southwest Connecticut and blacking it out.

4:13 PM – Cascading sequence essentially complete



The major portion of the northern section of the Eastern Interconnection (the area within the dotted line in the map above) was blacked out.

Some isolated areas of generation and load remained on line for several minutes. Some of those areas in which a close generation-demand balance could be maintained remained operational; other generators ultimately tripped off line and the areas they served were blacked out.

One relatively large island remained in operation serving about 5700 MW of demand, mostly in western New York. This service was maintained by generating stations south of Lake Ontario with Ontario generators at Niagara and St. Lawrence as well as the 765 kV and DC interties with Québec. This island formed the basis for restoration in both New York and Ontario.

Conclusion

This sequence of events for the August 14, 2003 blackout summarizes some of the many significant events that occurred before and during this widespread and complex system failure. It reflects events that have been identified and verified as of September 10, 2003. Much more data collection, analysis, and research must be completed before the Joint United States-Canada Power Outage Task Force will be able to state with confidence exactly what happened and why it happened. Our understanding of the events described here, and of those not yet fully catalogued, may change as the investigation progresses. The Task Force's future reports will include a more detailed timeline, and will address the causal relationships among these events.

Mr. SESSIONS. I thank the gentleman for his testimony.

At this time I would yield to the gentleman from Michigan, Mr. Camp, for such time as he may consume.

Mr. CAMP. I thank the Chairman for yielding.

Colonel McDaniel, it was certainly a trying time for all of us in Michigan. I want to thank you for your role in what I know were difficult days. My question was, in your role as homeland security adviser to the governor and as adjutant general for homeland security, what do you think, from your perspective, and also from the perspective of the State of Michigan, what do you think are the most important factors we should weigh as a committee in terms of how to prevent something like this from happening again, and also how to deal with it? You mentioned some of that in your testimony, but what do you think are the most critical things we ought to think about?

Colonel MCDANIEL. Thank you very much for this opportunity.

I am not sure that I can give you any real direction at this point on how to prevent it from happening again without really knowing the causes of it. Certainly, though, there are a number of lessons that we can take a way from it. First of all is the old military truism that no operational plan survives the first contact with the enemy. I think it was very important that we had a state response plan in place, that we had exercised that plan on a number of occasions, that everybody knew their role, and that therefore even though we had, frankly, new players in some of the roles, that everybody was able to step right in and work that plan because we had already exercised it earlier this year.

Secondly, the issue of communications is always going to be one that has to, no matter what the event is, communications is always going to be a key factor, no matter what way it goes. So I think that having some sort of redundant communication system is really vitally important. Thirdly, we are still in the early stages of having the states and the Department of Homeland Security work together, and that is a role that we need to really, really flesh out the skeleton of that plan, I think.

Mr. CAMP. How well did the states communicate with each other during that time? And also, the Canadian provinces? And did the federal government have any role in facilitating that?

Colonel MCDANIEL. There really was not much communications between states at that point. I really think that when you look at this type of event, that that is the role for the Department of Homeland Security or the Department of Energy. We need to focus on the response, on the consequence management. I think that they can do the 30,000-foot view and say, first of all, is this manmade or is natural? If it is manmade, is it intentional? If it is not, is it still ongoing? What are the parameters? What other resources need to be brought to bear? They can do that overall view, and we can focus on what our state resources are and what other resources might be necessary.

Mr. CAMP. What affect did the blackout have on fire, police, medical emergency personnel that you could discuss, and were there telecommunications problems particularly?

Colonel MCDANIEL. Right. As I indicated briefly in my testimony, Mr. Chairman, there were a number of problems that we had.

Number one, traffic signals not functioning is one of those problems that we should have taken care of years ago. I think that that really highlights an important need, because right there you have first responders diverted from where they might be needed to doing a fairly mundane traffic control function.

Secondly, it was interesting to see that a lot of first responders at our local units were relying upon cell phones that did not have an adequate radio system, and a number of cell towers did not have backup systems that worked.

If I could just follow up briefly, almost every type of critical infrastructure that should have a generator did have some sort of generator. However, getting back to my comment about the plans not surviving first contact, they had not tested those generators under load, so we had a lot of generators that just didn't work. They might have fired them up before, but they never tested them under a load and actually had them producing electricity. If this had continued, I think we would have had a problem with the amount of energy necessary for those generators. We were starting to get calls from both hospitals and some of the utilities wanting to know if we could help them find kerosene diesel, whatever they needed for their generators.

Mr. CAMP. Thank you for your testimony. I appreciate you coming out and helping the committee understand some of the concerns that went on during August. I appreciate that very much.

Colonel MCDANIEL. Thank you for the opportunity.

Mr. CAMP. Thank you.

Mr. SESSIONS. The gentlewoman from the Virgin Islands, Ms. Christensen, is now recognized.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman, and I want to thank the panelists. As we suspected, this would have been a really good test of our ability to deal with a terrorist attack, even though the at least to date it has not been shown to do that. Mr. McDaniel, a number of states like yours, as well as industries, have made significant progress in comprehensively assessing their own critical infrastructure vulnerabilities. What leadership role, if any, has the Department of Homeland provided in terms of guidance and assistance in those efforts? Or have you been doing it pretty much on your own without a framework and without the guidance?

Colonel MCDANIEL. No. Thank you for that question, because it is a good news-bad news sort of thing. We are still working towards that common goal. In some respects, it was last summer, July of 2002, that the Department of Homeland Security sponsored a critical infrastructure evaluation workshop put on by the Rand Corporation for all of the states which was very well received. They have given us technical support. They have given us coordination. So early on it was recognized that we needed a common framework in terms of how we would evaluate our critical infrastructure.

However, the bad news end of it is we are not there yet. The Assistant Secretary for the Department of Homeland Security pointed out that they recognized certain infrastructure that they believed were critical and needed protection during Iraqi Freedom–Liberty Shield. I would say only that those critical infrastructure that they identified and made known to the state may or may not have been the same ones that the states had identified. So this is still an on-

going process that needs to be worked through. As I said earlier, we are in the process of doing our strategic needs assessment sponsored by the Office of Domestic Preparedness. I think that is a vital first step towards coming up with a truly national plan for the protection of critical infrastructure.

Mrs. CHRISTENSEN. Thank you.

Mr. Dacey, I was interested in some of your comments and some of the parts of the report that talked about the private sector. Traditionally, that sector is resistant to increased governmental regulation, of course, and argues that market incentives will drive needed changes. Do you think that the market would, in the absence of another terrorist attack, increase security practices for the industry? And if not, what incentives do you think are needed to drive the industry to invest in increased security?

Mr. DACEY. What we have said at the General Accounting Office is essentially that when the CIP effort started in 1998, there was a call for an assessment by sector of what were the appropriate public policy tools, if any, that were necessary to get the cooperation and participation of the private sector. I think what we have said consistently is that needs to happen. In looking at several of the sectors earlier this year when we reported, there really had not been extensive efforts taking place to perform that assessment. That could range anywhere from providing research and development, from providing education and awareness grants, tax incentives, or regulation.

So we don't really say which of those should be done, but really that an analysis needs to be performed to consider what would be the appropriate incentives for those sectors to increase their participation in the program. I think also part of that is there is a need for the department to clearly state what their expectations are and the level of security, and send them to the private sector to determine whether or not they can meet those standards or expectations. I think that needs to happen as well to identify if there is any difference between the two.

Mrs. CHRISTENSEN. Thank you.

Thank you, Mr. Chairman.

Mr. SESSIONS. I thank the gentlewoman.

The gentleman from Pennsylvania is now recognized.

Mr. WELDON. Thank you, Mr. Chairman. Let me thank you both for coming in. I want to focus my comments and questions basically on one area of the GAO report, because GAO reports typically become very important tools for Members of Congress, especially in the context of going back and looking at how we deal with threats and the approaches that are used. I really have a problem with the section of the report starting on page 30, Analysis and Warning Capabilities Need to be Improved. I agree with that statement. But on page 33, Mr. Dacey, you allow the FBI and its Director to present the case that somehow technology was not available prior to 9–11 to do data-mining and data analysis.

Let me tell you something, I am not going to sit here and let that happen, because the facts just don't bear that out. In July when I chaired the House Defense R&D Subcommittee, on July 30, 1999, after looking at the Army's extensive LEWA you know what the LEWA is, their CERT down at Fort Belvoir. The Army developed

a capability that was cutting-edge, and that was to not just do information dominance on their systems, but to also use those systems, using tools like those developed by Battelle Labs, Starlight and Spires and others, to do data-mining and data analysis. They were on cutting-edge of that in the late 1990s, in 1997, 1998, and 1999. We put additional money in to allow them to accomplish that.

In July of 1999, I wrote to Deputy Secretary of Defense John Hamre. I said, "John, you have to look at this capability because it has tremendous implications for us to monitor external threats and to bring that together and assimilate it." He went down. He agreed with me. I had done some test work with him on an assessment of a person who was involved in the ending of the Yugoslavian war. From that, we put together a briefing in 1999 that I have a copy of, that basically outlined a national operations and analysis hub, a national data-mining center that would bring together all 33 classified systems of the federal government, all 33 classified systems. John Hamre said, "Congressman, I agree with you. I will pay for it. But you have to get the other agencies, the FBI, and the CIA, to agree, and that is a tremendous turf battle."

So John Hamre suggested to me that I convene a meeting in my office with his counterparts from the CIA and the FBI. In the fall of 2000, I did that. I had Deputy Secretary of Defense John Hamre, the deputy head of the FBI and the deputy director of the CIA in my office for an hour. We went over this initiative. We said we have to have better access to coordinate intelligence information so that we can see the bigger picture of what is occurring. And the CIA and the FBI, that are now trying to take credit for it in 2002 in saying there was no capability, in 2000 said, "We don't need it; we don't need that capability."

So it is important that GAO go back for the record, and I am going to ask unanimous consent to put this documentation in the record.

Mr. SESSIONS. Without objection, it will be accepted into the record.

Information is in the committee files.

Mr. WELDON. As well as news articles that ran in 1999 and 2000 that the GAO should have been aware of, that it was a major priority of this Congress that we establish an integration of data-mining and data analysis to avoid what happened on September 11, 2001. If we had done that back in 1999, if we had done that in 2000, we would have had a capability to pull the pieces together that in your report the FBI director in 2002 says, "Enhanced analytical data- mining capacity that was not then available." That is wrong. Raytheon had that capability. Busity Visioneering had it. The Army was using it down at the Fort Belvoir LEWA Center, and so was Special Forces, Special Operations Command down in Florida. They set up a mini-version of this analysis capability. In fact, before 9–11, they had a complete profile of al Qaeda, a complete profile by doing the data analysis that the FBI and the CIA say we don't need.

I think it is important because these agencies now want to rewrite history. They want to have us believe that they couldn't have done things before 9–11 because the technology wasn't there. That

is wrong. And in the record, I will put the facts to bear out before the comments of the head of the CIA or the FBI. The fact that you put that in the GAO report, this becomes like a Bible, like "oh, well, that is the case; there was no technology." I would ask you for the record to correct that, and I will give you all the documentation to back that up.

Mr. DACEY. I appreciate that. I will go back to check through our records as well, but I believe that references the fact not that it wasn't available, but that they did not have that capacity.

Mr. WELDON. No, what he said in the record, which was not refuted by the GAO, was it was not available. And I would also ask you to put in the record in two successive defense bills, language that we inserted that called for a national collaborative information analysis capability in 2 successive years. I mean, the GAO had to know that. It is a part of the record of defense authorization bills that we pass each year. I want to show the fact that the Congress as far back as 1999 and 2000 was clearly aware of what you are saying is a top priority now. We knew this was the case, not after 9–11, before 9–11.

Mr. DACEY. Right. And our work related to that was before 9–11 where we identified that these needs need to be filled and they didn't have them at the time.

Mr. WELDON. I just would ask you to correct for the record the fact that the Congress did not allow the FBI to try to rewrite history to make it appear as though there was no technology available. Those software systems by Battelle were done back in the mid-to late–1990s. They were clearly available to the FBI and the CIA before 2002. For the director to say that they weren't available is just technically inaccurate.

Thank you.

Mr. SESSIONS. I would like to inquire upon you, Colonel McDaniel, at the time you gave your original testimony you talked about at the border on the Canadian side, at what would be the equivalent of the United States Customs was not online and able to process, yet the United States Customs, at least that bridge there in Michigan was able to process those things. Was this off of generators? Was this off a well- executed plan? Was this off a backup? Or did they simply not go down?

Colonel MCDANIEL. They switched to generators, the U.S. Customs and the bridge itself. It is a privately owned bridge. Those two systems switched to generators themselves, and so there was a momentary blip. I just talked to them 2 days ago to confirm this. They held their breath to make sure the commuter systems didn't knock out. They didn't. Everything was ready to go and continued.

That bridge is obviously the auto industry's biggest in terms of free trade, and with the auto industry and the parts going back and forth, that is the most crucial crossing that we have. So it turned out, of course, the auto industry was down because of the loss of power as well. If not, though, again, it is the cascading effects that I tried to indicate in my written testimony that could have been worse there.

Mr. SESSIONS. The things which you have done within the State of Michigan to be in preparation for this event and many others, did it include this specific type of circumstance or was this some-

thing that was reasonably new and you treated as a real live exercise?

Colonel MCDANIEL. First of all, we absolutely did treat it as a real live exercise. Everybody in the state emergency operations center realized that it was a great opportunity to make sure that the plan worked. This was included in the plan. This was one of the potential events that might have occurred as a result of the millennium changeover that people were worried about, so that everybody was fairly ready. We could just pull the plan off the shelf and dust it off a little bit. So we were prepared for this potential event.

Mr. SESSIONS. At the time that you talked about the communications plans and the things that you felt that the communication was good back and forth, did within the State of Michigan, did you ever receive an indication before the blackouts occurred that there was a problem that you should be prepared or was that held within the power plants or did they communicate back and forth?

Colonel MCDANIEL. My understanding, and of course you are getting outside my area of expertise, but my understanding is that there were events that afternoon prior to the outage. We were not aware of those low-voltage type events at the state EOC, at the emergency management division of the state police or at the National Guard or at the governor's office. We were not aware of those events, and I do not believe the Public Service Commission, our regulatory agency for utilities was either. If we had been, it may have made a difference. I would be speculating to say that, but we could at least use some form of communication to the general public if we knew that was happening, rather than try and jerry-rig a system for getting the message out to the public after the fact. What we do is, Michigan State University is right there. It is large enough that it has its own power plant, not just generators, so that they can generate. They have a turbine hooked up to the boiler, in essence, so they generate enough power that we can send out a TV signal to the other TV signal receivers outside of the affected area and get the message out from the governor that way. But for having that system in place and having it almost immediately available, we may not have been able to get the message out to the general public as easily as we did. Certainly, I think that there should be some sort of emergency alert system that is in place, that is working from DHS down to the public, as well as to the state agencies themselves. Within the last week or so, I received a letter from the director of NOAA that went out to all the state homeland security advisers indicating that NOAA was going to be the primary agency to get the message out to the general public. I have not seen any acknowledgement of this as of yet from the Department of Homeland Security.

Mr. SESSIONS. Can you give me a sense of what happened on the ground in Michigan in terms of people's TVs going out, TV stations going out, radios going out, telephones going out? Was there a time frame or a timing delay that could have caused a lot of panic and chaos between the time that the TV station came on from the university?

Colonel MCDANIEL. This was early enough in the afternoon that it was still certainly daylight out, so the people had plenty of time to respond and prepare for the evening hours and try to stock up

at the stores, if they had not done that already. However, there was an immediate loss of electricity. For the radio and TV stations, there was a loss momentarily until the ones that had backup generators worked. Obviously, a lot of people did not have old-fashioned phones. Everybody's phone is portable, a hand-held device which requires electricity these days, or a cell device, and not all of those towers worked. So there were a number of instances where the communication systems were more reliant on electricity than we believed that they would be. Again, even those radio and TV stations that had generators, the generators didn't work because they had never been tested. So they weren't ready to work under load. They weren't the right capacity generator. And then the other problem, as I said, was 24 hours later they were staring to run out of power. Both TV and radio, as well as the telephone companies, were calling as well.

Mr. SESSIONS. It seems, at least to this member that perhaps part of our emergency preparedness plan should be, please, if you are a consumer, turn off anything that you don't reasonably need except a TV or a radio or something else. Did that becomes a glaring point to you and the people in Michigan at the time that this occurred because of the load factor?

Colonel MCDANIEL. Absolutely. I apologize. I meant to mention that before, both in terms of the use of electricity and the use of water. This was a very hot day in the summer where the usage on the Detroit water system was almost a billion gallons a day. The system, even after it came back up on generators, could only handle about 400 million gallons per day. If we had had a method, if we had some sort of warning that this was going to happen, and could have gotten out to decrease your electricity, decrease your water use ahead of time, it probably would have made it easier for the system to come back on.

Mr. SESSIONS. Had you seen brown-outs that had been occurring? I think we have gotten used to hearing the term "brown-outs" or rolling brown periods that have occurred. Was that seen at all a day or two or hours before?

Colonel MCDANIEL. No, there was no indication like that.

Mr. SESSIONS. No indication at all?

Thank you.

Mr. Dacey, you have heard a great deal of testimony today from any number of witnesses and I believe that probably you have a bird's eye view of a lot of the things that we have talked about that you have studied before today. Could you have seen this coming? Could you have seen the response? Was this predictable with how these things happen, not that the event happened, but the response? And what would be your analysis of that, because from this member's perspective, I was generally pleased with the lack of chaos that was exhibited all across the power grid, where it went down, by people. I felt like that elected officials and others were prepared and that they really did a good job.

What would be your evaluation from looking at it now if you had gone back and were offering as just a prediction?

Mr. DACEY. In terms of whether the whole process could have been foreseen, I guess that gets back to some of the earlier discussion. I think we are making progress based upon Mr. Liscouski's

testimony in really identifying some of the vulnerabilities in these infrastructures. We heard other testimony about the states doing efforts as well. I think that is critical, as well as the interdependencies, which we talked about earlier today. Because until we fully understand those, it is going to be very difficult to understand what are the implications, what happens next. I think just based upon a personal perspective, not based upon our security work, I was very pleased that nothing more serious happened than did. But in terms of again, projecting that, I don't know if that would have been possible. We are now discussing some of the kind of things though that may have contributed in terms of the capacity of our transmission lines. Those are all really a part of a vulnerability analysis and assessment that needs to be done across all of the infrastructures to decide what are critical points in those infrastructures. Do we have weaknesses or vulnerabilities? What is the cost to fix those, and how are you going to pay for those? I think that is the critical lesson to learn here in the process and that needs to be done. Again, there are efforts in that direction, but there is ways to go.

Mr. SESSIONS. I thank the gentleman.

At this time, the Chairman would like to not only thank both of you for being here today, but in particular Colonel McDaniel, I note from your resume that you have spent 18 years with the Michigan National Guard. This member is not only proud of your service, but also the other men and women who serve in the Guard, all across this great nation. You are a shining example of the type of people who serve this great nation. I want to thank you for your service, not only today and to the State of Michigan, but also to this nation for that which you do.

So I would like to thank both panels at this time for their participation.

The chair notes that some members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 10 days for members to submit written questions to these witnesses and to place their responses in the record.

There being no further business, I again thank the members of both the Cyber Security, Science Research and Development Subcommittee and the Infrastructure and Border Security Subcommittee and to our witnesses today.

The hearing is now adjourned.

[Whereupon, at 5:29 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE RECORD

QUESTIONS AND RESPONSES SUBMITTED FOR THE RECORD BY JAMES R. LANGEVIN

SEPTEMBER 4, 2003

There has been widespread concern in the industry and on the local level that DHS is not putting nearly enough effort into sharing information outside the Department. The Undersecretary for Information Analysis and Infrastructure Protection has not made any indication as to what priority DHS places on infrastructure protection. California and New York were the first states to identify their critical infrastructure, and several smaller states are following suit. Critical infrastructure typically includes the electrical grid, water supply, communications/telephone lines and bridges or tunnels. Unfortunately, once states have accomplished this, there has not been much support from DHS on what the next step is.

Question: **a. What role has the Department of Homeland Security played in providing information, promoting information exchange across sectors, or assisting with solutions for problems common to critical infrastructure industry? Has this role been sufficient? Could it be improved? If so, how? In particular, do you believe that those who need to know have the proper information regarding potential threats, so that they can allocate resources and improve protection in the right places?**

McCarthy Response:

The Department is addressing the issue of information sharing through two mechanisms: the Information Analysis & Infrastructure Protection Directorate, and the Department's Office of the Private Sector Liaison.

The Information Analysis & Infrastructure Protection Directorate (IAIP) has taken the lead on promoting information sharing across sectors. Its overall goal is to provide the private sector with "actionable intelligence"—timely, accurate information that can help apprehend terrorists and prevent their attacks. To that end, the IAIP recently established the National Cyber Security Division (NCSD), a 24 x 7 cyber "watchdog" that will provide analysis, alerts, and warnings, as well as improving information sharing. In the life span of the Department, the NCSD is relatively young, but we look forward to its continued growth and progress in the days and months to come.

The Office of the Private Sector Liaison is another key component to strengthening the public-private partnerships. Through Albert Martinez-Fonts, the Liaison's office provides businesses with a direct line into the Department. It acts both as an advocate for the private sector, by informing the Secretary of its concerns, and as a clearinghouse, by directing businesses to the appropriate agency or directorate. With so many of our critical infrastructures owned and operated by private entities, this office will play a pivotal role in ensuring that both sides know exactly what is at stake.

One of the Liaison's main services is coordinating with ISACs, trade associations, and businesses whenever there is a change in the threat level. The Liaison provides guidelines and suggestions to private sector entities, so they may properly respond to the changes. Additionally, the Liaison clarifies liability and compliance issues to those businesses affected by new homeland security laws or regulations. Over time, it is expected that both the IAIP and the Office of the Private Sector Liaison will experience increased efficiency.

Orszag Response:

Private-sector representatives regularly tell me that they do not receive useful guidance or information from the Department of Homeland Security. That is part of a broader problem: The Department has been moving much too slowly to spur homeland security activity in the private sector. As my co-authors and I discuss in *Protecting the American Homeland,* designing appropriate incentives for private firms to undertake homeland security investments is among the most difficult challenges in the homeland security area. In the two years since September 11th, we have failed to move aggressively enough in tackling this challenge.

Watson Response:

To date, DHS has not established an efficient, comprehensive mechanism to communicate changes in homeland security alert warning levels. However, by absorbing the National Communications System (NCS) and continuing to support its associated Telecom ISAC work, DHS has provided daily updates and periodic summaries of relevant information affecting most critical infrastructure sectors. These reports

are informative and include links or contact information so that recipients can follow up to learn more details as required. In addition, DHS forwards information from Telecom ISAC members, government agencies, and other ISACs regarding new threats, anomalous activity, or advisories of immediate concern to critical infrastructure owners and operators. The cooperation across the leading ISACs has improved steadily over the last year, and the DHS/NCS effort has been a major part of that cooperation. Until DHS puts together a comprehensive information sharing strategy and architecture in collaboration with the private sector, the existing solution will continue to be inadequate, serving neither the private nor public sector well.

Even though DHS has promoted information exchange across sectors by hosting meetings of the ISAC Council (ad hoc council of the leadership of the 10 largest industry ISACs), and meets regularly with the critical infrastructure Sector Coordinators to learn of sector and cross-sector requirements that require DHS assistance, it has not developed a comprehensive architecture describing the functions, relationships, and mechanisms for information sharing in coordination with the critical sectors. I would encourage a much more robust effort by DHS with Sector Coordinators, ISAC entities, and those representing critical infrastructure operations to develop and implement a full-function architecture. An attempt by DHS to independently craft a comprehensive approach without the commitment of the private sector that manages most of the critical infrastructures is doomed to failure.

Has DHS assisted with solutions? It is probably too early to answer this completely. DHS has established a dialog with Sector Coordinators and the ISACs, hosted the Homeland Security Standards Panel of the American National Standards Institute (ANSI HSSP), and is beginning to help in the development of sophisticated modeling and public-private exercises to determine requirements and then develop solutions.

Has this role been sufficient? By what measure? If the question is whether DHS efforts have been sufficient to solve critical infrastructure problems, the answer is no. If the question is whether DHS has met expectations given the short life of the department, its learning curve, and the as-yet undefined set of requirements from industry, the answer is a qualified yes.

Even though the Marsh Commission (President's Commission on Critical Infrastructure Protection) clearly identified the problem five years ago, and Federal government and industry stakeholders had accomplished a great deal since, the very act of reorganizing all the Federal agencies involved in critical infrastructure protection, installing an entirely new set of leaders, and refining requirements through three new national strategy documents has brought early progress nearly to a halt. DHS has done very well to work through this turmoil to get things moving again.

Could DHS's role in information sharing be improved? Absolutely.

Industry Sector Coordinators must be expeditiously identified for those new sectors added in the National Strategy for Homeland Security. The role of Sector Coordinator must be defined, promoted, and socialized at all levels of government and the critical infrastructure industries. The Sector Coordinators should be a first point of contact for information. An effort should be made to tailor homeland security alert levels to sectors or regions, rather than confuse everyone by publishing a one size fits all color code that few can use practically. Before being absorbed by DHS, the Critical Infrastructure Assurance Office (CIAO) developed and conducted Project Matrix, which methodically identified critical assets and dependencies within and across all Federal departments and agencies. What has become of Project Matrix? If its methodology was sound, could it be used by critical infrastructure sectors in a similar way?

Sectors generally have extensive knowledge of their critical assets, but not of their critical dependencies on other sectors, or detailed knowledge of others' dependencies on them. This knowledge deficit could be partially remediated by modeling interdependencies and conducting exercises designed to highlight interdependencies, identify regional stakeholders, resulting in comprehensive cross-sector contingency plans. Sector Coordinators and their representatives should be involved in the creation, design, development, and leadership of these exercises and models, rather than simply be invited as observers or last-minute add-on participants.

Do the right people have enough information regarding potential threats to properly allocate resources? Resource allocation is part of risk management decisions. I think DHS has the correct strategy here. Specifically, stakeholders need to understand the nature of critical vulnerabilities in sectors and the scope of potential impacts if exploited; consider these vulnerabilities in the context of intelligence, understanding threat and adversary capabilities; then make judgments on what protective actions should be prioritized. More structured engagement with the private sector on identification of critical vulnerabilities needs to be developed. This is more about

getting the right people together from each sector in organized effort than about a simulation task.

Except for a few specific instances, when industry stakeholders are given access to government classified information on threats, the information is insufficient to be actionable. In those instances when DHS learns of specific information that could help a single sector or company defend itself, it has been very proactive in getting that information to the right people as soon as possible. Rather than attempt to learn more about who or why someone or some group might target American critical infrastructures, I recommend greater efforts in vulnerability and interdependency analysis in order to get at the how and what could be done. Industry should lead in development of defense-in-depth technologies and procedures, with support and coordination provided by the government. The greatest progress toward a secure critical infrastructure can be made by hardening infrastructure protocols and implementing industry best practices. This is why I repeatedly stress the importance of research, modeling, and exercises.

Question: **b. One issue that has been raised is the private sector not sharing information on vulnerabilities with each other or government due to FOIA concerns. How do you think we can work around this stumbling block? One suggestion is to set up a national center to monitor critical infrastructure where information could be sent confidentially (would classification help); another is to strengthen the information sharing and analysis centers' and their relationship to DHS. What do you see as the advantages and disadvantages to either of these approaches? Is there a better way to spur sharing relationships so that the right people can be talking about these problems before they happen rather than after?**

McCarthy Response:

The GMU CIP Project held an ISAC Conference on August 11, 2003. The overall topic was "Information Sharing and Analysis Centers: Defining the Business Case." Participants included representatives from almost every critical sector, the ISACs, and members of federal and state governments. The result of this conference is a White Paper, including findings and recommendations, which is attached to this document.

One of the questions the Conference strove to answer was "What is government's role and responsibility to promote ISAC functionality and growth?" Overall, industry looks to government for cooperation in information sharing. The relationship should be embodied by a dynamic, two-way process: ISACs can share operational information, while the government provides timely intelligence and data analysis. This collaborative process would strengthen the ISAC relationship with government, and perhaps encourage more meaningful sharing on both sides.

Orszag Response:

I share the concern that extant rules on disclosure, including FOIA and FACA, may limit the degree of useful information sharing that occurs between the private sector and the government. However, I lack sufficient expertise in the area to provide specific recommendations to you.

Watson Response:

Industry is encouraged by the inclusion in the Homeland Security Act of a specific exemption to FOIA for critical infrastructure information (CII) voluntarily shared with DHS. With that provision, one obstacle to sharing vulnerability information with the Federal government has been removed. Additional barriers such as antitrust, liability, relevance, applicability, fairness, and competitive issues need to be addressed as well.

Follow-on efforts must be made with the 50 states and foreign governments to ensure that non-Federal jurisdictions can protect information from American companies as well, or they should only obtain CII information from DHS where it is protected as CII..

The idea of a national critical infrastructure information center, as opposed to strengthening and coordinating with the various ISACs, has both advantages and disadvantages. On the positive side, it would provide a single clearinghouse for all critical infrastructure information, simplifying the job of government in knowing whom to contact or where to go. On the negative side, it would add a bureaucratic layer, potentially dramatically slowing the flow information into and from the Federal government. Such a center would require special expertise from each of the critical sectors, access to industry ISACs, robust, secure communications capabilities with DHS and other relevant Federal departments and agencies, and equally robust, secure, and rapid communications capabilities with state and local governments and first responders. It could also create a target and a vulnerability due to the cen-

tralization of its information. Sensitive information is often compartmentalized and not centralized.

There is no one size fits all solution. Sector Coordinators, in collaboration with DHS, should establish the information sharing mechanisms preferred by each sector. Industry is deriving value from the existing ISACs, and I believe they will continue to evolve, maturing into reliable, timely clearinghouses of great benefit to their sectors. Because of the heterogeneous nature of the sectors, any universal approach will not achieve the full goals intended by the original recommendations of the original President's Commission. As such, I do not support the idea of a Super ISAC beyond the current cooperative model developed through collaboration by the sectors and DHS. DHS has a legitimate need for certain information. The more specifically DHS can state information requirements, the more likely the department would receive it. DHS should be identifying the categories of information they would like to see for specific critical DHS functions from the private sector and then let the private sector determine if and what information can be provided. Again, a more structured approach communicated to the private sector would go a long way.

The National Infrastructure Advisory Council (NIAC) will be submitting recommendations to the President soon on Vulnerability Disclosure Guidance and Enhancing Information Sharing. The NIAC includes key critical infrastructure corporate, state and local leaders, and has been very inclusive of Sector Coordinators and the ISACs as it has developed its guidance. The National Security Telecommunications Advisory Committee (NST AC) will also be submitting recommendations to the President on Barriers to Information Sharing. I respectfully advise the Committee to review these recommendations to develop appropriate public policy.

c. Mr. McCarthy, one of your graduate students recently received a fair amount of national notoriety for mapping the fiber-optic network that connects every business and industrial sector in the American economy.

Question: **i) Could you discuss that project and it's potential impact in further detail? "What was the response it received from national security officials and owners of critical infrastructure? Did the DHS comment on it?**

Question: **ii) In light of this achievement, has DHS been able to produce a comprehensive national critical infrastructure and key asset list, database, or map? If so, can you describe its progress? In your estimation, how long would it take for DHS to perform a comprehensive national assessment of critical infrastructure and compile a comprehensive national list ? What impediments exist to getting this done? What would it take for the DHS to produce an ″integrated critical infrastructure and key asset geospatial database″ as envisioned in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets? Once it was completed, what would be the best use of such a database?**

McCarthy Response:

i) Sean Gorman, a graduate student in George Mason University's School of Public Policy has spent the past four years mapping the nation's fiber-optic network and the industrial sectors that are linked to it. The map was created by mining publicly available information and combining it with mathematics to create a geospatial representation of our nation's communications infrastructure. This project is the basis for Mr. Gorman's PhD thesis.

This experience has taught us how to do this kind of research and how to reach out to various government agencies, make it available to them, and also expand our understanding and the body of knowledge. Meetings with appropriate stakeholders allowed the research project to set up some guidelines of what would be a good idea to publish and what wouldn't, and to set up a structure to look at what was and wasn't sensitive.

The research itself is focused on methods used to further the research community's understanding in the areas of Spatial Small Worlds and Network Theory. A by-product of this research is information that may be useful to government agencies in protecting our homeland; this portion of the research has been shared with the appropriate agencies. As soon as the project was proposed, the need to study these systems in terms of their impact to our National Security, National Economic Security, Public Health and Safety, and Public Confidence was apparent. This research has as an objective to evaluate these systems to understand their:

Reliability—stability of existing systems and parts of systems

Redundancy—alternatives identified in advance of disruption

Resiliency—how fast can it systems can be restored after disruption

Vulnerability—economic, social, and societal impact of system disruptions

All of these questions need to be answered in order to manage priorities in directing safety activities in any diverse and spatial distributed system. Sources of potential disruption are natural disaster (floods, hurricanes, tornadoes, earthquakes, etc.), technological problems including (fires, short circuits, etc.) or terrorist attack. While each of these types of potential disruptions are important, the need to better understand the probability and implications of deliberate attacks has only recently become an area of serious academic research. This kind of work is vital to managing the Nation's critical information infrastructure assets.

ii) Mr. Gorman's work, although comprehensive, deals with only one small piece of the nation's key assets and critical infrastructures. Robert Liscouski, DHS Assistant Secretary for Infrastructure Protection, has pointed out that it could take years to create a comprehensive risk assessment database.. There are thirteen defined critical infrastructures, plus five key asset categories. The issue is not one of specific impediments or delays, but rather that the process is necessarily complex if it is to be comprehensive. Such a project will require intense, prolonged focus to be complete and accurate.

RESPONSES TO QUESTIONS FOR THE RECORD SUBMITTED BY THE HONORABLE JIM TURNER

SEPTEMBER 4, 2003

For all witnesses:

Question: **1. In your opinion, which of our critical infrastructure sectors pose the greatest national security concern, in terms of risk of attack, vulnerability to attack, and potential consequences? Please rank—in relative order starting with the highest concern—the top five critical infrastructure sectors that you believe pose the greatest risk. Briefly discuss the reasons for your selections and rankings.**

McCarthy Response:

It is impracticable to quantify which critical infrastructure is most important, or "of greatest national security concern." One key aspect of the criticality of a particular infrastructure, or set of infrastructures, may arise from physical aspects of siting, collocation, uniqueness and shortages of equipments, volatility of infrastructure components or materials, or the logistical or supply chain impact of loss of a critical path process. These aspects of criticality are loosely identifiable from geographic or spatial economic analyses in conjunction with interruption of service actions. Other key aspects of criticality of particular infrastructures, or sets of infrastructures, may result from interdependency between systems, cascading effects due to disruptions moving through interdependent infrastructure configurations, or system conditions reaching states of threshold failure. This would be the case where one infrastructure system fails because another infrastructure did not deliver its anticipated inputs, due to a lack of capacity or unfulfilled demand. With so many variables to consider, and so much data to weigh and process, I cannot say with any confidence that any infrastructure is any more critical or vulnerable than any other. The focus should be on maintaining robust systems for all critical infrastructures.

Orszag Response:

Although I am hesitant to select five sectors and then rank them, one sector clearly warrants immediate attention: the chemical industry. It is now more than two years after September 11th and more than a full year after Secretary Ridge wrote in the Washington Post that voluntary efforts were not sufficient to provide the proper level of security in the chemical industry. Yet nothing has happened to force chemical facilities to move beyond voluntary efforts. The continue lack of adequate security measures at the nation's chemical facilities, as vividly demonstrated in a recent 60 Minutes expose, is astonishing.

Watson Response:

I do not believe there is a single sector that is most critical. The PCCIP (Marsh Commission) got it right when it identified eight sectors as critical to the operation of government and the well-being of our citizens, their dependence on computer networks, and their interdependence. Successfully attacking any of the critical infrastructures would have cascading effects on multiple others. The problem, and the risk, is that these dependencies are still poorly understood. I do believe that the sector definitions need to be refined the original eight may accurately identify the most critical industry areas, but the sector definitions do not necessarily agree with how industry understands and organizes itself. For example, telecommunications (or communications) and IT are very different industries, but were grouped as a single

sector by the PCCIP. Also, electric power and oil and gas were identified as two sectors by the PCCIP, but most energy companies produce and provide both forms of energy.

Criticality must also be defined. Is it important to know what the immediate effects of a sector specific outage are on other sectors, or the long-term impact, if sustained? Does criticality include financial impact, cost of recovery, and effect on consumer confidence, or is it simply limited to the ability to conduct business in the affected sector?

A strong argument can be made that telecommunications is the most critical infrastructure, since it typically is the one other critical infrastructure sectors cannot work around. For electric power, backup generators can be employed for a time; water tanks can be provisioned; but no viable alternative to telecom is typically available. However, in terms of attack, many focus on transportation and IT because they are the infrastructures that can most easily be converted into offensive weapons.

All that said, the NIAC Interdependency and Risk Assessment Working Group submitted its final report to NIAC members October 14, 2003. That report included results of a survey of Sector Coordinators and key infrastructure owners and operators regarding their top dependencies. Respondents were asked to list the top three sectors on which they depend, and the top three sectors that depend on them. In terms of short-term dependencies, the overall top three were 1) telecommunications and IT, 2) electricity, and 3) transportation. However, adding long-term impacts broadens the list of critical dependencies. Without financial services, business comes to a grinding halt in a matter of days. Without safe food, clean drinking water, and available health care, public health also reaches a crisis in days. Without emergency police, fire, and medical services, the ability to respond and contain emergencies is severely impacted. Long-term impacts of transportation failures are far more severe than the short term.

Rauscher Response:

With brief reflection on which of the nation's critical infrastructure sectors poses the greatest national security concern, one could identify the financial sector—because it has been the target of past attacks, or the communications sector—because of it's vital role in the operations of all sectors, or the energy sector—because of its foundational role as enabler for all other sectors. However, with the stakes being what they are, considerably more discussion is needed. My most useful guidance to the Committee is a review of the underlying method of identifying where the real greatest concern is.

Ranking infrastructure sectors is difficult, and can be misleading without specifying prioritizing parameters. By definition, each critical infrastructure sector is inherently critical. Also, each sector has direct and indirect dependencies on the other sectors. In fact, there are intricate webs of dependencies threaded throughout these sectors. In addition to this complexity, some dependencies are new or are otherwise not well understood.

The question of which infrastructure sectors are at most risk of attack is deferred to those responsible to gather and process the information that can support such insights. Vulnerabilities and consequences are addressed below.

Which critical infrastructure sector poses the greatest national security concern, in terms of vulnerability to attack? The sector that poses the greatest national security concern is the one that does not have a comprehensive list of its vulnerabilities based on the intrinsic attributes of its basic building blocks, and does not have a systematic framework for effectively covering these vulnerabilities. An impact on anyone sector can have a domino effect on all of the other sectors

All of our critical national infrastructure sectors have vulnerabilities. Furthermore, there are vulnerabilities that cannot be removed—they will exist and we must learn how to address them while they remain in our midst. With the current, extensive discussion on "vulnerabilities", clarification is helpful regarding the use of this term. A "vulnerability" is an opening, or a soft area, or susceptibility. Vulnerabilities are intrinsic attributes of the building blocks that make up our infrastructure. For example, the Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) Physical Security Focus Group identified eight building blocks, or ingredients, that make up the communications infrastructure: Power (internal systems), Environment, Hardware, Software, Network, Payload, Policy, and Human.

Each of these ingredients has intrinsic vulnerabilities. For example, Environments can be accessed or destroyed, People can be deceived or fatigued, Policies have unintended side effects, and Hardware semiconductor materials can be overstressed by electromagnetic energy or fail in extreme temperatures.

As Superman had a vulnerability to kryptonite, so the building blocks of our infrastructure have attributes that we must first identify, and then learn to protect appropriately. For example, the NRIC effort previously mentioned required an unprecedented level of industry engagement and collective expertise to systematically identify the vulnerabilities in each ingredient. This process then produced world class, voluntary, Best Practices guidance for preventing the future exercise of such vulnerabilities, or for mitigating the impact of a future attack. Furthermore, because the intrinsic attributes of these ingredients are commonly known, this vulnerability framework is effective in avoiding disclosure of sensitive information.

The crucial concept is not so much to identify which sector has the greatest vulnerability, but to identify which sector has the greatest vulnerability that is remaining unaddressed. There are surface vulnerabilities that exist in a configuration or combination of ingredients. These can sometimes be removed by a reconfiguration or replacement of one ingredient with another. However, it is a misperception to think that all vulnerabilities can be removed. They must be identified, their nature understood, and then addressed through protective or other appropriate means to prevent their exercise by threats, or ameliorate their impact, if successfully reached with a threat.

Which critical infrastructure sector poses the greatest national security concern, in terms of potential consequences and far-reaching impact on other sectors? The nature and target of any future attack will determine which critical infrastructure sector, once disrupted, would have the greatest potential consequences. Obviously, the sector targeted could have some direct consequences from a successful attack. However, the nature of the attack would determine the extent. For example, the detonation of a primitive explosive device near a communications network node could temporarily cripple communications support for other sectors' critical facilities in that immediate area, but broader regional traffic could be rerouted. A different attack on the same sector could attempt to spread a virus throughout an entire national network. Another scenario is one in which a compromised sector is deliberately unharmed while it is being used to unleash havoc on another.

Without consideration for what vulnerability analysis is underway and what protective measures are in place, the following sectors present the highest potential risk to national security:

Energy
Information and Communications
Banking and Finance
Transportation
Postal and Shipping

This priority scheme is based on (a) the ease at which problems propagate within the sector, (b) the extent of other sectors' dependencies on it, and (c) the potential impact of a sector's loss of crucial functionality.

Question: **2. Do current efforts by the Administration and the Department of Homeland Security match the gravity and seriousness of the threats we face in the critical infrastructure sectors you identify? What more should be done to address the risks in the sectors you identify?**

McCarthy Response:

Although the Department is still in its formative stages, it is doing a remarkable job of ramping up projects and setting its agenda in order to face the critical infrastructure threat. For example, the DHS recently tapped the CIP Project to do a Mitigation Priority Analysis in the wake of Hurricane Isabel. We have been asked to evaluate the telecommunications, transportation, water, and energy sectors in the National Capital Region. Specifically, we will study how the four critical sectors prepared, reacted to, and recovered from the hurricane. This project will help identify the kinds of risks and vulnerabilities faced by these sectors, and provide guidance on how to address them.

Another example of the Department's evolving schema is the recent development of the USCERT (Computer Emergency Response Team). It is a partnership between the NCSD and Carnegie Mellon's CERT/Coordination Center (CERT/CC), which will work with the private sector to improve warning and response mechanisms to cyber incidents. In addition, the USCERT will collaborate with the private sector to develop and implement new detection and response tools.

These projects are excellent examples of the intelligence and initiative at work in the Department, even in this early stage of development. Of course there is more to do, but the Department is dealing with an enormous learning curve—bringing together old agencies with new ones, balancing security needs with efficiency, and anticipating the unanticipated are not easy tasks. But as the groundwork is laid for

further growth, I am confident that the Department will rise to the challenge that Congress and the nation have put in front of it.

Orszag Response:

As I stated in testimony before the 9—11 Commission on November 19, 2003, the general lack of action in strengthening market incentives to undertake homeland security investments more than two years after the September 11th attacks is simply unacceptable. In my opinion, the Department of Homeland Security bears primary responsibility for this lack of action.

Watson Response:

The Administration agreed with the Marsh Commission regarding the most critical infrastructure sectors, and studied the issue further, identifying additional critical sectors in the National Strategy for Homeland Security. That strategy is supported by national physical and cyber security strategies, which articulate the gravity and seriousness of the threats to critical infrastructures. I believe DHS understands the seriousness of this issue, but has been hampered by internal churn caused by simultaneously merging 22 Federal agencies, identifying and training new leaders and employees at all levels, sorting out real stakeholders from pretenders, and having to conduct day-to-day operations while reorganizing and hiring. Rather than try to determine which sector is most important, it would be far more effective to address cross-sector dependencies, considering all the identified critical infrastructure sectors. This is why I stressed the importance of computer modeling and tabletop exercises in my testimony.

Rauscher Response:

My observations of the efforts of the Administration and the Department of Homeland Security, related to the protection of our critical national infrastructure sectors, is that:

1. Critical infrastructure protection has been identified as a vital component of the Homeland Security strategy
2. There is a concerted effort to advance the National Strategy for Homeland Security
3. The Department of Homeland Security has begun to provide national coordination for infrastructure protection
4. The Department of Homeland Security has also begun to implement creative, new technologies and capabilities in their approach

A brief discussion of each of these areas, as related to the communications sector, follows.

1. Critical infrastructure protection has been identified as a vital component of the Homeland Security strategy

The President's National Strategy for Homeland Security underscores that critical infrastructure protection is vital to protecting the nation. For the communications infrastructure sector, this stated policy is and continues to be addressed in several notable ways.

First, the government-industry partnership-based National Communications System (NCS) National Coordinating Center for Telecommunications (NCC) and Telecom-ISAC (Information Sharing and Analysis Center) trusted environment and functions have been integrated into the Directorate of Information Analysis and Infrastructure Protection (IAIP).

Second, the President's National Security Telecommunications Advisory Committee (NSTAC) has been repositioned to within DHS and continues to advance policy guidance on several critical subject areas regarding critical infrastructure protection, including, for example, matters of concern with the banking and finance sector.

Third, the joint government-industry Network Security Information Exchange (NSIE) continues to maintain dialogue on classified subject matter, other sensitive information, and on special subjects of concern. In addition, there are various other activities in which DHS exhibits its commitment of critical infrastructure protection.

In summary, protection of the communications sector is the stated policy of the Administration and DHS and this policy has been acted upon with the necessary private industry cooperation. To ensure a continued strong protection program for the communications sector, the Administration and DHS should continue to work closely with private industry, and specifically, support the trusted environment of the NCC and Telecom-ISAC.

2. Advancing the National Strategy for Homeland Security

A basic learning from the September 11, 2001 Al Qaeda Attack was that the then existing methods of defending against terrorism were inadequate. This is a primary motivation behind the restructuring that has taken place under the new department.

If a defensive strategy is based primarily on threat knowledge, then those vulnerabilities targeted by the known threats will likely be protected well. Speed and focus are the hallmarks of this approach, enabling efficient deployment of resources. However, this approach may leave some "cockpit doors" unaddressed. On the other hand, the systematic vulnerability approach covers all vulnerabilities—independent of whether historic or fresh threat information is available. While this approach takes longer, it yields a substantially higher degree of confidence because it protects all vulnerabilities, and thus is prepared for any permutation of attack method. It is the only approach that can help us be as prepared and as secure as possible. It is the only approach that can let us sleep well at night.

Given the complexity of many of our sectors, it is vital that such a very disciplined approach be followed. One further motivation for a systematic vulnerability approach is articulated in the President's National Strategy for Homeland Security: "Terrorism depends on surprise." The sophisticated terrorists of the twenty-first century conduct surveillance and patiently plan. We cannot afford to take shortcuts that would leave our coverage of the unexpected wanting. This contrasting discussion of the two approaches does not suggest the selection of one over the other, but rather the deployment of both. It is best to see these two approaches as complimentary, where the vulnerability identification and protection functions are guided primarily on a vulnerability approach, and the threat intelligence and risk dissemination functions are guided primarily by the traditional means.

The progress of the DHS IAIP Protective Security Division has mostly been along the lines of applying threat-based approaches. Although there have been numerous enhancements in this area, it is not enough. It is however, the best first step, in that it allows for a speedy, effective focus, and immediate efficient use of limited resources. The Protective Security Division plans to supplement its enhanced threat-based strategy with one of systematic vulnerability assessment, and to partner closely with private industry as it advances this strategy. It is vital that this course be maintained.

From my unique position of having led the communications industry's top experts in the development of over two hundred and fifty Homeland Security Best Practices during the past two years, I have made a straightforward—yet strikingly critical—observation: Formal training directly enables or limits abilities to solve particular problems. Careful consideration should be given to the various disciplines available and the nature of the challenges being faced. Specifically, law enforcement professionals are often highly trained in methods of processing threat and risk information. Computer "science" training offers proficiency in translating logic ad other functionality into automated processes, but is actually based very little on fundamental scientific approaches to problem solving. However, it is the classical training of the engineer and scientist to do thorough, systematic, "cover-all-bases" procedures. In critical infrastructure protection, it is essential that DHS fully utilize the appropriate compliment of disciplines, paying particular attention to include industry-experienced engineers and scientists when comprehensive and systematic approaches are required. While the careful, systematic, thorough work of the engineer and scientist is often slower, it is absolutely essential.

In summary, one of the critical roles for DHS is to draw the distinction between the protection methods of the past and the new methods needed for the future challenges of terrorism. It is vital that DHS implement its plans to augment the traditional threat-based approach with a systematic vulnerability-based approach.

3. Provide national coordination for infrastructure protection.

With the NCS integrated into the 1A1P, and as such the NCC and Telecom-ISAC also, DHS is providing important coordination within the communications sector and increasingly important coordination among other sectors. In preparation for an emergency, and during an emergency response, cross-industry and government-industry coordination is essential.

The Department of Homeland Security also disseminates threat information through its trusted stakeholder channels. In addition to Daily Reports, DHS provides special notices and alerts. The communications sector also benefits from periodic DHS briefings to the Telecom-ISAC and its coordination between infrastructure sectors. During the August 2003 Power Blackout, the Telecom-ISAC received updates on anticipated regional power recovery timeframes from the Electricity Sector ISAC that enabled the communications network operators to more effectively manage logistics for, and deploy, limited resources.

DHS also recognizes its need to receive counsel and advice from private industry. The communications sector is very complex, as there is a host of technological, competitive, regulatory, legal, and other issues in play. DHS appropriately relies on experts from service provider, network operator and equipment supplier perspectives.

The NCS has been an active participant in the NRIC Homeland Security Best Practices work.

4. Implement creative, new technologies and capabilities in their approach

In order to meet the riveting challenges of our post-September 11 world, capabilities need to be augmented to embrace new technologies and capabilities. It is essential that DHS be open to new approaches, and to be capable of effectively screening through options to find those that should be implemented. One example is DHS' continued engagement of the Wireless Emergency Response Team (WERT), which was formed on September 11, 2001, to use advanced wireless technology to support traditional Search and Rescue efforts. Another example is Wireless Priority Service (WPS), which provides priority access for the wireless air interface for first responders and others with national security and emergency preparedness responsibilities. However, while the capabilities of WPS are currently available for one wireless technology platform, half of the potential capacity for providing this essential service remains undeveloped. In the absence of additional funding and/or direction by Congress, this capacity will remain untapped until the end of FY05.

In addition to including new capabilities, it is encouraging to see expanded outreach raising the awareness of existing NCS programs, such as the Government Emergency Telecommunications System (GETS), Telecommunications Service Priority (TSP), and SHAred RESources (SHARES) High Frequency (HF) Radio Program (SHARES), which allow for landline priority service access, determine pre-emergency priority restoration status, and provide a emergency message handling system by bringing together existing HF radio resources, respectively.

An area where new approaches are desperately needed across all sectors is cyber security. In addition to strengthening reactionary measures—such as our cyber threat detection and response capabilities—an appropriate portion of this attention needs to be given for longerterm fixes that address the roots of all these problems. What are often referred to as "vulnerabilities" in the cyber community are usually the manifestations of software design errors. Bold, new, robust paradigms for software programming languages and compilers are needed.

The frontier of new possibilities is vast. To optimize the effectiveness and economics of critical infrastructure protection, DHS must remain vigilant regarding applicable new technologies and capabilities.

Question: **3. In your opinion, is the DHS Directorate of Information Analysis and Infrastructure Protection (I AlP) optimally organized to address the critical infrastructure sectors of greatest national security concern? Does it have adequate access to intelligence? Does it have relevant sector-specific technical expertise? Is it adequately staffed? Is its relationship with other relevant federal agencies—for example the DOE and EPA—on security matters clearly and well defined? Is the IAIP directorate sufficiently transparent to state and local officials and to owners of critical infrastructure?**

McCarthy Response:

I am not privy to the Department of Homeland Security's intelligence data or hiring practices, and therefore unable to comment on this question.

Orszag Response:

I do not have the relevant expertise to respond to this question. My colleagues (James Steinberg, Ivo Daalder, or Michael O'Hanlon) would be better qualified to answer it.

Watson Response:

It's too early to tell whether DHS/IAIP is optimally organized. The organization is maturing and leaders are still making changes as they see needs. Almost all intra-government efforts are not transparent outside of the government. It's also too early to tell whether it is adequately staffed or has developed effective relationships with other relevant Federal agencies. I do not have visibility into IAIP's access to intelligence, so cannot comment on its adequacy. IAIP has offered to house sector experts from each critical infrastructure, because they realize they do not have sufficient industry expertise. To date, the railroads have responded by seating two sector representatives within the

CSTARC. Regarding transparency, our experience to date is that DHS has been relatively opaque to state, local, and industry, it has been extraordinarily difficult to find people within DHS to discuss specific issues like interdependency modeling, exercises, and strategy, but I attribute this primarily to reorganization churn.

Rauscher Response:

The Department of Homeland Security Directorate of Information Analysis and Infrastructure Protection's organizational structure is critical to its being able to fulfill its role in supporting the protection of the nation's critical infrastructure. The form of this organizational structure should follow its functional priorities. For the communications infrastructure, these priorities are to establish and maintain trusted dialogue with the vast and diverse industry members, provide speedy dissemination of relevant threat information to these industry members, support emergency coordination within. the communications sector, and facilitate emergency preparedness and response coordination across sectors. In addition to these priorities, the communications industry may look to the DHS IAIP to support special needs from time to time. It is important for its structure to be flexible to speedily and effectively address these concerns when they arise.

It is vital for the IAIP to have immediate access to intelligence on physical and cyber threats. Such information is vital to trusted representatives of key communications companies to use to better protect their networks and other critical facilities. In order for this information to be useful, it needs to be transferred in a timely fashion and with appropriate details in order for it to be leveraged for effective critical infrastructure protection purposes. Currently, the DHS IAIP NCS provides daily reports, and, from time to time, special information reports and alerts, to the communications industry. Communications companies throughout the industry use this information to adjust their physical and cyber security protective procedures. For example, an alert detailing a specific threat can be used to guide the review of specific industry-agreed NRIC Best Practices. The communications industry also provides information back through the trusted environment of the NCS NCC and Telecom-ISAC. Critical infrastructure information sharing processes should be continuously improved with methods of better identifying data relevant to specific infrastructure concerns and strengthened with updated safeguards against leaks.

The IAIP cannot establish nor maintain needed expertise for the communications sector without close partnership with private industry. The nation's public communications infrastructure includes many networks consisting of thousands of network nodes that are operated by scores of distinct companies. The NCS Telecom-ISAC, NSTAC and the NRIC have provided coordination for cross-industry and government-to-industry responses, national policy guidance, and detailed Best Practices, respectively.

IAIP staffing level requirements will fluctuate substantially depending on the partnership architecture implemented. For example, the nation's communication's infrastructure is largely privately owned and operated. Strategies that have little, or ineffective dependence on private industry, and attempt to duplicate industry expertise will be much larger than necessary and an unnecessary expense. Also, because such a staff will not have day-to-day responsibilities for operating actual networks, such a strategy will result in unpreventable latency and limitations in the development of expertise. On the other hand, the NCS NCC has effectively implemented a partnership strategy with the communications industry since well before September 11, 2001. As a benchmark, the NCC staffing level needs have been raised due to a number of factors, including: a higher national priority for the reliability and security of the nation's public networks, a recognition for greater coordination among critical infrastructure sectors, and expanded industry membership.

For Peter Orszag's Response:

4. In your book, "Protecting the American Homeland: One Year On," you state that, "[Presidential Decision Directive]-63 designated key agencies to oversee the protection of critical national infrastructure, but many observers complained that the resultant apparatus was ineffective. Although the Office of Homeland Security now has broad supervision over this issue, it still needs closer attention." **Could you elaborate on this lack of effectiveness and what you mean by "closer attention"?**

Orszag Response:

"Closer attention" means grappling with the tradeoffs inherent in moving beyond a laissezfaire approach to homeland security. That approach will not work, but it is easy to go astray in devising alternatives—either by imposing excessive costs on the private sector or by failing to provide sufficient incentives for protection. The Department must exercise more leadership in how the nation should approach that difficult tradeoff.

Question: **5. In your book, "Protecting the American Homeland: One Year On," you state that, "The Administration's strategy leaves out several key priorities for action. . .[including] major infrastructure in the private sector, which the Bush Administration largely ignores. . . In early 2003, the**

Department of Homeland Security issued a strategy document for protecting critical infrastructure, but the document lacked the types of specific policy steps that are now overdue" What specific policy steps would you recommend that the DHS take?

Orszag Response:

Protecting the American Homeland identifies the specific steps that my co-authors and I believe are appropriate for protecting private-sector assets in the United States from terrorist attack.

For Mr. McCarthy and Mr. Watson

Question: **6. In your opinion, are the DHS and the White House providing comprehensive leadership to improve information sharing with state and local officials and with owners of critical infrastructure? Please discuss the effectiveness of measures already taken to improve information sharing, including Freedom of Information Act (FOIA) exemptions. Please discuss other measures that you believe the government should undertake to increase information sharing with critical infrastructure owners and with state and local officials?**

McCarthy Response:

This Administration is making great strides in engaging state and local governments, as well as owners and operators of critical infrastructures, in conversations about security, reliability, and performance. For example, our current Mitigation Priority Analysis project depends on inputs from a myriad of regional entities: the state/city governments of DC, Maryland, and Virginia; county governments, like Montgomery (MD), Arlington (VA), and Fairfax (VA); and the businesses that run the four sectors that are being studied, like PEPCO, Dominion Virginia Power, Metro, and various water processing plants. This is an important foray into establishing critical infrastructure processes on a regional level, as well as national.

The Administration has also addressed industry's concerns that sensitive, proprietary information remain private, even if shared with the government. In April, DHS released its draft Critical Infrastructure Information (CII) regulations. These regulations, once adopted, will allow owners of critical infrastructures to share certain information with the Department with assurances that such information can only be accessed by specific individuals. The information will be protected, and not subject to outside access through the Freedom of Information Act (FOIA) process. This is a first step, but an essential one, towards private sector information sharing.

The Department of Homeland Security is not the only agency concerned with keeping sensitive information from prying eyes. Other agencies have ″lead″ status with certain industries, and have established similar regulations concerning sensitive information. For example, after the 9–11 attacks, the Federal Energy Regulatory Commission (FERC) removed from its reading room detailed maps and other information about electric power facilities and natural gas pipelines. Although exempt from FOIA procedures, this information had traditionally been open and available to anyone who requested it. In February, 2003, FERC ruled that individuals wanting access to this information would have to apply for it. The application requirements include identification information, and take the need/purpose of the information into account. Access is granted on a case-by-case basis, and only to individual applicants.

Establishing a trusted relationship with industry can be a delicate process. Both DHS and the White House are laying the critical foundation to ensure that information sharing can be a positive experience for all involved.

Watson Response:

As stated above, DHS has reached out to the ISACs and the ISAC Council to establish information sharing mechanisms. The FOIA exemption in the law creating DHS removes a barrier to information to be shared by the private sector with DHS. (There is still an issue with sharing similar information at the state and local level where CII protection does not exist.) It is too early to assess whether these measures have been effective. Cross-sector and public-private information sharing is nearly as new to industry as it is to the Federal government, and we are developing mechanisms together. To date, DHS leaders have been very receptive to industry ideas regarding organization, protocols, contact lists, and frequency of communications.

One additional step that could be taken would be for DHS to sponsor research into real-time data sharing. Current ISAC and government efforts are limited to e-mail, phone, and webbased message traffic, which will always lag behind actual threats. The only way to get ahead of the curve is to establish real-time data sharing. The time between vulnerability disclosure and live exploitation is decreasing

dramatically, as is the time to maximum infection rate of a new worm or virus. Sometimes, filtering traffic at specific ports is the only interim defensive measure possible until vendors can develop software patches or signature updates for antivirus and intrusion detection programs. As these times approach zero, the only way defenders will have time to implement filters or block access will be real-time visibility of inbound and outbound traffic. Several companies, Federal agencies, and the CERT/CC have capabilities in this area, and the IT–ISAC is prototyping a multi-company and cross-ISAC capability. I believe both the sectors and the Federal government would benefit greatly from a comprehensive national capability to see real-time traffic in order to implement interim defensive actions in advance of attacks on critical infrastructure networks. Such a research project must include a consideration of privacy, protecting individuals, and companies' private, proprietary information should be built in to any real-time traffic sharing scheme.

One of the greatest barriers to information sharing is the lack of coordination of requests for information from multiple jurisdictions. DHS has not demonstrated sufficient intradepartment coordination, and has provided little to no leadership to the states. Since September 11, 2001, the private sector has encountered a flurry of state-by-state, municipality-by-municipality, and county-by-county information requests. These requests on industry have become unsustainable, and if left uncoordinated will lead to grossly inefficient and idiosyncratic security programs. Companies are diverting valuable resources in order to respond to state, municipal, and county inquiries. Thus, there is a compelling argument for Federal leadership and partnership with states, municipalities and counties in the formation of regularized inquiries to avoid inefficient duplication by multiple governmental entities. However, this should not be interpreted as a call for Federalization of security, but rather, should be viewed as a call for coordination among Federal, State, and local municipalities in regards to assembling and protecting information necessary to protect critical infrastructure information (CII) within DHS.

For example, it appears that earlier this year, DHS requested that states compile a list of their critical infrastructures. States were compelled to respond to the DHS request, for the state's response would help determine the amount of discretionary DHS funding the state would be allocated to improve emergency preparedness and response. However, the Emergency Response division within DHS did not coordinate the request with the IAIP division. An unfortunate oversight, for much of the information being requested of the states had already been compiled, and therefore protected under FOIA, by independent agencies that have now been subsumed by DHS. Therefore, I would argue that regardless of what governmental entity or authority seeks CII, industry should submit its CII only to DHS. The Federal law now provides DHS with the requisite authority to exempt CII from Federal FOIA disclosure. Most state and local governments have FOIA laws or information access laws that are not as stringent or broad enough to protect CII, which is most troubling. In addition, by having DHS as the main repository and clearing house for CII, Federal, state and local governments will not have to make duplicative requests to provide information that is already being held and protected by DHS. The administrative burdens placed on industry to provide duplicative information can be averted simply by having Federal, state, and local governments obtain the CII they require from DHS. DHS can than disseminate the information under the Federal law to other Federal, state, and local governments ensuring the protection of the provided CII. Finally, any Federal agency that has or will acquire CII through governmental request should send such CII information immediately to DHS for retention, as DHS has the proper legal authority to protect CII from disclosure.

Section 214 of the Homeland Security Act does not preempt state law and that the proposed rules under section 29.8(g) mirror the provisions of section 214. I do not advocate preemption, since a statutory change to section 214 would be required. Rather, it seeks DHS rules that would require DHS to become the CII repository for Federal, state, and local governments and that all requests for CII be first made to DHS by Federal, state, and local governments. In addition, DHS should require Federal, state, and local governments to make their initial CII inquiry to DHS, before seeking such information independently from the private sector. Under this proposal, State and local governments could still solicit information from individual companies. If the information was not currently held by DHS, the company would consider the request and respond accordingly to the Federal, state, or local government requestor. Of course, if the information had already been provided to DHS, industry would refer the Federal, state, or local government requestor back to DHS.

Question: **7. Do you believe that industry Information Sharing and Analysis Centers (ISACs) will be in a position to create a business case for traditional national defense or national security objectives? Why or why not?**

Are ISACs the best organizations to lead sector-based industry efforts to share critical infrastructure information? What is the role of the federal government in supporting industry ISACs? Is the federal government doing enough to support ISAC efforts?

McCarthy Response: Reference separate attachment on symposium summary Information is in committee files.

Watson Response:

First, it is important to remember that ISACs, as a generic group, do not represent the sectors. Again, there is no one size fits all solution for every sector. I do not believe ISACs should be in the traditional national defense or national security business, but should be a part of an overall assessment of threat that could be used for defending the country. Only when analysis indicates that industry sectors are the target of an attack on the United States should ISACs be involved in defensive efforts, and even then, it is the affected companies that must take defensive action, not the ISACs. I believe the ISACs are the best organizations to lead sector based industry efforts to share critical infrastructure information, but they are not the only sources of such information. Key owners and operators will have some information they can provide directly to other companies and governments to augment that coordinated by ISACs. Critical infrastructure owners and operators that do not belong to an ISAC may have information of which neither government nor ISACs are aware. As ISACs mature and information-sharing mechanisms become more robust, the ISACs will evolve into a more central role in critical infrastructure information sharing.

The Federal role in supporting ISACs is primarily participation as a full partner in the process. I recommend three areas for improvement in the Federal government's role as partner to industry:

a) Improve timeliness and quality of threat information shared with industry ISACs. Information is flowing from government to industry, but because of sanitization and classification requirements, information from government is usually hours or days later than that flowing from industry to government on the same threats. In addition, specifics regarding threat organizations, intents, and targets, are not often shared.

b) Provide feedback to industry on the value of information provided by ISACs to government, and details on how that information is being protected by government. ISACs have been providing threat, vulnerability, countermeasures, and best practice information, along with analysis, to government, but in most cases it seems to go into a black hole. Feedback regarding usefulness would be valuable in prioritizing ISAC efforts. Transparency regarding steps taken to protect industry information would encourage more sharing from industry to government.

c) Coordinate requests for industry information. Currently, ISACs and other industry organizations receive multiple requests daily from the Federal government, many from separate DHS organizations, for similar or identical data. Industry organizations cannot scale resources to respond to all these requests, and have little understanding of the intended use of the information requested. Also, industry receives little information regarding the protection of the information. DHS should consolidate Federal requests of industry information, provide to industry the intended use of the information, the steps to be taken to protect it, and benefit (feedback) to the industry organization providing the information.

Question: **8. When attempting to prioritize limited resources, how important is it to have in place a comprehensive national critical-infrastructure risk-and-vulnerability assessment? To the extent that you are aware, please describe DHS' progress to date to produce such and assessment, including a prioritized national list, database, and geospatial map of critical infrastructures and key assets. What more should be done to speed progress on such an initiative? In your estimation, and in light of assessments that have already been done by states and industry, how quickly could a rough draft of a comprehensive national assessment of critical infrastructure be completed?**

McCarthy Response:

A comprehensive assessment of critical infrastructure risk will take years to complete. Certainly, a tool like this will assist in setting critical infrastructure priorities, but it is not the only one. One prime alternative is the National Capital Region (NCR) Urban Area Security Initiative (UASI) Project. The overall intent of this effort is to use the National Capital Region as a real world laboratory exercise to evaluate and propose future methods of critical infrastructure protection activities. George Mason plays an important role in Critical Infrastructure Protection Over-

sight, collaborating with university, industry, and government partners. Together, we will conduct an analysis of each critical infrastructure sector, with a focus on assessing vulnerabilities.

I do not have data on exactly what critical asset lists the Department does or does not have; understandably such information should be kept under lock and key. What I do know is that until such time as a comprehensive risk assessment can be completed, the Department must continue to think "outside the box." It must rely on creative and innovative projects like the NCR project to help set priorities and allocate the resources accordingly.

Watson Response:

A single, comprehensive national critical infrastructure risk and vulnerability assessment would not only be cumbersome, but a very dangerous target list. Most of it would also grow quickly out of date. Understanding regional cross-sector dependencies would help regional stakeholders make resource decisions, but a national list would have little value beyond the Ooh factor and braggadocio. At the national level, strategy, policy, and doctrine are most useful. Operational action must occur at the regional, operational level, and local, tactical level of defense. Use military planning as a model. Military units develop and maintain defensive plans that cover their specific bases, stations, units, taskforces, and ships. Every level of command develops plans and procedures appropriate to its area of influence (reach) and area of interest (threat). Neither the military service headquarters nor the Joint Chiefs of Staff get involved in specific unit planning. Rather, the Services and JCS provide strategy, policy, and doctrine, on which local commanders base their decisions. This is a good model for critical infrastructure protection planning, and supports my argument for regional exercises to identify key stakeholders and local cross-sector dependencies, and to develop cross-sector regional contingency plans. In the cyber dimension, planning must be global, since there are no borders in cyberspace. Therefore, cyber elements of regional exercises should be global, not regional or local.

In addition, the network elements most vulnerable at any given time are a function of what the threats are, a scenario which changes daily. For example, if current threat analysis suggested that nuclear power plants were being targeted, the list of telecommunications, emergency service facilities and other infrastructures most vulnerable would be significantly different than if certain water facilities were the target. As such, any list being generated is static, being compiled in the absence of specific threat scenarios and even at its best, would not be particularly meaningful for any significant period of time.

Question: **9. What progress has been made by states and industries to comprehensively assess critical infrastructure risks? Has the DHS done enough, in your opinion, to 1) provide sufficient leadership, guidance, and assistance to states and industry; and 2) leverage work already done by states and industry as it seeks to produce its own comprehensive national assessment?**

McCarthy Response:

We are aware that many states are currently in the initial stages of evaluating their risk status and levels of preparedness. The Department has contributed heavily to these efforts, as much as a young organization could reasonably be expected to contribute. It is equally important for states and industry to assume responsibility for action on these fronts. The Department also appears to have established strong working ties into the various state and industry efforts, and those contacts are likely to lead to a more informed national assessment.

Watson Response:

Several critical infrastructure sectors have completed sector-wide risk assessments, and indeed some of these have been doing so for several years. I recommend asking the Sector Coordinators about sector-specific risk assessments. The states are beginning to make assessments. Notable among these are New York and New Jersey, following the terrorist attacks of 9/11/2001. DHS is still too new to provide comprehensive guidance, but the priorities outlined in the Marsh Commission report and the three national strategies (Homeland Security, Physical Infrastructures, and Cyber Security), have provided sufficient direction for industries and states to get to work on assessments and contingency plans. Again, I believe a comprehensive national assessment would be largely useless, except in the cyber dimension.

QUESTIONS AND RESPONSES FROM DENISE SWINK, ACTING DIRECTOR, OFFICE OF ENERGY ASSURANCE SUBMITTED BY RICK A. DEARBORN, ASSITANT SECRETARY, CONGRESSIONAL AND INTERGOVERNMENTAL AFFAIRS

HEARING ON SEPTEMBER 17, 2003

Question: **1. Subsequent to the blackout of August 14,2003, have your investigations revealed any possibility that a cyberattack caused part or all of the power grid failure? If so, please elaborate.**

Answer: 1. A great deal of work has been done in this area including interviews with key personnel at sites where the outage related events began. As stated in the *U.S. Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout in the United States and Canada,* no evidence has been identified indicating that malicious actors are responsible for, or contributed to, the outage. There is also no evidence suggesting that viruses and worms prevalent across the Internet at the time of the outage had any significant impact on power generation and delivery systems. However, as discussed in response to Question 2, the Task Force Security Working Group (SWG) has concerns with respect to: the possible failure of alarm software; links to control and data acquisition software; and the lack of a system or process for some operators to view adequately the status of electric systems outside their immediate control.

Question: **2. Have your investigations revealed the failure of some computer monitoring systems at electric power facilities either before or during the blackout of August 14th? If so, please elaborate.**

Answer: 2. As discussed in the interim report, SWG analysis suggests that failure of a software program—not linked to malicious activity—may have contributed significantly to the power outage of August 14,2003. Specifically, key personnel may not have been aware of the need to take preventive measures at critical times because an alarm system was malfunctioning. The SWG continues to work closely with the operators of the affected system to determine the nature and scope of the failure, and whether similar software failures could create future system vulnerabilities.

Analysis of information derived from interviews with operators suggests that, in some cases, visibility into the operations of surrounding areas was lacking. Some companies appear to have had only a limited understanding of the status of the electric systems outside their immediate control. This may have been, in part, the result of a failure to use modem dynamic mapping and data sharing systems.

Question: **3. How can the Congress, federal agencies, and state and local governments best work together to coordinate the necessary upgrades and protections to computer systems at electric power facilities so that we lessen the threat of a cyberattack?**

Answer: 3. The nation's electric power facilities, in large part, belong to private companies. These companies must comply with numerous Federal and State statutory and regulatory requirements, and are closely regulated by Federal and State regulation bodies. However, these same companies are reluctant to apply cyber security guidelines and recommendations that have a questionable business case in light of a poorly defined threat. The threat in cyberspace is very difficult to define and is a point of controversy in the cyber security arena.

In order to persuade private sector companies to invest in cyber security, it is necessary for all concerned parties to work cooperatively to make a sufficient business case for these expenses. Better analysis/definition of the threat in an unclassified form is necessary in order to promote the adoption of upgrades and protections necessary to lessen the threat of a cyber attack.

Question: **4. This month, the American Society of Civil Engineers (ASCE) released a** *Progress Report on its 2001 Report Card on America's Infrastructure.* **In this report, the ASCE examined current status and trends in the nation's deteriorating infrastructure. In their assessment, the Energy infrastructure received a D+. Roads and Bridges received a D+/C; Transit a C-; Drinking Water a D; Wastewater a D; Dams a D; and Hazardous Waste a D+. Does the poor state of a number of our infrastructure sectors have serious negative implications for the security of those sectors against potential terrorist attack? What is the relationship between reliability and security when it comes to critical infrastructure protection?**

Answer: 4. The state of our infrastructure does play a role in our ability to protect against a potential terrorist attack and to respond to an actual terrorist attack. The better the condition of our infrastructure, the better our ability will be to protect against and respond to a terrorist attack. It is important to have a robust infra-

structure with an appropriate level of redundancy that can withstand an attack and still have capacity to meet critical needs and support an emergency response. Additionally, advance planning, good information systems, and well rehearsed infrastructure management techniques can aid in our response to an attack.

The relationship between reliability and security is vital for critical infrastructure protection. Private sector companies are driven by both legal requirements and the business case that supports a particular decision. The reliability of the services provided by various sectors is the foundation that helps these companies avoid regulatory penalties and provide customer satisfaction and public confidence in their operations. Therefore, the aging state of most of these critical infrastructures forces the companies that own and operate them to balance their limited resources between maintaining the infrastructure and protecting it. Since the cyber threat is poorly defined and the need to maintain operational reliability is an easily defined business case, limited resources are made available to the protection of the infrastructure, especially the cyber part of the infrastructure. This situation is further complicated by a general lack of understanding by the private and public sectors regarding the interdependencies of the critical infrastructures. For example, decisions on the appropriate security level for a bridge should include consideration of vital energy or telecommunications carried by that bridge in addition to the bridge's role in the transportation system.

Criticality of assets is very different depending on the approach you take to defining the criteria.

QUESTIONS FOR THE RECORD

HOUSE SELECT COMMITTEE ON HOMELAND SECURITY HEARING: ″IMPLICATIONS OF POWER BLACKOUTS FOR THE NATION'S CYBER-SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION: THE ELECTRIC GRID, CRITICAL INTERDEPENDENCIES, VULNERABILITIES, AND READINESS.″

SEPTEMBER 17, 2003

ASSISTANT SECRETARY LISCOUSKI

Question: **(1) Subsequent to the blackout of August 14, 2003, have your investigations revealed any possibility that a cyber-attack caused part or all of the power grid failure? If so, please elaborate.**

No. The investigation found no evidence that attackers were responsible for, or contributed to, the outage. AI-Qaeda claims to the contrary are false.

Question: **(2) Have your investigations revealed the failure of some computer monitoring systems at electric power facilities either before or during the blackout of August 14th? If so, please elaborate.**

Yes, a combination of human operator and non-malicious computer failures contributed to the August 14 power outage. The following timeline was derived from detailed discussions with FirstEnergy and the Midwest Independent Transmission System Operator (MISO). All times are approximate:

Time	Activity
12:40 EDT	At the MISO, a MISO EMS engineer purposely disabled the automatic periodic trigger on the State Estimator (SE) application, which allows MISO to determine the real-time state of the power system for its region. Disabling of the automatic periodic trigger, a program feature that causes the SE to run automatically every 5 minutes, is a necessary operating procedure when resolving a mismatched solution produced by the SE. The EMS engineer determined that the mismatch in the SE solution was due to the SE model depicting Cinergy's Bloomington-Denois Creek 230–kV line as being in service, when it had actually been out of service since 12:12 EDT.
13:00 EDT	After making the appropriate changes to the SE model and manually triggering the SE, the MISO EMS engineer achieved two valid solutions.

Time	Activity
13:30 EDT	The MISO EMS engineer went to lunch. He forgot to re-engage the automatic periodic trigger.
14:40 EDT	An operations engineer discovered that the SE was not solving. He went to notify an EMS engineer.
14:41 EDT	FirstEnergy's server running the AEPR software failed to the backup server. Control room staff remained unaware that the AEPR software was not functioning properly.
14:44 EDT	An MISO EMS engineer, after being alerted by the operations engineer, reactivated the automatic periodic trigger and, for speed, manually triggered the program. The SE program again showed a mismatch.
14:54 EDT	FirstEnergy's backup server failed. AEPR continued to malfunction. The Area Control Error (ACE) calculations and Strip Charting routines malfunctioned, and the dispatcher user interface slowed significantly.
15:00 EDT	FirstEnergy used its emergency backup system to control the system and make ACE calculations. ACE calculations and control systems continued to run on the emergency backup system until roughly 15:08 EDT, when the primary server was restored.—At 15:05 EDT, FirstEnergy's Harding-Chamberlin 345–kV line tripped and locked out. FE system operators did not receive notification from the AEPR software, which continued to malfunction, unbeknownst to the FE system operators.
15:08 EDT	Using data obtained at roughly 15:04 EDT (it takes about 5 minutes for the SE to provide a result), the MISO EMS engineer concluded that the SE mismatched due to a line outage. His experience allowed him to isolate the outage to the Stuart-Atlanta 345–kV line (which tripped about an hour earlier, at 14:02 EDT). He took the Stuart-Atlanta line out of service in the SE model and got a valid solution.
15:08 EDT	The FirstEnergy primary server was restored. ACE calculations and control systems were now running on the primary server. AEPR continued to malfunction, unbeknownst to the FirstEnergy system operators.
15:09 EDT	The MISO EMS engineer went to the control room to tell the operators that he thought the Stuart-Atlanta line was out of service. Control room operators referred to their ''Outage Scheduler'' and informed the EMS engineer that their data showed the Stuart- Atlanta line was ''up'' and that the EMS engineer should depict the line as in service in the SE model. At 15:17 EDT, the EMS engineer ran the SE with the Stuart-Atlanta line ''live.'' The model again mismatched.
15:29 EDT	The MISO EMS Engineer asked MISO operators to call the PJM Interconnect to determine the status of the Stuart-Atlanta line. MISO was informed that the Stuart-Atlanta line had tripped at 14:02 EDT. The EMS engineer adjusted the model, which by that time had been updated with the 15:05 EDT Harding-Chamberlin 345–kV line trip, and came up with a valid solution.
15:32 EDT	FirstEnergy's Hanna-Juniper 345–kV line tripped and locked out. The AEPR continued to malfunction.
15:41 EDT	The lights flickered at FirstEnergy's control facility, because the facility had lost grid power and switched over to its emergency power supply.
15:42 EDT	A FirstEnergy dispatcher realized that the AEPR was not working and informed technical support staff of the problem.

Question: **(3) In your written testimony you state that, ″We have conducted vulnerability assessments at electric power facilities, we have a protection**

strategy for key components, and we are working with industry and federal partners to determine the best way to implement that strategy.″ Could you describe for me what this protection strategy is for situations where a vulnerability assessment determines that a power facility might be subject to a cyber attack? I realize that there will be differences specific to each facility, but if you could generally elaborate on the strategy please.

The statement addressed the conduct of physical security vulnerabilities at electric power facilities and strategies the Office of Infrastructure Protection (IP) is devising for those facilities and other key components of the electric power infrastructure. Specifically, the National Cyber Security Division (NCSD) is examining critical infrastructures and associated key facilities, assets, physical plant, and control networks with a focus on their dependencies on cyber systems.

Regardless of whether a specific vulnerability is a physical- or cyber-induced, IP's strategy is to identify vulnerabilities, correlate those vulnerabilities to the known threat environment, and provide appropriate technical and other assistance to mitigate risks. IP shares identified vulnerabilities with the infrastructure owners and operators and, if requested, technical assistance. Mitigation actions range from advice about rewriting software code to improving physical security weaknesses.

Question: **(4) How can the Congress, federal agencies, and state and local governments best work together to coordinate the necessary upgrades and protections to computer systems at electric power facilities so that we lessen the threat of a cyber attack?**

IP believes that Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection, which President Bush signed on December 17, 2003, establishes the necessary national framework to guide federal infrastructure protection policy and programs. Specifically, it clarifies federal roles and responsibilities and describes interfaces with state and local authorities and the private sector. IP is moving swiftly to implement HSPD–7, which we believe will make a visible and measurable improvement in infrastructure protection. Key to that effort is a National Plan for Critical Infrastructure and Key Resource Protection that integrates both physical and cyber security measures in one planning framework.

Question: **(5) There is widespread acknowledgement of the importance of creating a comprehensive national critical infrastructure risk assessment in order to prioritize DHS efforts and manage spending. Carrying out comprehensive risk assessments, in general, is also mandated by Section 201 of the Homeland Security Act. In testimony before the full Committee on September 10, 2003, Governor Gilmore commented several times on the lack of an overriding homeland security strategy, based on a thorough threat, vulnerability, and consequence assessment, to drive priorities and DHS actions. In response to a question from Congressman Shays; Governor Gilmore remarked that the Administration has written a number of strategies but that none of them were based on an adequate risk assessment.**

On September 17, 2003 you testified before the joint hearing of the Subcommittee on Infrastructure and Border Security and the Subcommittee on Cybersecurity, Science, and Research and Development. Congresswoman Sanchez and Congresswoman Jackson-Lee questioned you in detail on the progress and status of such a comprehensive risk assessment. In response, you stated that, "I would be surprised, frankly, if we had that done in the next five years," and that "there will be no timeline in which we will say we are finished."Given the importance of comprehensive risk assessments and the requirements of the Homeland Security Act to develop a comprehensive national plan for securing the key resources and critical infrastructure of the U. S., does the DHS plan to publish at a certain point in time a document containing a comprehensive risk assessment of critical infrastructure, which would aid in the prioritization of protective measures?

Yes. IP expects to publish a plan by the end of September 2004. In the meantime, since March of last year, IP has on two occasions shared a comprehensive national risk assessment with the States. Moreover, the IAIP Directorate conducts assessments on every occasion in which the Secretary elevates the threat level. In these cases, IP provides guidance on setting priorities for protective measures. IP's first effort, which also featured the implementation of actions based on our risk assessment, took place during Operation LIBERTY SHIELD. The second was in response to the Congressional requirement to allocate grant funding based on identified threats and vulnerabilities. Results from both assessments were briefed to Congressional leadership.

Risk assessment is the cornerstone of IP's risk-managed, threat-driven operating model. Vulnerability assessments and threat assessments are part of this model. IP

examines and addresses vulnerabilities across the Nation's infrastructure by using a five-step risk management methodology that measures the national risk profile in the context, and absence, of threat information. The major steps of the risk management methodology include:

– Identifying critical infrastructure
– Assessing vulnerabilities
– Normalizing, analyzing, and prioritizing protective measures .
– Implementing protective programs
– Measuring effectiveness through performance metrics

The threat environment is dynamic. So, IP uses this methodology across and within sectors so that when credible and actionable threat information is known, the Office can assess the sector-specific and cross-sector impacts using existing vulnerability assessment information. This allows IP to quickly prioritize protective measures across and within sectors, and implement these measures quickly, to reduce the overall risk posed by the threat.

Question: **(6) The DHS has indicated that it will "provide core expertise in critical infrastructure sectors" and that it would organize along critical infrastructure sector lines. It is important for us to understand the progressthat has been made in staffing up the Office of Infrastructure Protection and integrating the organizations that it inherited. In your testimony, you indicated that the Infrastructure Protection Office currently has roughly 200 employees, staffing up to 450–500 people in 2004. Please provide a current detailed organizational chart of the Office of IP that indicates key functions and the number of employees by function. Please also provide a detailed list of currently staffed positions (by function and title; it is not necessary to provide individual names) as well as a list of open positions that you will fill by 2004.**

Please also provide a detailed list of employees (by title; do not indicate individual names) in your office with particular technical expertise in each of the critical infrastructure sectors. Please organize this list by the CIP sectors indicated in the The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Within each sector, please indicate title, level of education, predecessor federal agency (EPA, 000, etc. as appropriate) and years of relevant experience in that sector. Also please indicate open positions and expected hiring for 2004.

The following two figures depict Office of Infrastructure Protection positions.

Figure 1: Detailed Organization Chart

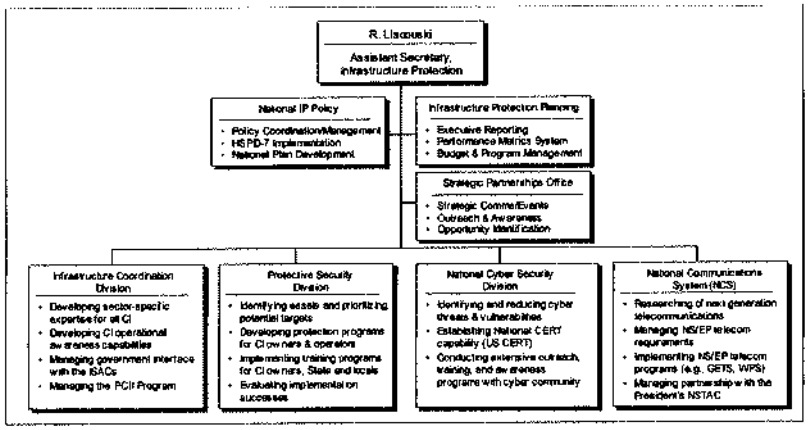
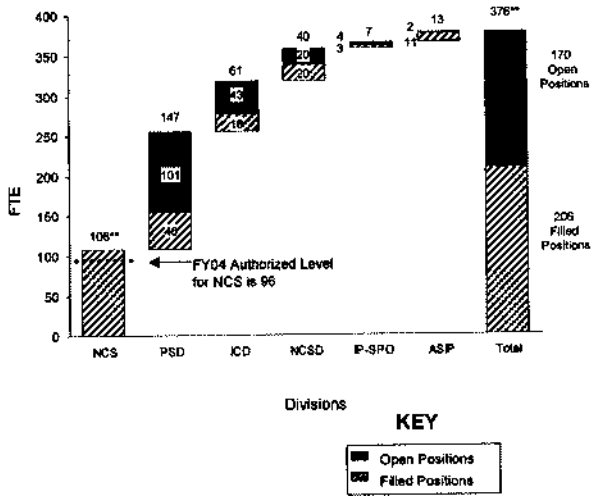


Figure 2. Office of Infrastructure Protection, Filled and Vacant Positions by Division[1]



IP possesses significant technical expertise that it is applying to address infrastructure threats and vulnerabilities. The Infrastructure Coordination Division serves as the focal point for infrastructure expertise and leads efforts to monitor and coordinate with each of the thirteen infrastructure sectors. In the coming months, ICD will formally establish a National Infrastructure Coordination center, where analysts will be assigned to monitor each of the thirteen infrastructure sectors

(6b) Please provide summary statistics (actual number of personnel as well as a percent of total Infrastructure Protection Office employees) for personnel along the following lines—

i) Professional vs. administrative
ii) Contractor vs. DHS employee
iii) Detailee vs. DHS employeeivy Technical expert vs. other
v) Advanced degree vs. bachelors degree or lower

Category 1: Professional
Professional staff: 192 (93.2%), Administrative staff: 14 (6.8%)

Category 2: Government v. Contractor
Government FTE: 206 (63.1%), Onsite Contractor: 120 (36.9%)
Category 3: Detailees
DHS Employee FTE: 178 (86.4%), Detailees from other agencies: 28 (13.6%)
Category 4: Technical Expert
Technical Expert: 146 (70.9%), Other: 60 (29.1%)
Category 5: Advanced Degrees
At this time, there are 49 employees with advanced degrees in the Office of Infrastructure Protection.

Question: **(7) Please provide a comprehensive list and brief description of all programs that the Office of IP has in place and initiatives that it is pursuing to increase critical infrastructure protection.**
The attached inventory of IP programs provides a high level summary of key selected programs.

Question: **(8) During the September 17, 2003 hearing, Congressman Lucas asked whether the "DHS relies too heavily on voluntary private sector action to improve their infrastructure protection." You responded that you**

[1] Notes: "Open Positions" based on FY04 authorized staffing level of 364 FTE; Total headcount increases to 376 when the 12 NCS detailees are included (which is beyond the current NCS authorized level of96); Large number of open positions in PSD is driven by need to establish field organization; All data accurate as of 3–19–04

"do not believe the voluntary approach in the private sector [to critical infrastructure protection] is the inappropriate approach." Do you believe, however, that the federal government should be doing more in any particular sectors? In particular, can you provide a more detailed answer to Mr. Lucas' question in light of an October 2002, letter to the Washington,Post, in which Secretary Ridge and former EPA administrator Whitman stated that for chemical facilities, "voluntary efforts alone are not sufficient to provide the level of assurance Americans deserve." Please respond to comments by Patrick Wood, chairman of the FERC, who stated in the Wall Street Journal in an article on the August, 2003, blackout that, "We cannot simply let markets work. We must make markets work"

IP has not seen the full transcript of Mr. Wood's comments and is unaware of the full context in which they were written. IP's philosophy is to work with industry advisory groups and private-sector standard-setting organizations to foster development of standards that will be voluntarily adopted by industry and, ultimately, by individual owners and operators. If IP judges that voluntary standards prove inadequate to meet pressing security concerns, the Office will consider additional steps to improve the protection of our Nation's infrastructures. For now, the programs IP has developed and is implementing will enhance the security and resiliency of the Nation's critical infrastructures and assets by providing practical, actionable advice and with tools and methodologies to improve security at little or no cost.

Question: **(9) In the absence of a comprehensive critical-infrastructure risk assessment from the DHS, can you let the committee know, in your opinion, which of our critical infrastructure sectors pose the greatest national security concern? Rank—in relative order starting with the highest concern the top five critical infrastructure sectors that you believe pose the greatest risk. Briefly discuss the reasons for your selections and rankings. In each of the sectors you describe, what has the private sector done since 9/11 to increase protection? What key initiatives have the Administration and the DHS pursued to improve protection and since when?**

Security considerations preclude an answer in this response. IP would welcome the opportunity to address this matter before the committee in closed session.

(10) In past testimony and reports, the General Accounting Office (GAO) has identified a number of significant CIP challenges, including:

- Clear delineation of CIP roles and responsibilities for federal, state, local, and private sector actors; clarification of how CIP entities will coordinate their activities
- Clear definition of interim objectives and milestones
- Clear timeframes for achieving objectives
- Establishment of performance metrics
- Improvement in analytical and warning capabilities

Please provide a detailed list of what significant interim objectives and milestones the DHS Infrastructure Protection Office has in place to improve critical infrastructure protection? [Q00605] What firm timeframes does the Office of IP have in place for these objectives?

IP has completed a number of actions not addressed here and is continuing to develop and implement guidelines and milestones for the CIP framework. This framework formulates a clear CIP plan, policies, priorities, and measures. In order to do so, the Office is forging partnerships with the key Federal, State, local, and industry stakeholders that will be crucial to our success. To drive and sustain this effort, IP is pursuing a systematic, risk management-based approach to identify, evaluate, and measure each of the critical infrastructures against a common and consistent set of factors. Some key objectives and milestones include:

1. Formulate a clear CIP plan, policies, priorities, and measures by—
   - Completing implementation of a DHS program office to handle foreign acquisition, control, or influence over critical infrastructure (2nd Quarter 2004)
   - Completing implementation of the Critical Infrastructure Information (PCII) program for protected CII voluntarily submitted by industry (4th Quarter 2004)

2. Clarifying ambiguous roles, responsibilities, and authorities with respect to CIP by—
   - Circulating the National Plan for Critical Infrastructure and Key Resources Protection to key Federal, State, and local critical protection stakeholders (4th Quarter 2004)

• Completing training for all State homeland security advisors and relevant Federal officers on their roles and responsibilities for infrastructure protection (4th Quarter 2004)

3. Developing nationwide critical infrastructure and key asset registry by
• Identifying and validating inventory of all critical infrastructure and key asset databases across federal, state, and local jurisdictions and the private sector (3rd Quarter 2004)
• Evaluating, setting priorities for, and consolidating all critical asset databases into a single database (3rd Quarter 2004)

4. Producing vulnerability assessments by sector, region, and localities by—
• Completing vulnerability assessments for the top 50 sites identified under HSPD #7, paragraph 7(a} (4th Quarter 2004)

5. Mapping threats to vulnerabilities by—
• Developing pilot risk assessment software to analyze economic consequence and loss of life for attacks against specific infrastructure targets and develop and disseminate risk assessment briefings for the first 500 of 1,000 critical facilities (3rd Quarter 2004)

6. Employing risk mitigation methodology to set priorities for protective actions and distribution of funds by—
• Collecting and evaluating protection and risk assessment methodologies used by the private sector; Federal, State, and local governments; and national laboratories to assess gaps in current infrastructure protection methodologies and developing plan to mitigate gaps in current methodologies (3rd Quarter 2004)
• Deploying the first 25–30 Protective Security Advisors to train infrastructure owners and operators to identify vulnerabilities and ensure appropriate protective measures are taken (4th Quarter 2004)

7. Establishing comprehensive overview of the status of physical and cyber infrastructure by—
• Identifying and modeling widespread cyber disruption scenarios (2nd Quarter 2004)
• Developing and piloting geospatial analysis tools and capabilities for the telecommunications and energy infrastructures (3rd Quarter 2004)

8. Issuing timely, effective warnings for specific, imminent threats by—
• Implementing Emergency Notification Service to automatically alert appropriate constituents of DHS alerts, warnings, and information bulletins (2nd Quarter 2004)
• Expanding coverage of the Critical Infrastructure Warning Information Network (CWIN) across government and industry CIP community to at least 100 total nodes (4th Quarter 2004)

9. Building partnerships with industry and other non-governmental groups by—
• Redesigning the Information Sharing and Analysis Center (ISAC) model in partnership with the ISAC Council and sector coordinators (3rd Quarter 2004)

10. Enhancing our ability to measure success and performance of our national infrastructure protection program—
• Conducting industry-wide survey for establishing baseline security measures that is sponsored by the American Society for Industrial Security in coordination with the Office of Infrastructure Protection (3rd Quarter 2004)
• Designing, develoing, and distributing metrics and feedback mechanisms for all CI sectors and key assets (4t Quarter 2004)

What performance metrics does the Office of IP have in place to measure its progress against objectives, milestones, and timeframes?

IP tracks progress of the objectives and milestones listed above on a monthly basis. Moreover, the Office is in the process of developing a Performance Measurement System that tracks both program efficiency and effectiveness. Underlying this system will be measurement methodologies that are statistically and scientifically valid and defendable. IP's goal is to use metrics to not only measure historical progress, but to prompt actions and behaviors that improve the protection and security of our nation's infrastructures.

Question: **(11) A number of states and industries have made significant progress in comprehensively assessing their own critical infrastructure vulnerabilities? What leadership role, if any, has the DHS played in providing leadership, guidance, and assistance to states and industry in these efforts? Has the DHS intelligently leveraged the work already done by**

states and industry to assess CI vulnerabilities as it seeks to perform its own comprehensive CI risk assessment?
In October 2003, the Office provided analyses and recommendations in two sets of sector-specific reports: the Potential Indicators of Terrorist Activities Report and the Characteristics and CommonVulnerabilities Report. Eight categories were selected for special attention during Operation LIBERTY SHIELD, and IP designed a comprehensive national plan to increase the protection of America's citizens and specific infrastructure within the United States during Operation Iraqi Freedom. As part of LIBERTY SHIELD, Secretary Ridge asked State governors to provide additional protection for 145 specific assets that fell within one of the those same eight categories:

- Chemical Facilities
- Nuclear Power Plants
- Nuclear Spent Fuel Storage Facilities . Petroleum Facilities
- Liquefied Natural Gas Storage Facilities . Railroad Bridges
- Subways
- Highway Tunnels

Using the above eight LIBERTY SHIELD-designated categories as a starting point, DHS has developed a Buffer Zone Protection Plan (BZPP) template for each. These plans were prepared to assist in better integrating federal, state, and local as well as private sector security planning and were distributed throughout the protective security community. BZPPs are designed to identify site-specific vulnerabilities, describe the types of terrorist tactics and activities that likely would be successful in exploiting those vulnerabilities, and recommend preemptive and protective actions to mitigate vulnerabilities so that terrorists are no longer able to successfully exploit them. As previously referenced in response to 0.00600, IP works with private industry to promote voluntary cooperation to protect critical infrastructures; this initiative offers an illustrative example of our philosophy in practice.

Question: **(12) To date, are you aware of how many states have performed comprehensive critical-infrastructure risk analyses? How many of the risk assessments performed by states has the Infrastructure Protection Office collected? What has the Infrastructure Protection Office done, if anything, to integrate the assessments conducted by the states into the comprehensive risk assessment efforts of the DHS?**
All of the states and territories completed their assessments by the end of last year. All of the inputs are being integrated into our risk assessment processes. Once completed, IP will start an iterative process with the states and territories to improve the quality and usefulness of the entire risk assessment effort.

Question: **(13) Does the DHS have insights into what methodology the states are primarily using for their risk assessments? What guidance has the DHS provided to states on what methodology they should be using? Are you familiar with the Department of Defense's CARVER methodology, which was used by California in its assessment of its critical infrastructure vulnerabilities? Do you have an opinion on whether the CARVER methodology is the most thorough standard that states should be following? If not, what methodology does the DHS recommend that states be following?**
IP is currently compiling and reviewing the submissions and inputs from the states on methodologies they are using to examine vulnerabilities. The Office is familiar with CARVER and believes it is a useful methodology. There are other acceptable methodologies developed by the government and by private industry. In the end, applying common principles to the process of identifying vulnerabilities, correcting them, and measuring performance is more important than the actual methodology used.

Question: **(14) How is the DHS Office of IP organized to coordinate with private sector ISACs? Are ISACs the best organizations to lead sector-based industry efforts to share critical infrastructure information? What role do you see for the ISACs going forward? Is the federal government doing enough to support ISAC efforts? Do you see role for federal funding of the ISACs?**
1The Infrastructure Coordination Division is the focal point for collaboration with the private sector ISACs. HSPD–7 reaffirmed the relationship between the ISAC community and the federal government. IP is collaborating with the ISAC Council to develop a framework that allows us to move forward as a community. The ISACs offer a primary means to support two-way information sharing between the owners and operators of facilities in an individual sector and across the thirteen infrastructure sectors. IP is satisfied with its current effort with the ISACs, but is actively

looking for ways to expand and improve information sharing capabilities with the critical infrastructure sectors. In addition to the ISACs, IP is working closely with the Sector-Specific Agencies and Sector CoordinatorslSector Leadership for each critical infrastructure sector to improve information sharing and operational coordination. Consistent with the provisions of HSPD–7, IP sees strong, trusted working relationships between all these entities—DHS, Sector-Specific Agencies, Sector Coordinators, and ISACs—as a cornerstone of an effective national risk management approach to protect critical infrastructures.

AIP continues to support the work of the critical infrastructure sectors and their ISACs, including financial support for sector-specific and cross-sector desktop exercises, cross-sector studies, and joint meetings.

Question: **(15) This month, the American Society of Civil Engineers (ASCE) released a Progress Report on its 2001 Report Card on America's Infrastructure. In this report, the ASCE examined current status and trends in the nation's deteriorating infrastructure. In their assessment, the Energy infrastructure received a D+; Roads and Bridges received a D+/C; Transit a C-; Drinking Water a D; Wastewater a D; Dams a D; and Hazardous Waste a D+. Does the poor state of a number of our infrastructure sectors have serious negative implications for the security of those sectors against potential terrorist attack? What is the relationship between reliability and security when it comes to critical infrastructure protection?**

The report cited is but one factor in our evaluation of the security of our national infrastructure which is, in many ways, a different issue than its reliability. In general, the more fragile an infrastructure, the nearer it is to the limits of its inherent resiliency and sustainability. It follows that a less robust infrastructure is more vulnerable to attack, is less likely to recover, and therefore poses a higher risk than a healthy one. The interplay between the security situation at specific facilities and the net overall effect on the entire infrastructure is a complex one, not susceptible to a broad response. For example, bridges may be vulnerable, but an attack on all at once would be an unlikely scenario. This is obviously a sensitive subject and we would ask that this report and its implications be discussed more fully in a classified environment.

United States Gengeral Accounting Office
Washington, DC 20548

December 8, 2003

The Honorable Dave Camp
Chairman, Subcommittee on Infrastrucutre
and Border Security
Select Committee on Homeland Security
House of Representatives

The Honorable Mac Thornberry
Chairman, Subcommittee on Cybersecurity,
Science, and Research and Development
Select Committee on Homeland Security
House of Representatives

Subject: *Posthearing Questions from the September 17, 2003, Hearing on "Implica*tions of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness"

As requested in your letter of November 5, 2003, this letter provides our responses for the record to the questions you posed to GAO. At the subject hearing, we discussed the challenges that the Department of Homeland Security (DHS) faces in integrating its information gathering and sharing functions, particularly as they relate to fulfilling the department's responsibilities for critical infrastructure protection (CIP).

Question: **GAO released a report on information sharing in August of this year. It found that "no level of government perceived the [information sharing] process as effective, particularly when sharing information with federal agencies." How does [this] finding relate to what happened during the August 2003 blackout?**

In our August 2003 report on information sharing, we identified initiatives that had been undertaken to improve the sharing of information to prevent terrorist attacks and surveyed federal, state, and city government officials to obtain their perceptions on how the current information-sharing process was working.[1] Our survey showed that none of the three levels of government perceived the current information-sharing process to be effective when it involved the sharing of information with federal agencies. Specifically, respondents reported that information on threats, methods, and techniques of terrorists was not routinely shared, and the information that was shared was not perceived as timely, accurate, or relevant. Further, 30 of 40 states and 212 of 228 cities responded that they were not given the opportunity to participate in national policy making on information sharing. Federal agencies in our survey also identified several barriers to sharing threat information with state and city governments, including the inability of state and city officials to secure and protect classified information, their lack of federal security clearances, and a lack of integrated databases. Further, this report identified some notable information-sharing initiatives. For example, the Federal Bureau of Investigation (FBI) reported that it had significantly increased the number of its Joint Terrorism Task Forces and, according to our survey, 34 of 40 states and 160 of 228 cities stated that they participated in information-sharing centers.

Performed primarily before DHS began its operations and not focused on the federal government's CIP efforts, this report did not specifically relate to the impact of these information-sharing challenges on any specific events, including the August 2003 blackout. However, as indicated in our written statement for the September 17 hearing,[2] our past information-sharing reports and testimonies have identified information sharing challenges and highlighted its importance to developing comprehensive and practical approaches to defending against potential cyber and other attacks, as well as to DHS meeting its mission.

Question: **A June 2003 GAO report on federal collection of electricity information found significant gaps in collection for information needed by different federal agencies. The report does not mention DHS. In light of the Department's responsibilities with respect to the electrical component of**

---

[1] U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened, GAO–03–760 (Washington, D.C.: Aug. 27, 2003).*

[2] U.S. General Accounting Office, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues,* GAO–03–1165T (Washington, D.C.: Sep. 17,2003).

critical infrastructure, what can you say about the kinds of information it needs, and whether it has the ability to obtain that information?

With the ongoing transition (or restructuring) of electricity markets from regulated monopolies to competitive markets, accurate information on electricity trading and pricing is becoming more critical not only for evaluating the potential benefits and risks of restructuring, but also for monitoring market performance and enforcing market rules. Our June 2003 report focused on describing the information that is collected, used, and shared by key federal agencies—such as the Federal Energy Regulatory Commission and the Energy Information Administration within the Department of Energy—and the effect of restructuring on these agencies' collection, use, and sharing of this information.[3] In the aftermath of electricity price spikes and other efforts to manipulate electricity markets in California, our work focused on the oversight of restructured electricity markets-not the physical security of the system's components. With this focus, we did not include DHS in the scope of our work.

However, we have made numerous recommendations over the last several years related to information sharing functions that have been transferred to DHS. One significant area concerns the federal government's CIP efforts, which is focused on the sharing of information on incidents, threats, and vulnerabilities, and the providing of warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector. Although improvements have been made, further efforts are needed to address the following critical CIP challenges:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;
- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector; and
- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other CIP efforts.

Regarding the kinds of information that DHS needs, the Homeland Security Act and other federal strategies acknowledge the importance of information sharing and identify multiple responsibilities for DHS to share information on threats and vulnerabilities for all CIP sectors. In particular:

- The Homeland Security Act authorizes DHS's Under Secretary for Information Assurance and Infrastructure Protection to have access to all information in the federal government that concerns infrastructure or other vulnerabilities of the United States to terrorism and to use this information to fulfill its responsibilities to provide appropriate analysis and warnings related to threats to and vulnerabilities of critical information systems, crisis management support in response to threats or attacks on critical information systems, and technical assistance upon request to private-sector and government entities to respond to major failures of critical information systems.

The *National Strategy to Secure Cyberspace* encourages DHS to work with the National Infrastructure Advisory Council and the private sector to develop an optimal approach and mechanism to disclose vulnerabilities in order to expedite the development of solutions without creating opportunities for exploitation by hackers.[4] DHS is also expected to raise awareness about removing obstacles to sharing information concerning cybersecurity and infrastructure vulnerabilities between the public and private sectors and is encouraged to work closely with private-sector information sharing and analysis centers (ISACs) to ensure that they receive timely and actionable threat and vulnerability data and to coordinate voluntary contingency planning efforts.

- The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* describes DHS's need to collaborate with the intelligence com-

[3] U.S. General Accounting Office, *Electricity Restructuring: Action Needed to Address Emerging Gaps in Federal Information Collection,* GAO–03–586 (Washington, D.C.: Jun. 30, 2003).

[4] The White House, *National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

munity and the Department of Justice to develop comprehensive threat collection, assessment, and dissemination processes that are distributed to the appropriate entity in a timely manner.[5] It also enumerates several initiatives directed to DHS to create a more effective information-sharing environment among the key stakeholders, including establishing requirements for sharing information; supporting state and local participation with ISACs to more effectively communicate threat and vulnerability information; protecting secure and proprietary information that is deemed sensitive by the private sector; implementing processes for collecting, analyzing, and disseminating threat data to integrate information from all sources; and developing interoperable systems to share sensitive information among government entities to facilitate meaningful information exchange.

Other efforts may help to identify specific information needs for the critical infrastructure sectors, including the electric power sector. For example, we are currently beginning work to determine the status of the ISACs in undertaking the voluntary activities suggested by federal CIP policy to gather, analyze, and disseminate information to and from infrastructure sectors and the federal government. In addition, according to the chairman of the recently established ISAC Council, the mission of the council is to advance the physical and cybersecurity of the critical infrastructures of North America by establishing and maintaining a framework for interaction between and among the ISACs. Council activities include establishing and maintaining a policy for inter-ISAC coordination, a dialog with governmental agencies that deal with ISACs, and a practical data and information sharing protocol (what to share and how to share).

Finally, as we discuss in more detail in the response to the next question, Congress and the administration have taken steps to help improve information sharing. These include the incorporation of provisions in the Homeland Security Act of 2002 to restrict the use and disclosure of critical infrastructure information that has been voluntarily submitted to DHS. However, the effectiveness of such steps may largely depend on how DHS implements its information sharing responsibilities and the willingness of the private sector and state and local governments to share such information. It may also require the consideration of various public policy tools, such as grants, regulations, or tax incentives.

Question: **The creation of "Critical Infrastructure Information" provides companies with a mechanism to voluntarily give this information to the federal government. Do you think that private companies will avail themselves of this opportunity? Do you think that Critical Infrastructure Information protections are sufficient? What other incentives might the federal government use to obtain this information for homeland security purposes? Should the federal government require the submission of this information so as to inform the Department of Homeland Security of potential cross-sectoral weaknesses and vulnerabilities?**

The Homeland Security Act of 2002 includes provisions that restrict federal, state, and local governments' use and disclosure of critical infrastructure information that has been voluntarily submitted to DHS. These restrictions include exemption from disclosure under the Freedom of Information Act, a general limitation on use to CIP purposes, and limitations on use in civil actions and by state or local governments. The act also provides penalties for any federal employee who improperly discloses any protected critical infrastructure information. In April 2003, DHS issued for comment its proposed rules for how critical infrastructure information volunteered by the public will be protected. At this time, it is too early to tell what impact the act will have on the willingness of the private sector to share critical infrastructure information or whether the protections that these provisions provide are sufficient.

Regarding other incentives that the federal government might use and the need to require submission of critical infrastructure information, the *National Strategy for Homeland Security* states that, in many cases, sufficient incentives exist in the private market for addressing the problems of CIP.[6] However, the strategy also discusses the need to use all available public policy tools to protect the health, safety, or well-being of the American people. It mentions federal grant programs to assist state and local efforts, legislation to create incentives for the private sector, and, in some cases, regulation. The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* reiterates that additional regulatory directives and mandates should only be necessary in instances where the market forces are insuffi-

[5] The White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: February 2003).

[6] The White House, *National Strategy for Homeland Security* (Washington, D.C.: July 2(02).

cient to prompt the necessary investments to protect critical infrastructures and key assets. The *National Strategy to Secure Cyberspace* also states that the market is to provide the major impetus to improve cybersecurity and that regulation will not become a primary means of securing cyberspace.

Last year, the Comptroller General testified on the need for strong partnerships with those outside the federal government and stated that the new department would need to design and manage tools of public policy to engage and work constructively with third parties.[7] We have also previously testified on the choice and design of public policy tools that are available to governments.[8] These public policy tools include grants, regulations, tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address security concerns. Some of these tools are already being used, for example, in the water and chemical sectors.

Without appropriate consideration of public policy tools, private-sector participation in sector-related information sharing and other CIP efforts may not reach its full potential. For example, we reported in January 2003 on the efforts of the financial services sector to address cyber threats, including industry efforts to share information and to better foster and facilitate sector-wide efforts.[9] We also reported on the efforts of federal entities and regulators to partner with the financial services industry to protect critical infrastructures and to address information security. We found that although federal entities had a number of efforts ongoing, Treasury, in its role as sector liaison, had not undertaken a comprehensive assessment of the public policy tools that potentially could encourage the financial services sector to implement information sharing and other CIP-related efforts. Because of the importance of considering public policy tools to encourage private-sector participation, we recommended that Treasury assess the need for public policy tools to assist the industry in meeting the sector's goals. In addition, in February 2003, we reported on the mixed progress that five ISACs (including the Electricity ISAC) had made in accomplishing the activities suggested by Presidential Decision Directive (PDD) 63.[10] We recommended that the responsible lead agencies assess the need for public policy tools to encourage increased private-sector CIP activities and greater sharing of intelligence and incident information between the sectors and the federal government.

Question: **In the absence of a comprehensive critical-infrastructure risk assessment from the DHS, can you let the committee know, in your opinion, which of the critical infrastructure sectors pose the greatest national security concern? Rank-in relative order starting with the highest concern—the top five critical infrastructure sectors that you believe pose the greatest risk. Briefly discuss the reasons for your selections and rankings. In each of the sectors you describe, what has the private sector done since 9/11 to increase protection? What key initiatives have the Administration and the DHS pursued to improve protection and since when?**

Much of our work on federal CIP has focused on cybersecurity and the overall threats and risks to critical infrastructure sectors. This work did not include assessments of specific sectors that would enable us to identify or rank which of the sectors pose the greatest national security concern or greatest risk. We believe that all the critical infrastructures are important in that, as defined by the USA PATRIOT Act and highlighted in the *National Strategy for Homeland Security,* they represent "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." Further, determining which sectors pose the greatest risk would require not only an assessment of individual sector security, but also consideration of the interdependencies among sectors. For example, assuring electric service requires operational transportation and distribution systems to guarantee the delivery of the fuel that is necessary to generate power. Also, the devices that control our physical systems, including our electrical distribution system, transportation systems, dams, and other important infrastructures, are increasingly con-

---

[7] U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will Be Pivotal to Success,* GAO–01–886T (Washington, D.C.: June 25, 2002).

[8] General Accounting Office, *Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy,* GAO–02–549T (Washington, D.C.: Mar. 28, 2(02).

[9] U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats,* GAO–03–173 (Washington, DC,: Jan. 30, 2003).

[10] U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors,* GAO–03–233 (Washington, D.C.: Feb. 28, 2003).

nected to the Internet. Thus, the consequences of an attack on our cyber infrastructure could cascade across many sectors.

The administration has taken a number of steps to improve the protection of our nation's critical infrastructures, including issuance of the *National Strategy to Secure Cyberspace* and the complementary *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Called for by the *National Strategy for Homeland Security,* these two strategies identify priorities, actions, and responsibilities for the federal government, including lead agencies and DHS, as well as for state and local governments and the private sector. However, we have not undertaken an in-depth assessment of DHS's cyber CIP efforts that could enable us to describe what DHS or the private sector have done to improve protection.

In past testimony and reports, the General Accounting Office (GAO) has identified a number of significant CIP challenges, including:

i) Clear delineation of CIP roles and responsibilities for federal, state, local, and private sector actors; clarification of how CIP entities will coordinate their activities

ii) Clear definition of interim objectives and milestones

iii) Clear timeframes for achieving objectives

iv) Establishment of performance metrics

v) Improvement in analytical and warning capabilities

Question: **Please provide a detailed list of what significant interim objectives and milestones the DHS Infrastructure Protection Office has in place to improve critical infrastructure protection. What firm timeframes does the Office of IP have in place for these objectives? What performance metrics does the Office of IP have in place to measure its progress against objectives, milestones, and timeframes?**

We have made numerous recommendations over the last several years related to information-sharing functions that have now been transferred to DHS, including those related to the federal government's CIP efforts. As you indicate, among the challenges we have identified is the need for a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures. We also identified the need to improve the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector. The Homeland Security Act of 2002 makes DHS and its Information Assurance and Infrastructure Protection directorate responsible for key CIP functions for the federal government, including developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States.

The *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* issued in February 2003 by the President identify priorities, actions, and responsibilities for the federal government, including federal lead departments and agencies and DHS, as well as for state and local governments and the private sector. Both define strategic objectives for protecting our nation's critical assets. The cyberspace security strategy provides a framework for organizing and prioritizing the individual and concerted responsibilities of all levels of government to secure cyberspace. The physical protection strategy discusses the goals and objectives for protecting our nation's critical infrastructure and key assets from physical attack. However, as we have previously testified, neither of the strategies (1) clearly indicates how the physical and cyber efforts will be coordinated; (2) defines the roles, responsibilities, and relationships among the key CIP organizations, including state and local governments and the private sector; (3) indicates time frames or milestones for their overall implementation or for accomplishing specific actions or initiatives; or (4) establishes performance measures for which entities can be held responsible.

We have not undertaken an in-depth review of the department's cyber CIP efforts, which would include an assessment of its progress in developing a comprehensive national plan that addresses identified CIP challenges and the development of analysis and warning capabilities.

Question: **How is the DHS Office of IP organized to coordinate with private sector Information Sharing and Analysis Centers (ISACs)? Are the ISACs the best organizations to lead sector-based industry efforts to share critical infrastructure information? What role do you see for the ISACs**

going forward? Is the federal government doing enough to support ISAC efforts? Do you see fa] role for federal funding of ISACs?

According to an official in the Infrastructure Protection Office's Infrastructure Coordination Division, this division is responsible for building relationships with the ISACs and is currently working with them and the sector coordinators (private sector counterparts to federal sector liaisons) to determine how best to establish these relationships. In addition, this official said that DHS's interagency Homeland Security Operations Center provides the day-to-day operational relationship with the ISACs to share threat and warning information.

As mentioned previously, we are currently beginning work that will focus on the status of ISAC efforts to implement the activities suggested by federal CIP policy. This work should provide more information about obstacles to greater information sharing, the role of the ISACs in sharing critical infrastructure information, and the assistance provided to these organizations by DHS and other federal lead agencies. Such federal assistance could include funding, such as the examples of ISAC funding that we discussed in our February 2003 report.[11] Specifically, the Energy ISAC reported that in the fall of 2002, the Office of Energy Assurance (then within the Department of Energy and now transferred to DHS) had agreed to fund ISAC operations-an agreement sought so that membership costs would not prevent smaller companies from joining. The new, cost-free Energy ISAC began operations and broad industry solicitation for membership in February 2003. Further, for the Water ISAC, the Environmental Protection Agency provided a grant for system development and expanded operations.

Question: **This month, the American Society of Civil Engineers (ASCE) released a Progress Report on its 2001 Report Card on America's Infrastructures. In this report, the ASCE examined current status and trends in the nation's deteriorating infrastructure. In their assessment, the Energy infrastructure received a D+. Roads and bridges received a D+/C. Does the poor state of a number of our infrastructure sectors have serious negative implications for the security of those sectors against potential terrorist attack? What is the relationship between reliability and security when it comes to critical infrastructure protection?**

The ASCE's 2003 progress report on its 2001 report card does not discuss the implications of deteriorating infrastructure conditions and security against potential terrorist attack.[12] Further, GAO has not specifically assessed whether the poor state of infrastructure sectors may have serious negative implications for security against potential terrorist attack. However, the relationship between reliability and security may be an appropriate consideration as DHS and the critical infrastructure sectors identified in federal CIP policy continue their efforts to assess the vulnerabilities of these sectors to cyber or physical attacks.

We are sending copies of this letter to DHS and other interested parties. Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512–3317. I call also be reached by e-mail at daceyr@gao.gov.

Sincerely yours,

ROBERT F. DACEY
Director, Information Security Issues

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed over-

[11] GAO–03–233.

[12] American Society of Civil Engineers, *2003 Progress Report: An Update to the 2001 Report Card, September 2003.*

sight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548
To order by Phone: Voice: TDD: Fax: (202) 512–6000, (202) 512–2537, (202) 512–6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:
Web site: www.gao.govjfraudnetjfraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424–5454 or (202) 512–7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512–4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548