HOMELAND CYBERSECURITY AND DHS ENTERPRISE ARCHITECTURE BUDGET HEARING FOR FISCAL YEAR 2005

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

OF THE

SELECT COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MARCH 30, 2004

Serial No. 108–44

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
23–174 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, MississPpi
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., North Carolina
Donna M. Christensen, U.S. Virgin Islands
Bob Etheridge, North Carolina
Ken Lucas, Kentucky
James R. Langevin, Rhode Island
Kendrick B. Meek, Florida
Ben Chandler, Kentucky

JOHN GANNON, *Chief of Staff*
TEPHEN DEVINE, *Deputy Staff Director and General Counsel*
THOMAS DILENGE, *Chief Counsel and Policy Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MARK T. MAGEE, DEMOCRAT *Deputy Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH & 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
Ben Chandler, Kentucky
Jim Turner, Texas, ex officio

CONTENTS

Page

STATEMENTS

WITNESSES

APPENDIX

HOMELAND CYBERSECURITY AND DHS ENTERPRISE ARCHITECTURE BUDGET HEARING FOR FISCAL YEAR 2005

Tuesday, March 30, 2004

House of Representatives,
Select Committee on Homeland Security,
Subcommittee on Cybersecurity, Science,
and Research and Development,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:06 a.m., in Room 2325, Rayburn House Office

Building, Hon. Mac Thornberry [chairman of the subcommittee] presiding.

Present: Representatives Thornberry, Smith, Camp, Linder, Gibbons, Cox (ex officio),

Lofgren, Andrews, (Del.) Christensen, Etheridge, Lucas, Langevin, Meek, and Turner (ex officio).

Also Present: Representative Dunn.

Mr. Thornberry. The hearing will come to order. I would like to welcome our witnesses and guests to this hearing of the Subcommittee on Cybersecurity, Science, and Research and Development.

Last year, we received a number of perspectives on cybersecurity from academia, think tanks, the technology industry, government agencies, users, and others. All want the Department to succeed in its mission to protect our Nation. All emphasized the importance of cyberspace and the need for stronger cybersecurity in government, industry, academia, and at home.

Now, as we move into the second year of the Department of Homeland Security there remain many areas in cybersecurity in need of improvement. Cyber is an area that can touch across virtually every aspect of our lives, from electrical grids, airport control towers, manufacturing, banking, chemical plants, and many other areas.

With the creation of the National Cybersecurity Division last June, I was pleased the Department acknowledged the need to consolidate the cyber mission into an organization that could have one voice in dealing with international, Federal, State, local, and private sectors. However, over the course of recent months I have been concerned that many of the cybersecurity resources within the Department remain fragmented and have not been integrated under the Cybersecurity Division.

Our Nation needs a seamless, well-functioning organization within the Department to work with industry, other government elements, academia, and the home user. That is part of the external cybersecurity mission of the Department.

But there is also an internal cybersecurity mission for the Department. The Chief Information Officer has responsibility for protecting the Nation's most sensitive data that has been entrusted to the DHS to counter terrorism against the homeland. As the Department develops its enterprise architecture, privacy and classified information are two areas that must be considered as the networks from the 22 agencies are brought together.

I also believe that the Department must be a role model for the rest of government as well as the private sector in how they secure their own information infrastructure. DHS needs to "walk-the-talk" and achieve the highest standards within the Federal Government and cybersecurity. The creation of the Department should also result in efficiencies through integration and also find the most effective use of resources.

I look forward to hearing about your progress in both areas over the course of the past year.

PREPARED STATEMENT OF THE HONORABLE MAC THORNBERRY, CHAIRMAN, SELECT COMMITTEE ON HOMELAND SECURITY

I would like to welcome our witnesses and guests to today's hearing.

Last year, this subcommittee received a number of perspectives on cybersecurity, from academia, think tanks, the technology industry, government agencies, users, and others. All want the Department of Homeland Security to succeed in their mission to protect our nation. All emphasized the importance of cyberspace and the need for stronger cybersecurity in government, industry, academia, and at home.

As we move into the 2nd year for the Department of Homeland Security, there remain many areas in cybersecurity in need of improvement. Cyber is an area that cross-cuts virtually very aspect of our lives. Electrical grids, airport control towers, manufacturing, banking, chemical plants, and many other areas are dependent upon their computers, information, and networks to be reliable and secure from attacks.

With the creation of the National Cybersecurity Division (NCSD) last June, I was pleased that the Department acknowledged the need to consolidate the cyber mission into an organization that could have "one voice" in dealing with international, federal, state, local and private sectors. However, over the course of recent months, I am concerned that many of the cybersecurity resources within the Department remain fragmented and have not been integrated under NCSD.

Our nation needs a seamless and well-functioning organization within the Department to work across industry, other government elements, academia, and the home user. That is part of the external cybersecurity mission for the Department of Homeland Security.

There is also an internal cybersecurity mission for the Department. The Chief Information Officer has the responsibility for protecting our nation's most sensitive data that has been entrusted to DHS to counter terrorism against the homeland. As the Department develops its enterprise architecture, privacy and classified information are two areas that must be considered as the networks from the 22 agencies are brought together.

I also believe the Department must be a role model for the rest of the government—as well as the private sector—in how they secure their own information infrastructure. DHS needs to "walk the talk" and achieve the highest standards within the federal government in cybersecurity. The creation of the Department should result in efficiencies through integration and also find the most effective use of resources. I look forward to hearing about your progress and plans for the coming year.

Before we turn to our witnesses, let me yield to the distinguished ranking member, the gentlelady from California.

Ms. LOFGREN. Thank you, Chairman Thornberry.

The Select Committee on Homeland Security is in the process of tracking the first ever authorization bill through the Department of Homeland Security, and I believe that today's hearing before this subcommittee will serve as an important part of the authorization process. We will focus on cybersecurity activities of the Infrastructure Protection Directorate and will explore the information technology and enterprise architecture issues facing the agency, and it will give us an opportunity to understand resource and policy issues pertaining to the budget request for the next fiscal year.

In addition, members may explore additional legislative issues relevant to the Director's activities for possible inclusion into the authorization bill.

Certainly, we have no shortage of issues to discuss with our witnesses today. Earlier this month President Bush and Secretary Ridge celebrated the first anniversary of the creation of the Department of Homeland Security. At the event, the President said, quote, one of the most important steps we have taken to fight terrorism is creating the Department of Homeland Security combined under one room with a clear chain of command many agencies responsible for protecting our Nation. Creating the newest department of our Federal Government was a tough task that required a lot of hard work, changing some old habits in order to merge into a new department. Unquote.

I think this assessment of the Department is pretty optimistic, and I know that while rank and file employees have worked very hard over this past year to get it up and running, I am not convinced that the leadership of the Department of Homeland Security should be celebrating at this time, particularly in the area of cybersecurity.

I am concerned about cyber policy in the Department. I am not convinced that cybersecurity is a priority within the overall Department of Homeland Security, and I am troubled by the lack of concrete cybersecurity accomplishments over the past year.

The release of the National Strategy to Secure Cyberspace was at the beginning of 2003. This policy paper established cybersecurity goals. At the end of 2003, the Department of Homeland Security convened a cybersecurity summit with major players in the technology industry in the Silicon Valley. Other than these two events, I am just not familiar with the work that is going on in DHS, and I think I am safe in saying that members of this subcommittee are somewhat frustrated.

The threat of a cyber attack is very real. In 2003, we saw increasing worm and virus spreads, and Business Week estimated that the damage from worms last year alone was over $13 billion.

Today's witnesses are Mr. Robert Liscouski, Assistant Secretary for Infrastructure Protection, Information Analysis, and Infrastructure Protection Directorate, and Mr. Steven Cooper, Chief Information Officer of the Department of Homeland Security. I hope that the witnesses today will be able to reassure this subcommittee that work is being done within the Department and that cybersecurity in fact is a priority for the administration.

I would also like to note my frustration at the tardiness with which the statements were delivered to the committee. The rules of the Homeland Security Committee prescribe that witnesses who wish to submit a written statement shall file them—not may, but shall file them 72 hours prior to the hearing. Mr. Liscouski's statement was filed 14 hours prior to this committee and Mr. Cooper's statement was filed 45 minutes before the committee hearing, and I think that that is a real disservice to every member of the committee as we obviously have not had the time to really study Mr. Cooper's statement or Mr. Liscouski's statement.

Before concluding, I would like to thank the chairman of this committee, Mr. Thornberry, who has led our committee with great skill and intelligence, and I appreciate his leadership. Thank you.

Mr. THORNBERRY. I thank the gentlelady, and let me echo her frustration with the delays in having the statements before us. Obviously, it makes it more difficult for all of us to do our job well.

Let me just, as a brief aside on timing. My understanding is that we will have votes roughly around 11:30. Mr. Liscouski also has another hearing in the Intelligence Committee around that time, and so I don't want to limit anything but the briefer we can all be in our questions and responses we can cover more territory. I appreciate both of our witnesses. Without objection, other members of course may submit opening statements for the record.

PREPARED STATEMENT OF THE HONORABLE JIM TURNER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND RANKING MEMBER, SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH & DEVELOPMENT

Thank you Mr. Chairman.

Good Morning Gentlemen. Mr. Liscouski, it is a pleasure to have you testify before our Committee again. Mr. Cooper, I believe this is the first time you have appeared before us—welcome.

The Department of Homeland Security's cybersecurity mission is two-fold. First, it is the key agency responsible for coordinating our nation's efforts to protect our computer networks and critical infrastructures. Second, it must ensure that its own information technology systems are well-integrated and armed with appropriate safeguards.

We recognize that these tasks are not easy but they must be done to help ensure the security of our homeland. The ever-changing nature of technology means that the Department must have the best expertise, personnel, tools, and full authority to effectively accomplish its mission.

Unfortunately, the Department is not making the progress needed to secure our nation from a cyber attack. It is also not moving quickly enough to integrate and protect its own information technology systems.

Mr. Liscouski, six months ago you appeared before this Subcommittee and told us that the Department, having finally found a Director to lead its cybersecurity efforts, was undertaking significant initiatives to further our country's efforts to secure cyberspace and prepare and respond to network attacks. To date, however, the cybersecurity initiatives that the have been unveiled have not gotten us much further than we were before the creation of the Department. Indeed, some of the initiatives appear to duplicate existing efforts.

Let me just mention a few specific areas in which I see the Department's efforts lagging.

- First, it is not apparent to me that the Department has in place the ability and authority to direct other agencies with specific expertise in the event of a cyber crisis.
- Second, the Department does not appear to have an effective and meaningful public—private cybersecurity partnership. Many in the private sector have little or no idea what you are doing, what is expected of them, or how they are supposed to integrate and coordinate with the Department.
- Third, the Department has not sufficiently moved forward with the *National Strategy to Secure Cyberspace* released by the Administration a year ago. Why haven't we yet seen clear assignments of responsibilities and deadlines for the Strategy's implementation? If it is because the strategy won't work or is ineffective—we need to know that.

- Lastly, Mr. Liscouski, the Department's 2005 budget does not clearly lay out what your directorate is planning to do to further our cybersecurity efforts. We've only seen broad assertions and categories of activities. There seems to be lacking a clear vision on what the Department is doing to secure cyberspace.

Mr. Cooper, I must say I am equally concerned about the state of the Department's efforts to build robust information technology systems within the Department and secure its own internal networks. There are specific areas, in particular, for which I am concerned.

- First, the Department's efforts to date have been too slow. Just last week, I saw one official stating that simple e-mail can't get passed to people in the same office and that it takes hours for e-mail to bounce around the Department to reach its destination. We won't win the war on terror if Homeland Security officials can't even talk to each other.
- Second, good and consistent information technology policies can help speed the integration of terrorist watch lists, strengthen the security of our borders, and allow us to "connect the dots" to find terrorists. It worries me, Mr. Cooper, that you have publicly suggested that a consolidated watchlist may not be necessary. In my view, achieving this goal is critical for making our homeland security programs work.
- Third, it is not clear to me, Mr. Cooper, that you have the sufficient authority to coordinate and direct the divisional Chief Information Officers within the Department. If this is a problem, I hope that you will be candid with us regarding any additional authorities your position requires.
- Lastly, this past December, the Department received a 34—the lowest grade of any agency—in the Government Reform Committee's annual grading of agencies on the security of their computer systems. The Department should be setting an example for the rest of government to follow—not trailing at the back of the class.

Gentleman, I thank you for appearing before our Committee today to address these important issues.

I appreciate both of our witnesses being here today. Let me first call on Robert Liscouski, Assistant Secretary for Infrastructure Protection at the Department of Homeland Security.

STATEMENT OF ROBERT LISCOUSKI, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY

Mr. LISCOUSKI. Thank you, Mr. Chairman, and distinguished members of the subcommittee. I appreciate the opportunity to be here this morning.

As you pointed out, I am responsible for infrastructure protection at the Department of Homeland Security, and I am pleased to be here before you today to discuss our progress that we have made in the National Cybersecurity Division and to discuss the President's fiscal year 2005 budget request.

In today's highly technical and digital world, we recognize that attacks against us may manifest themselves in many forms, including both physical and cyber attacks. And in addition, we recognize the potential impact of collateral damage from any one attack to a variety of assets. This interconnected and interdependent nature of our infrastructure makes our physical and cyber assets difficult to separate, and it would be irresponsible to address them in isolation.

The integrated approach that DHS takes toward protection of physical and cyber assets and responsive threats and protection of its vulnerabilities enables us to consider the full range of risks to the Nation, including loss of life, destruction of infrastructure services, economic impact, and national security implications. Recognizing that future terrorist attacks may not be limited to either physical or cyber acts but rather a combination of the two to amplify the impact, my office is organized to examine and address threats and vulnerabilities across the nation's infrastructure by using a five-step risk management methodology that measures the Nation's risk profile in the context of and in the absence of threat information. Those major steps of the risk management methodology include the identification of the critical infrastructure assets, the assessment of vulnerabilities, the normalization analysis and prioritization of protective measures, implementing protective programs, and then finally the measurement of effectiveness and performance outputs so we can determine whether what we are doing is the right thing.

The National Cybersecurity Division was created in June of 2003 to serve as a national focal point for the public and the private sectors to address the cybersecurity issues and to coordinate the implementation of a national cyber strategy to secure cyberspace.

Under that mandate, the National Cybersecurity Division has been working closely with our partners in the Federal Government, the private sector, and academia on a variety of programs and initiatives to protect our information infrastructure. We recognize that the challenge is vast and complex, that the threats are multifaceted and global in nature, and that our strengths and our vulnerabilities lie in our interdependencies; that the environment changes rapidly, and that information sharing and coordination are crucial to improving our overall national and economic security.

The activities of the National Cybersecurity Division then are based on this understanding and designed to address each of the priorities set forth in the National Strategy to Secure Cyberspace.

Priority one, a national cyberspace secure response system;

Priority two, a national cyberspace security threat and vulnerability reduction program;

Priority three, a national cyberspace security awareness and training program;

Priority four, securing the government's cyberspace; and,

Priority five, national security and international cyberspace security cooperation.

When I appeared before the committee—before the subcommittee in September of 2003, I announced that Mr. Amit Yoran was to become the Director of the National Cybersecurity Division. Under his leadership, the division has aggressively pursued partnerships and programs and is building a strong team to meet its objectives. I also announced the creation of the U.S. Computer Emergency Readiness Team, or the US–CERT. The US–CERT is a key component of our cyber strategy and readiness and response system and the National Cybersecurity Division's operational arm. The US–CERT provides a national coordination center that links public and private response capabilities to facilitate information sharing across infrastructure sectors and to help protect and maintain the continuity of our Nation's cyber infrastructure.

On 28 January of this year, the Department of Homeland Security through the US–CERT unveiled the National Cyber Alert System. It is an operational system developed to deliver targeted and timely and actionable information to Americans to secure their computers. At the U.S. government, we have the responsibility to alert the public of imminent threats and to provide protective measures where we can, and minimally to provide information necessary for the public to protect their systems.

The day we inaugurated the system, the US–CERT site received more than 1 million hits. And today, from the first few weeks of that site, we have more than 250,000 direct subscribers who receive the National Cybersecurity Alert information to enhance their cybersecurity. And I urge you all to visit that site at www.US–CERT.gov, to subscribe to our information services.

To facilitate the preparation interagency and public-private cooperation coordination during and to recover from cyber incidents, we have created the Cyber Interagency Incident Management group, or Cyber IIMG. The Cyber IIMG coordinates intergovernmental preparedness and operations to respond to and recover from cyber incidents and attacks. The group brings together senior officials from national security, law enforcement, defense, intelligence, and other government agencies that maintain significant cybersecurity capabilities and that can bring to bear in response to an incident and, importantly, possess the necessary statutory authority to act.

We have also broadened our interagency partnerships to create two new groups addressing the various challenges before us. The first is a Chief Information Security Officers Forum, CISO Forum, established to provide a trusted venue for our government information security offices to collaborate and share effective practices, initiatives, capabilities, successes, and challenges.

The second group is the Government Forum of Incidents Response and Security Teams, FIRST, a group of technical and tactical practitioners of security response teams responsible for securing government information technology systems. GFIRST members work together to understand and handle computer security incidents and to encourage proactive and preventive security practices.

One of our most important constituencies of course is the private sector, because as you well know it is estimated that 85 percent of America's critical infrastructure is owned and operated by the private sector, and technology developed by the industry continues to fuel the growth and the evolution of the Internet.

In December 2003, the Cybersecurity Division co-hosted the first National Cybersecurity Summit, which allowed the Department to work side by side with leaders in industry to address key cybersecurity issues facing the Nation. The Cyber Division is also working closely with research and academic communities to better educate and train future cyber analysts, and we are participating in the National Science Foundation Scholarship For Service, or the Cyber Corps program as well as the National Security Agency's Information Assurance Centers for Excellence, academic excellence in 26 States, for which there are 50 centers.

The National Cybersecurity Division is only 9 months old, but these initiatives represent considerable progress toward making cybersecurity a reality and reflect our collective commitment to do much more. Each accomplishment fosters further activity which we have outlined in our fiscal year 2005 budget. The national cybersecurity budget for fiscal year 2005 request is $79 million, and it is based upon ongoing and future activities necessary to meet our mission.

The division is positively exploiting the work of its predecessors and building crucial partnerships as part of DHS's overall efforts to enhance the protection of our Nation's critical infrastructure. We have much to do and it will take time, resources, dedication, energy, and hard work to succeed. We are committed to that challenge, and we look forward to the opportunities to update the subcommittee on our progress.

We are also approaching the next National Cybersecurity Day, I would like to point out, which is this Sunday. And as Americans turn their clocks forward, we also urge them to take this opportunity to review and improve their cyber readiness.

Again, I thank you for the opportunity to testify before you today, and I would be pleased to answer the questions at your convenience.

[The statement of Mr. Liscouski follows:]

PREPARED STATEMENT OF THE HONORABLE ROBERT LISCOUSKI

Good morning, Chairman Thornberry and distinguished Members of the Subcommittee. My name is Robert Liscouski, and I am the Assistant Secretary for Infrastructure Protection in the Department of Homeland Security (DHS). I am pleased to appear before you today to provide an update on the Department's National Cyber Security Division's efforts in coordinating cyber security initiatives since my appearance in September 2003 and to discuss the President's FY 2005 budget request for the Division. In my testimony today, I will share information on a number of initiatives that use diverse channels of communication to reach our government partners as well as our mutual constituents—home users, small and medium-sized businesses, and corporations.

Introduction

March 1st marked the one-year anniversary of the Department of Homeland Security. In his remarks commemorating that day, Secretary Ridge stressed the Department's goal to strengthen information sharing and infrastructure protection over the next year. We in the Information Analysis and Infrastructure Protection Directorate (IAIP) take that mandate to heart in our collective efforts and activities to protect the Nation. Established by the Homeland Security Act, the IAIP Directorate leads the Nation's efforts to protect our critical infrastructures from attack or disruption, and under the leadership of Under Secretary Frank Libutti has made significant strides toward that objective.

The IAIP Directorate includes the Office of Information Analysis, the primary gathering and analytic center for threat information and intelligence within DHS, and the Office of Infrastructure Protection (IP), for which I am responsible. In today's highly technical and digital world, we recognize that attacks against us may manifest in many forms, including both physical and cyber attacks. In addition, we recognize the potential impact of collateral damage from any one attack to a variety of assets. This interconnected and interdependent nature of our infrastructure makes our physical and cyber assets difficult to separate, and it would be irresponsible to address them in isolation. The placement of our two offices within the Directorate underscores this linkage and enables us to work together to share intelligence and other information and coordinate our efforts to mitigate our vulnerabilities. Further, IP's component divisions work closely together to coordinate efforts regarding both physical and cyber threats and vulnerabilities and to develop plans that address the interdependencies between them.

Homeland Security Presidential Directive 7 (HSPD 7), released by President Bush on December 17, 2003, requires the development of a National Infrastructure Protection Plan that sets out a roadmap for assessing both physical and cyber vulnerabilities and, once the vulnerabilities are determined, articulating the protective actions that need to be taken. As such, IAIP takes a holistic view of critical infrastructure vulnerabilities and works to protect America from all threats by ensuring the integration of physical and cyber security approaches in the Directorate's Office of Infrastructure Protection.

This integrated approach to physical and cyber threats and vulnerabilities enables us to consider the full range of risks to the Nation, including loss of life, disruptions of infrastructure services, economic impact, and national security implications. Recognizing that future terrorist attacks may not be limited to either a physical or cyber act, but rather a combination of the two to amplify impact, IP includes the National Cyber Security Division, the Protective Security Division, the Infrastructure Coordination Division, and the National Communications System and is organized to examine and address threats and 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 our risk management methodology include:

- Identification of critical infrastructure
- Assessing vulnerabilities
- Normalizing, analyzing, and prioritizing protective measures
- Implementing protective programs
- Measuring effectives through performance metrics

By performing each of these steps continuously across and within each critical infrastructure sector, and by integrating threat information, we are continually improving our national critical infrastructure protection program—physical and cyber—and driving better correlation of protective programs to the dynamic threat environment.

National Cyber Security Division Mission: Coordinating our National Cyber Security

In support of the broader IAIP mission, the National Cyber Security Division was created in June 2003 to serve as a national focal point for the public and private sectors to address cyber security issues and to coordinate the implementation of the *National Strategy to Secure Cyberspace* released by the President in February 2003.

Under that mandate, the National Cyber Security Division has been working closely with our partners in the federal government, the private sector, and academia on a variety of programs and initiatives to protect our information infrastructure. We recognize that the challenge is vast and complex, that the threats are multi-faceted and global in nature, that our strengths—and our vulnerabilities—lie in our interdependencies, that the environment changes rapidly, and that information sharing and coordination are crucial to improving our overall national and economic security. The activities of the National Cyber Security Division, then, are based on this understanding and are designed to address each of the priorities set forth in the *National Strategy to Secure Cyberspace* ("the Strategy"):

Priority I:A National Cyberspace Security Response System
Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program
Priority III: A National Cyberspace Security Awareness and Training Program
Priority IV: Securing Government's Cyberspace
Priority V:National Security and International Cyberspace Security Cooperation

Meeting the Mandate: Readiness and Response

The National Cyber Security Division's primary overarching goal since its creation has been to enhance the Nation's Cyberspace Security (Readiness and) Response System (Priority I) that will, where possible, deter and prevent a cyber attack from occurring, limit its scope and impact on the critical infrastructures, and expedite recovery. In October 2003, we participated in *Livewire,* the first ever national-level cyber exercise to baseline our capabilities and communication paths for responding to national attack. The exercise involved over 300 participants representing more than 50 organizations across federal, state, and local governments and the private sector. Cyber attack simulation scenarios were developed to stress cyber interdependencies across our critical infrastructures and baseline our ability to collaborate across the public and private sectors. The information gleaned from *Livewire* validated the National Cyber Security Division's approach and activities. In that context, I will outline the National Cyber Security Division's accomplishments to date and discuss on-going and future programs that all serve to enhance our national cyber security.

When I appeared before the Subcommittee in September 2003, I announced the appointment of Mr. Amit Yoran as the Director of the National Cyber Security Division. Under his leadership, the Division is aggressively pursuing partnerships and programs and building a strong team to meet its objectives. I also announced the creation of the U.S. Computer Emergency Readiness Team, or US–CERT. US–CERT is a key component of our Cyber Security Readiness and Response System and the National Cyber Security Division's operational arm. Through its initial partnership with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, US–CERT provides a national coordination center that links public and private response capabilities to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of our Nation's cyber infrastructure. The overarching approach to this task is to facilitate and implement systemic global and domestic coordination of deterrence from, preparation for, defense against, response to, and recovery from, cyber incidents and attacks across the United States, as well as the cyber consequences of physical attacks. To this end, US–CERT is building a cyber watch and warning capability, launching a partnership program to build situational awareness and cooperation, and coordinating with U.S. Government agencies and the private sector to deter, prevent, respond to and recover from cyber— and physical—attacks.

One direct impetus of the *Livewire* exercise was to validate the importance of building a cyber information dissemination mechanism to reach our stakeholders. On January 28, 2004, the Department of Homeland Security through USCERT unveiled the National Cyber Alert System, an operational system developed to deliver targeted, timely and actionable information to Americans to secure their computer systems. As the U.S. Government, we have a responsibility to alert the public of imminent threats and to provide protective measures when we can, or least provide the information necessary for the public to protect their systems. The offerings of the National Cyber Alert System provide that kind of information, and we have already issued several alerts and the initial products of a periodic series of providing "best practices" and "how-to" guidance. We strive to make sure the information provided is understandable to all computer users, technical and non-technical, and reflects the broad usage of the Internet in today's society. I am pleased to report that Americans are exhibiting a keen interest in the alert system. On January 28th, the day we inaugurated the system, the US–CERT site received more than one million hits. Within the first few weeks, more than 250,000 direct subscribers received National Cyber Alerts to enhance their cyber security. For your reference and for your constituents, I urge you to visit *www.us-cert.gov* to subscribe to a number of our information services to facilitate protecting your computer systems. As we increase its outreach, the National Cyber Alert System is looking at other vehicles to distribute information to reach as many Americans as possible.

The *Livewire* exercise reiterated the critical need for government to share information and coordinate efforts at cyber incident preparation that enhance our effectiveness in responding to cyber activity. To facilitate preparation and interagency and public-private coordination during, and to recover from cyber incidents, we created a Cyber Interagency Incident Management Group, or Cyber IIMG. The Cyber IIMG coordinates intra-governmental preparedness and operations to respond to, and recover from, cyber incidents and attacks. The group brings together senior officials from national security, law enforcement, defense, intelligence, and other government agencies that maintain significant cyber security capabilities that they can bring to bear in response to an incident and, importantly, possess the necessary statutory authority to act. By meeting monthly, the Cyber IIMG is developing cyber preparedness and response plans that will help it to support the IIMG during national events with cyber implications, and ensure that during a cyber crisis the full range and weight of federal capabilities are deployed in a coordinated and effective fashion.

To enhance the level of communication among federal agencies in a crisis, DHS' IP is continuing to widen the reach of the Critical Infrastructure Warning Information Network, or CWIN. For those who are not familiar, CWIN is a technologically advanced, secure network for infrastructure protection, communication and cooperation, alert, and notification. As a private communications network, CWIN serves as a reliable and survivable network with no logical dependency on the Internet or the public switched network. In the event a significant cyber attack disrupts our telecommunications networks and/or the Internet, CWIN provides a secure and survivable capability for members to communicate. It is important for us to understand and prepare for any contingency. In this vein, DHS is extending the reach of CWIN's survivable architecture beyond federal agencies by working with critical private sector companies to establish CWIN nodes at their Network Operations Centers. The goal is to increase the number of CWIN nodes to 100 by the end of 2004, making it a robust and resilient capability that supports national cyber operations and response during times of crisis.

Key components of the National Cyber Security Division's efforts are laid out in Priority IV of the Strategy: Securing Government's Cyberspace. Consistent with law and policy, the National Cyber Security Division works with the Office of Management and Budget and the National Institute of Standards and Technology regarding the security of federal systems and coordinates with federal law enforcement authorities as appropriate. We have taken great steps to integrate existing frameworks into the system, such as the continued functionality of the Federal Computer Incident Response Center (FedCIRC) is being transitioned within US–CERT, as well as to create a new forum for coordination toward greater cyber security in the federal government.

We have also broadened our interagency partnerships to create two new groups addressing the various challenges before us. The first is the Chief Information Security Officers Forum (CISO Forum), established to provide a trusted venue for our government information security officers to collaborate and share effective practices, initiatives, capabilities, successes and challenges. The second is the Government Forum of Incident Response and Security Teams (GFIRST), a group of technical and tactical practitioners of security response teams responsible for securing Government information technology systems. GFIRST members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices. The purpose of the GFIRST peer group is to:

- Provide members with technical information, tools, methods, assistance and guidance;
- Coordinate proactive liaison activities and analytical support;
- Further the development of quality products and services for the federal government;
- Share specific technical details regarding incidents within a trusted U.S. Government environment on a peer-to-peer level; and
- Improve incident response operations.

The National Cyber Security Division has taken on aggressive plans for accelerated information sharing and collaboration efforts in both the CISO Forum and GFIRST. Already, both groups have increased information sharing horizontally across previously somewhat stove-piped organizations and improved the overall cyber preparedness of the U.S. Government.

Meeting the Mandate: Assessment and Analysis

A major component of the National Cyber Security Division's mission is our focus within the Office of Infrastructure Protection to coordinate efforts on physical and cyber threat and vulnerability identification and assessment, and the implementation of protective measures to reduce vulnerabilities that will enable IAIP to systemically address the security status of U.S. networks and the cyber components and dependencies of our critical infrastructures. This effort directly responds to the calls in the Strategy and HSPD 7 to:

- Develop a National Infrastructure Protection Plan;
- Complete and maintain a critical cyber asset inventory;
- Implement and expand standard methodologies to perform threat, risk, and vulnerability assessments;
- Develop and maintain an interdependency analysis capability to systematically understand the relationships between cyber and physical assets; and
- Identify and implement priority protective measures to mitigate vulnerabilities.

The National Cyber Security Division currently houses a number of operational, data analysis, and other diagnostic tools to assist in assessing our vulnerabilities. The US–CERT is developing a comprehensive Watch Operation that will provide a 24x7 single point of contact for national cyber incident detection, evaluation, response, coordination, and restoration. Some key tools that US–CERT funded and/or executed include:

- Common Vulnerability and Exposures (CVE), a dictionary of standard names for vulnerabilities that makes it possible to correlate information across vendor products
- Malware Analysis, a laboratory operation performing detailed analysis and characterization of malicious code to adequately notify the Government of specific dangers and threats to the critical infrastructure
- Security Analysis Program (SAP), a set of analysis tools and capabilities offered through US–CERT to (1) help agencies better monitor network security activity; (2) assist agencies in identifying configuration problems, unauthorized/unnecessary network traffic, network backdoors, and routing anomalies; and (3) gain better global situational awareness of network health and malicious activity. The use of these tools by the federal civilian agencies represents one way that we are transferring technology used by the military to increase our overall capabilities.

As part of our efforts to improve our situational awareness and analysis capabilities, the National Cyber Security Division is coordinating with the National Communications System (NCS) on the Global Early Warning Information System (GEWIS). GEWIS is an effort underway within IAIP to find a wide variety of sources, including open source and approved private information, which can be analyzed to provide better situational awareness of the Internet and its underlying infrastructures. GEWIS will allow DHS to assess the health of the Internet in a timelier manner and, as a result, coordinate with the appropriate stakeholders in responding to Internet events. GEWIS is currently being used by IP in conjunction with other resources to provide the current situational awareness capability. GEWIS is continuing to evolve, and over time will provide enhanced functionality.

Meeting the Mandate: Awareness, Outreach, and Cooperation

So far I have discussed the accomplishments we have made in readiness and response, assessment, analysis, and warning efforts at the National Cyber Security Division. Another major component of our work lies in the outreach and awareness programs that support every aspect of our efforts to improve and sustain cyber security. The Strategy clearly identifies the users and stakeholders in cyber security in Priority III as home users and small business, large enterprises, institutes of higher education, the private sectors that own and operate the vast majority of the Nation's cyberspace, and state and local governments. In Priority V, the Strategy also emphasizes that international cooperation is crucial to protecting ourselves in a world where attacks cross borders at light speed. The following components make up the National Cyber Security Division's outreach and awareness programs and serve as the basis for our recently initiated Partnership Program.

One of our most important constituencies is the private sector. It is estimated that eighty-five percent of Americas critical infrastructure is owned and operated by private companies, and technology developed by industry continues to fuel the growth and evolution of the Internet. In December 2003, the National Cyber Security Division co-hosted the first National Cyber Security Summit in Santa Clara, California with the Information Technology Association of America, TechNet, the Business Software Alliance, and the U.S. Chamber of Commerce. This event was designed to energize the public and private sectors to implement the *National Strategy to Secure Cyberspace*. The Summit allowed the Department of Homeland Security to work side-by-side with leaders from industry to address the key cyber security issues facing the Nation. Five interest areas were established to focus specifically in the areas of:

- Increasing awareness
- Cyber security early warning
- Best practices for information security corporate governance
- Technical standards and common criteria
- Security across the software development lifecycle

Perhaps most importantly, the Summit served as a call to action. It represented a logical transition point from developing a national strategy to energizing the public-private partnership to implement concrete, measurable actions to improve the security of America's cyber systems. The efforts of these working groups as well as those of other industry leaders will be vital as we move forward in implementing the National Strategy.

In addition to the National Cyber Security Summit, the National Cyber Security Division is working with a host of groups to better understand and address their cyber security issues and concerns. These groups include, among others, the President's National Infrastructure Advisory Council, the President's National Security Telecommunications Advisory Committee, and the private sector Information Sharing and Analysis Centers (ISAC). As a result of the working relationships that have been developed among state and local cyber security representatives, we are also facilitating a multi-state ISAC that will even further enhance information sharing at the state and local levels.

The National Cyber Security Division is also working closely with the research and academic communities to better educate and train future cyber analysts. We are participating in the National Science Foundation's Scholarship for Service, or "Cyber Corps" program as well as the National Security Agency's fifty Information Assurance Centers for Academic Excellence in twenty-six states. We are looking at a number of additional ways to raise cyber security awareness in our educational and professional programs, including exploring the K–12 curriculum with the Department of Education and exploring the possibility for the private sector to create independent information technology certification programs for IT security professionals.

A crucial role for the National Cyber Security Division is to cooperate and leverage expertise within the Department of Homeland Security. Within IP, the National Cyber Security Division coordinates with the Protective Security Division (PSD) on our physical and cyber interdependencies and activities. In addition, it works closely with the National Communications System (NCS), which runs the CWIN program and the Global Early Warning Information System (GEWIS) described above, and brings NCS's telecommunications system expertise to its efforts. Through its integrated approach to addressing the critical infrastructure, the Office of Infrastructure Protection also coordinates efforts with the 13 critical infrastructure sectors laid out in HSPD 7 and their respective Information Sharing and Analysis Centers (ISACs).

The National Cyber Security Division coordinates closely with IP's Infrastructure Coordination Division on the cyber elements of their efforts.

In addition to our coordinated work within IP, the National Cyber Security Division works with a number of other DHS organizations. Close linkage between the Office of Infrastructure Protection and the Office of Information Analysis, led by Assistant Secretary Patrick Hughes, promotes the ability to map threat information with cyber vulnerabilities. This mapping allows for the effective prioritization of potential risks so agencies may implement remediation efforts as quickly as possible to limit the impact of computer incidents.

The technology that drives cyber security needs and product demands develops very rapidly in today's environment. Therefore, IAIP and the Science and Technology Directorate (S&T) are working together to coordinate research and development activities in the important areas of critical infrastructure protection and cyber security. A program of regular, interactive meetings between the two directorates ensures a two-way flow of information and coordination of technical activities. S&T's cyber security portfolio scope and activities are driven by the threats and issues that warrant national-level concerns, including cyber attacks by hostile adversaries against the Nation's critical infrastructures, or attacks whose consequences are of sufficient magnitude to cause widespread economic or social disruptions. The National Cyber Security Division provides important input regarding the research and development requirements for S&T's cyber security portfolio based on its activities and insight into the needs for greater protection of our cyber systems. Initial technical emphases for the Cyber Security Portfolio include:

- Improving the security of Internet infrastructure protocols and developing migration paths for these protocols into commercial use;
- Research, development, testing, and evaluation investments aimed at next-generation cyber security technologies aimed at prevention of and protection against attacks; threat identification and tracking; monitoring, detection, and attribution of attacks; and immediate as well as longer-term response to attacks;
- Economic assessment and modeling to support the development of business cases for cyber security in addition to providing a foundation for risk-based cyber security decision making.

I have addressed many of our national efforts, but I want to emphasize our international partnership efforts as well. As the Strategy says, "America's cyberspace is linked to that of the rest of the world." Cyberspace is truly borderless, and our communications networks are inarguably interconnected. We need to defend our systems from the outside, but we can only do so with global cooperation and coordination. Therefore, the National Cyber Security Division's Partnership Program includes outreach and advocacy efforts with our global partners, through US–CERT outreach activities and in bilateral and multilateral discussions in conjunction with the Department of State, the Department of Justice, and the Department of Defense.

The National Cyber Security Division is only nine months old, but these initiatives represent considerable progress toward making cyber security a reality and reflect our collective commitment to do more. Each accomplishment fosters further activity, which we have outlined in our FY 2005 budget request.

National Cyber Security Division Budget Request FY 2005

The National Cyber Security Division Budget Request of $ 79 million for the fiscal year 2005 is based on the on-going and future activities necessary to meet our mission. The budget plan is organized around National Cyber Security Division's program initiatives in (1) Readiness and Response; (2) Strategic Initiatives; (3) Information Sharing and Coordination; and (4) Management and Administration. Please let me highlight some key initiatives in the plan.

Readiness and Response

The core building block for an effective National Cyberspace Security Readiness and Response System is the U.S. Computer Emergency Readiness Team (US–CERT).

US–CERT will require full funding of $59.3 million for its various existing and projected programs, including sustaining and improving the GEWIS, CWIN, Watch, and other programs described above. In its inaugural year, US–CERT is making significant progress in establishing critical operational capabilities and building key relationships within government, private industry, and academia. To further these advancements, FY05 will be a significant year for the US–CERT to continue building and enhancing present capabilities into even more responsive and robust ones.

Strategic Initiatives

The National Cyber Security Division's Vulnerability Assessment and Reduction Program in response to HSPD 7 is a central aspect of its Strategic Initiative endeavors, and the requested funding of $7.0 million will build upon the initial efforts undertaken in FY03 and FY04. Additional aspects of the Strategic Initiatives program include software assurance efforts, continued awareness and training efforts, and a series of tabletop and other exercises including a second *Livewire* exercise, our participation in the National-Level Exercise Program, and a planned set of cyber-specific tabletop exercises at the State and local level.

Information Sharing and Coordination

A critical aspect of the National Cyber Security Division's activities is outreach to the public and private stakeholders in the U.S. and interaction with global partners. $8.7 million will be used to support a variety of public awareness campaigns and outreach efforts—such as continued support of the Stay Safe Online campaign—as called for in the Strategy. IAIP will also build and expand international partnerships to raise cyber security awareness and cooperation to promote a global culture of security. Most importantly, it accomplishes the operational partnership executive of information sharing and collaboration.

Management and Administration

The National Cyber Security Division is building a significant team of technical and security experts and determining the infrastructure it needs in support of its numerous initiatives toward greater national cyber security.

Conclusion

The creation of the National Cyber Security Division reflects the recognition that we as a Nation are utilizing sophisticated information networks to increase productivity, encourage innovation in products and services, enhance daily lives, and communicate globally in an instant. Importantly, we are also using these innovations to enhance our national and economic security, facilitate our law enforcement and public safety efforts, and protect our individual privacy. As technology has developed, we have found more exciting ways to use it, and we have become increasingly dependent on it. But, we have also acknowledged that its proliferation across our critical infrastructures—the very same proliferation that makes us more advanced as a society and an economy—also makes us vulnerable to those who would use it to harm us. IAIP, through the coordinated efforts of its component divisions including the National Cyber Security Division, is working diligently to address those vulnerabilities and provide greater security without stunting the growth and benefits of the digital economy for all Americans. We are approaching the next National Cyber Security Day this Sunday, and as Americans turn their clocks forward, we will also be urging them take the opportunity to review—and improve—their cyber readiness.

In its short life, the National Cyber Security Division is positively exploiting the work of its predecessors, leveraging the existing expertise around it, and building crucial partnerships as part of DHS' overall efforts to enhance the protection of our Nation's critical infrastructures. We have addressed crucial operational components of our program and are improving them, and we are developing strategic plans for the future. We know we still have much to do and that it will take time, resources, dedication, energy, and hard work to succeed. We are committed to that challenge, and we look forward to future opportunities to update the Subcommittee on our progress.

Again, thank you for the opportunity to testify before you today. I would be pleased to answer any questions you have at this time.

Mr. THORNBERRY. Thank you.

Now we turn to Mr. Steven Cooper, who is the Chief Information Officer for the Department of Homeland Security.

STATEMENT OF STEVEN COOPER, CHIEF INFORMATION OFFICER, DEPARTMENT OF HOMELAND SECURITY

Mr. COOPER. Mr. Chairman and members of the subcommittee, good morning. I am Steve Cooper, Chief Information Officer for the Department of Homeland Security. It is my pleasure to appear before the subcommittee, and I wish to thank the chairman and members for providing me the opportunity to update you on our efforts and progress in integrating and securing information systems within the Department and to discuss the President's fiscal year

2005 budget for information technology. I would request that my written testimony be entered into the record.

Mr. THORNBERRY. Without objection, your testimony shall be in the record.

Mr. COOPER. Thank you.

The challenges facing those of us who comprise the information technology function of the Department of Homeland Security is complex. There are three major areas of focus.

The first is to ensure that the women and men on the front lines of the Department have all of the information technology enabled solutions and tools they need to safeguard the United States and to deliver our safety and service-related operational functions and capabilities. The war on terrorism is real, and we must deliver new mission solutions with quality and speed in a cost effective manner while maintaining already existing mission solutions that we inherited when the Department was formed.

The second area addresses the integration of IT enabled solutions. Guided by our enterprise architecture, we are identifying opportunities to consolidate and streamline mission solutions. In mission areas like threat identification and management, identity credentialing, in collaboration we have identified multiple solutions in use within the various organizational elements of the Department. Our goal is to help facilitate and support the operators and subject matter experts in our business units, and determine the optimal number and nature of mission solutions needed.

And the third area is to realize efficiency and economies of scale that the President and Congress have set forward when creating the Department of Homeland Security. Here, we must rapidly identify and eliminate existing overlap or redundancy within our IT infrastructure within the Department. However, we must ensure that we do no harm to mission solutions while we restructure and consolidate our infrastructure. In this case, we really are changing the tires on the car while it is moving.

In order to guide the information technology function in achieving success in these three overarching focus areas, I have, in concert with our Department of Homeland Security CIO Council, set eight priority force the IT function. I would like to share these with the committee.

Very quickly, they are: Information sharing, mission rationalization, IT portfolio management, information security, infrastructure transformation, enterprise architecture, IT governance, and IT human capital.

These priorities are aligned with the strategic priorities of the Department set forth by Secretary Ridge and Deputy Secretary Loy. For each priority, we are in the process of developing a case for change, the business case, a road map that outlines the activities, tasks, and deliverables needed to achieve the desired objectives and metrics by which we will measure success. I would like to highlight two of these eight.

First is enterprise architecture. In my previous testimonies, I have discussed the vision of strategy of DHS and how that strategy must be supported by a disciplined capital planning investment control process that is guided by business-driven enterprise architecture. With the release of the first version of enterprise architecture in September 2003, we made progress toward the goal of achieving, one, Department of Homeland Security IT infrastructure. Version 1 of the enterprise architecture describes a target information management infrastructure that will be dramatically different from the one we have today, one that will provide timely, accurate, useful, and actionable information to all individuals and stakeholders who require it all of the time. We believe this effort was truly unique in the Federal Government, and that we delivered a comprehensive and immediately useful target enterprise architecture in less than 4 months.

Version 1 of our enterprise architecture contributed to some of our investment decisions for fiscal year 2005. Work is currently under way on Version 2 of the enterprise architecture. This work will develop additional detail around the target architecture and enhance the transition strategy from Version 1 into a more detailed transition plan that will specifically enable the implementation of the target enterprise architecture.

Version 2 is currently on track for completion by the end of this fiscal year. Along with continuing the hard work of developing greater detail, we will continue reaching deeper to find more opportunities to consolidation and begin to develop new and improved mission support capabilities enabled by information technology.

Version 2 of the enterprise architecture, together with the associated transition plan, will serve as the basis for further improving DHS mission performance and facilitating information technology, alignment, integration, and consolidation.

DHS is a new organization formed a little over a year ago from 22 legacy agencies, each with their own culture, processes, and legacy information technology systems. Many of these legacy agencies had developed their own enterprise architectures prior to the establishment of the Department. The challenge for us is to implement an integrated DHS enterprise architecture, bringing together the good work that has been done within each of the organizational elements and, during that process, ensuring that the entire Department has the IT capabilities needed to accomplish our mission capabilities every day.

One challenge to achieving integrated homeland security enterprise architecture is having enterprise architecture that is sufficiently mature to support detailed alignment and analysis for IT investment management decision making. We used Version 1 to identify what we called quick hits, and these are outlined in release one of our enterprise architecture; we are currently developing Version 2 to support more detailed investment decision making.

Another potential challenge is overcoming resistance to change and obtaining management and organizational buy-in into our enterprise architecture initiative. The Department has placed a very high priority on our efforts. Deputy Secretary Loy has directed the major organizational components of DHS to participate in the development of Version 2. As we speak, there are more than five different business focus area teams comprised of subject matter experts from across the Department working in facilitated team sessions to make sure that the business model for enterprise architecture Version 2 accurately and comprehensively captures the capabilities and requirements needed to accomplish the Department's mission. The extent of each organizational element's participation in these business area focus teams is reported to the DHS Management Council and monitored on a bi-weekly basis.

The development of an enterprise architecture is an enormously complex process requiring considerable resources and a systematic methodology. However, DHS has already made good progress in meeting the goals of our desired target enterprise architecture. We are well on our way to consolidating many of the management functions from each of the 22 agencies, including financial and human resources. We have reduced to 10, 19 financial management service providers. We have moved from 13 separate contracting offices to eight. We have moved from 22 human resource offices to seven. We have moved from eight different payroll systems to three, and department experts expect to reduce this to one by the end of the year. And we have moved from 22 property management systems to three.

These are a few up-to-date examples of the progress we are making. It is, however, clear that we still have a long way to go.

I would like to highlight our fiscal year 2005 budget request very quickly.

Information contributes to every aspect of homeland security and is a vital foundation of the homeland security effort. My office has responsibility for providing IT leadership that will foster best management practices in managing IT, enhance efficiencies through shared services and coordination of acquisition strategies, ensuring systems are properly accredited and certified as secure, and being an advocate for business transformation, all necessary toward ensuring that our homeland is more secure. The leadership and funding provided through the Department's IT investments are crucial for maintaining an enterprise architecture that is fully integrated with other management processes, and for allowing the Department to participate in many of our e–Gov initiatives across the Federal enterprise.

The President's budget request for fiscal year 2005 includes a request for 226 million for departmentwide information technology investments. Included in the request is $95 million for information technology services, a portion of which will provide funding for the departmentwide geographic information system capability to improve the Department's enterprise portal. This funding provides for continuation of our enterprise architecture and planning efforts to address our evolving financial management system, eMERGE2, and funding to enable the development, the beginning of the development of our human resources information technology solutions.

Additionally, the request includes $31 million for information security-related activities.

Finally, the fiscal year 2005 budget request includes $100 million for wireless communications.

I would like to highlight some key things related to one of our eight priorities in closing, and that is information security.

Since its creation, the Department of Homeland Security has moved out aggressively to design and implement an information security program that will not only ensure compliance with all appropriate standards and regulations, but to also ensure that the entire

Homeland Security community has a secure and trusted computing environment from which to operate. The heart of our reporting structure is built around the congressional requirements expressed in FISMA, the Federal Information Security Management Act. In order to effect a comprehensive information security program, and in accordance with the provisions of FISMA, I have designated a Chief Information Security Officer who manages and oversees all the internal Homeland Security Department's information systems security activities. The FISMA report details compliance with Federal laws and policies and DHS information security policies and standards. DHS is in the process of implementing enterprise management tools to ensure the accuracy and completeness of FISMA reporting across the Department.

FISMA requires each agency to perform for each program and system periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices. We do follow and will apply the Self–Assessment Guide for Information Technology Systems from the National Institute of Standards and Technology and as mandated by law. This self-assessment guide utilizes an extensive questionnaire which we have already begun using in delivering our first Department of Homeland Security report.

I have selected a commercial off-the-shelf product called "Trusted Agent FISMA". This is an automated enterprise based management tool that maintains FISMA reporting data from all of our components and their plans and activities that captures and tracks security weaknesses and associated corrective milestones. In addition, it collects, processes, and stores all of the self-assessment information in accordance with the NIST guidance. We have deployed this system throughout DHS and have generated our first quarterly report. We expect this to improve the timeliness and accuracy of our reporting as this information is available *real-time* to the Secretary and other cognizant officials.

I thank you again for the opportunity to testify before you today, and am pleased to answer questions that the committee may have.

PREPARED STATEMENT OF STEVEN COOPER, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. Chairman and Members of the Subcommittee:

Good morning, I am Steve Cooper, Chief Information Officer for the Department of Homeland Security (DHS). It is my pleasure to appear before the Subcommittee, and I wish to thank the Chairman and Members for the providing me the opportunity to update you on our efforts and progress in integrating and securing information systems within the Department and to discuss the President's FY 2005 budget request for Information Technology. I will also update the Subcommittee on our Enterprise Architecture program efforts.

Enterprise Architecture

In his proposal for creating the Department over a year ago the President highlighted the use of enterprise architecture techniques to improve both the sharing and use of information. The President stated that the "development of a single enterprise architecture for the department would result in elimination of the sub-optimized, duplicative, and poorly coordinated systems <and processes> that are prevalent in government today. There would be rational prioritization of projects necessary to fund homeland security missions based on an overall assessment of requirements rather than a tendency to fund all good ideas beneficial to a separate unit's individual needs even if similar systems are already in place elsewhere."

In my previous testimonies, I've discussed the vision and strategy of DHS and how that strategy must fulfill the President's vision. Additionally, it must be supported by a disciplined capital planning and investment control process that is guided by business-driven enterprise architecture. With release of the first version of the enterprise architecture in September 2003, we made progress toward the goal of one DHS infrastructure. Version 1 of the enterprise architecture describes a target information management infrastructure that will be dramatically different from the one we have today, one that will provide timely, accurate, useful and actionable information to all individuals who require it all the time. We believe this effort was truly unique in the federal government in that we delivered a comprehensive and immediately useful target enterprise architecture in less than four months.

However, Version 1 of the Homeland Security Enterprise Architecture (HLS EA) defines the enterprise architecture at a conceptual level and outlines a general transition strategy that must be broken down further for the architecture to be implemented. Version 1, which was published at the end of September 2003:

- Identified common activities
- Proposed conceptual projects
- Proposed reusable business components
- Proposed Technology Patterns
- Began communications effort
    - Increased understanding of EA planning and integration
    - Increased the knowledge of the target architecture

Work is currently under way on Version 2 of the enterprise architecture. This work will develop additional detail around the target architecture and enhance the transition strategy from Version 1 into a more detailed transition plan that will more specifically enable the implementation of the target enterprise architecture. This effort currently consists of 5 business teams composed of about 45 business people charged with the responsibility of decomposing the common business activities. During this effort for Version 2, we will:

- Verify and augment transitional projects
- Verify and augment reusable business components
- Verify and augment technology patterns
- Prepare an HLS–EA Framework that identifies the products that will be produced by the department and that are expected to be produced by the Transitional Project Managers
- Prepare governance procedures and bodies to ensure alignment with the HLS–EA
- Ensure the integration of the transitional projects

Concurrently with the Version 2 effort, the enterprise architecture team is working with several large project offices, e.g., ACE and US–VISIT, to determine alignment to the transition strategy so that these project offices can immediately begin building to the target architecture.

Version 2 is currently on track for completion early in the 4th quarter, FY04. Along with continuing the hard work of developing greater detail, we will continue reaching deeper to find more opportunities for consolidation and opportunities to develop new and improved mission support capabilities enabled by information technology. Version 2 of the enterprise architecture, together with the associated transition plan, will serve as the basis for further improving DHS mission performance and facilitating IT alignment, integration, and consolidation.

Technical Reference Model Status

In Version 1 of the EA, we developed the DHS Technical Reference Model (TRM) by extending the TRM from the Office of Management and Budget Federal (OMB) Enterprise Architecture (FEA). The value of the TRM is to provide a common set of terminology for describing and organizing technology. We are currently working on further developing the DHS TRM by improving the structure of technology categories so that they promote consistency and are more meaningful across the Department.

In addition, we have made progress on filling in the Standards Profile (SP). The Standards Profile provides guidance to the components and major programs on what technologies to use to implement solutions to ensure consistency and interoperability with other solutions within the Department and the homeland security community. Our approach is to collect all of the technology standards from the component CIO offices and to organize them into the revised TRM for analysis. In many cases, the standards in place are consistent across the components and these consensus standards will be adopted as the Departmental standard. Standards that are adopted fall, generally, into four categories: Move-to, Divest, Hold, or Contain. As part of the process, we have assigned “stewardship” of specific standards to individuals within my CIO shop or to other appropriate individuals in the Department. As the standards are developed, they reviewed by the Applied Technology Working Group, in accordance with the EA Governance Process as a part of the IT strategic management framework, and are adopted by the Enterprise Architecture Board (EAB).

One particular area where the TRM from the EA Version 1 has been useful is in guiding investment in IT is in the area of "technology patterns." Patterns are repeatable solutions to recurring technical challenges that are based on best practices, typically from industry. In Version 1 of the EA, we identified over a dozen patterns that have significant applicability within the Department. As a result, one of the major business/IT initiatives within the Department, the eMERGE[2] program of the Resource Management Transformation Office (RMTO) has adopted the pattern approach and is in the process of acquiring technologies that implement several of the patterns identified. These patterns and technologies will form a technology foundation for other programs to leverage.

Implementation of "Quick Hits"

Definitions for the Quick Hits, foundational elements and activities that had to be in place to support achievement of an integrated enterprise architecture, have been completed and stewards have been recommended. The Quick Hits have begun to be integrated into existing projects. For example, RMTO will soon begin implementing some of the technology patterns included in the Technology Patterns Quick Hit. The Consolidated Enforcement Environment (CEE) project has formed a case management working group and is incorporating the Standardized Investigation Case Management Quick Hit into their plans and will be coordinating with the Department of Justice on a long term solution. The One Face at the Border initiative met the requirements for the Integration POE Workforce Quick Hit. The Office of Infrastructure Management, within the DHS CIOs office, is working toward Network Integration as part of their One DHS Infrastructure project.

Challenges Achieving an Integrated Enterprise Architecture, Timelines and Implementation

DHS is a new organization, formed a little over a year ago from 22 legacy agencies, each with their own culture, processes, and legacy IT systems. Many of these legacy agencies had begun development of their own Enterprise Architectures prior to the establishment of DHS. The challenge for DHS is to implement an integrated DHS Enterprise Architecture while ensuring that, during the process, the entire Department has the IT capabilities needed to accomplish the mission.

One challenge to achieving an integrated HLS EA is having an EA that is sufficiently mature to support detailed alignment and analysis for IT investment management decision-making. As I've noted previously, DHS developed Version 1 of the DHS EA in 4 months ending in September 2003. We also used Version 1 to identify Quick Hits and we are currently developing the HLS EA version 2, to support IT investment management.

Another potential challenge is overcoming resistance to change and obtaining management and organizational buy-in into the EA. The Department has placed a very high priority on the HLS EA. Deputy Secretary Loy has directed the major organizational components of DHS to participate in development of Version 2 of the DHS EA. As we speak, there are more than 5 different Business Focus Area Teams, composed of subject matter experts from across the Department, working in facilitated team sessions to make sure that the business model for EA Version 2 accurately and comprehensively captures the capabilities needed to accomplish the Department's mission. The extent of each organizational element's participation in these Business Area Focus Teams is reported to the DHS Management Council and monitored on a bi-weekly basis.

The development of an EA is an enormously complex process. The goal was to produce a foundation for enabling DHS to make decisions about DHS investments immediately and to begin to direct its resources away from stove-piped, duplicative systems and move to interoperable, enterprise wide systems providing improved mission capability. Although Version 1 of the EA is relatively conceptual in nature, it does provide a foundation for implementation. As noted, DHS has been using the principles and transition strategy as a basis for beginning to redirect resources from current investments.

As we speak, DHS is working on Version 2 of the EA. This version will include a transition plan that will be completed in June 2004. Version 2 will continue to build on the hard work of the first version by developing greater detail, reaching deeper to find more opportunities for consolidation, and establishing a consolidated framework for meeting mission need.

One of the difficulties in expediting implementation of such a major change, such as EA, is the degree to which that change can be managed and accepted by an organization. However, DHS has already made significant progress in meeting the goals of the EA. We are well on our way to consolidating many of the management functions from each of the 22 agencies, including financial and human resources systems.

- 19 financial management service providers were reduced to 10
- separate contracting offices were reduced to 8
- 22 human resource offices were reduced to 7
- 8 different payroll systems were reduced to 3 and DHS expects to reduce this to one by the end of the year.
- 22 property management systems have been consolidated to 3.

These are just a few of the examples of progress. And it is clear we still have a long way to go.

One of the first things we need to do is implement a full governance structure with enforcement authority to ensure that investments are aligned with the strategic goals. We have already made progress in this area. This week the DHS Enterprise Architecture Board (EAB)is open for business. The EAB is charged with the responsibility of reviewing all investments for their alignment to our EA. What this means is that all investments going through the FY06 budget process will have to demonstrate that it is achieving the goals of our transition strategy and that it is aligned to the technology standards identified in the EA. This will mean that the EAB will be responsible for reviewing nearly 300 investments this year. That is a daunting task for an organization.

Another area we could focus on to expedite the implementation is to increase the number of working groups focusing on specific areas within DHS that support the DHS mission. Currently, DHS has the Resource Management Transformation Office (RMTO), which is consolidating an enterprise solution for DHS administrative functions, such as accounting, acquisition, budgeting, grants, and procurement.

Department-wide Information Technology Investments Budget Request FY 2005

Information contributes to every aspect of homeland security and is a vital foundation for the homeland security effort. My office has responsibility for providing IT leadership that will foster best management practices in managing IT, enhance efficiencies through shared-services and coordination of acquisition strategies, ensuring systems are properly certified and accredited as secure, and being an advocate for business transformation, all necessary toward ensuring the homeland is made more secure. The leadership and funding provided through the Department's IT investments are crucial for maintaining an enterprise architecture that is fully integrated with other management processes, and for allowing DHS to participate in many E-Gov Initiatives.

The President's budget request for FY 2005 includes a request for $226 million for Department-wide Information Technology Investments. Key strategic issues in FY 2005 will be to build and expand upon the foundational work completed in FY 2003 and FY 2004; to facilitate consolidation of management function capabilities; to lead the implementation of the Department's Enterprise Architecture; and, to continue to coordinate information integration efforts within DHS.

Included in the request is $95 million for Information Technology Services, a portion of which will provide funding for the Department-wide Geographic Information System (E–GIS) capability; to improve the Department's Enterprise Portal; this funding provides for continuation of the DHS Enterprise Architecture and planning; evolving the Financial Management System, eMERGE^2; and, development of the Human Resources information technology solution.

Additionally the request includes $31 million for Security activities, which will provide funding for continuation of the Homeland Security Information Technology and Evaluation program; and for continued support of terrorist information integration and sharing.

Finally, the FY 2005 request includes $100 million for Wireless Communications, which includes funding for enhancement of the Integrated Wireless Network (IWN) and Tech Ops Support. The Expanded IWN initiative expands to other DHS agencies the pre-existing Justice-Treasury IWN partnership established prior to the inception of the Department of Homeland Security (DHS), and which includes mobile radio (MR) and the application of emerging technologies as it pertains to domestic law enforcement and counter/anti-terrorist operations (including missions in the U.S. Territories), tactical communications, legacy systems support, and airborne and non-Coast Guard marine communications. It also continues the funding for the SAFECOM project.

Information Security

Since it's creation, the Department of Homeland Security has moved out aggressively to design and implement an Information Security Program that will not only ensure compliance with all appropriate statutes and regulations, but to also ensure that the entire Homeland Security community has a secure and trusted computing environment from which to operate. The heart of our reporting structure is built around the congressional requirements expressed in the Federal Information Security Management Act known as FISMA. In order to effect a comprehensive Information Security Program and in accordance with the provisions of FISMA, I have designated a Chief Information Security Officer (CISO) who manages and oversees all of the internal Homeland Security Department's Information Systems Security activities.

Due to the comprehensive nature of the FISMA reporting requirements, and to avoid duplication of effort, DHS uses the FISMA reports to satisfy the annual requirement to verify to the Secretary the status of the Information Security Program. Additional mechanisms, such as program briefings, status information and incident reports ensure continuous visibility to the Secretary throughout the year.

The FISMA report details compliance with Federal laws and policies and DHS information security policies and standards. DHS is in the process of implementing enterprise management tools to ensure the accuracy and completeness of FISMA reporting across the Department.

FISMA requires each agency to perform for each program and system "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices" annually. NIST SP 800–26, *Self-Assessment Guide for Information Technology Systems,* is the required self-assessment guide required by OMB policy. This, self-assessment guide utilizes an extensive questionnaire (containing specific control objectives and suggested techniques which the security of programs and systems can be measured. OMB's FISMA implementing guidance also requires agencies to maintain a Plan of Action and Milestones process that captures and tracks security weaknesses, and associated corrective milestones.

I have selected a Commercial off the Shelf Product called "Trusted Agent FISMA". This is an automated enterprise based management tool that maintains FISMA reporting data from all our components and their POA&M's that will capture and track security weaknesses and associated corrective milestones; in addition it will collect, process and store self-assessment information in accordance with NIST SP 800–26. We have deployed this system throughout DHS and have generated our first quarterly report. We expect this to improve the timeliness and accuracy of our reporting as this information is available *real-time* to the Secretary and other cognizant officials.

With this tool we will be able to focus our compliance and as well as leverage the effort of the DHS Inspector General to corroborate the accuracy of the FISMA information and improve the compliance stature of the department.

I thank you again for the opportunity to testify before you today and I am pleased to answer any questions you may have.

Mr. THORNBERRY. Thank you.

I will yield my time to the chairman of the full committee, Chairman Cox.

Mr. COX. Thank you, Mr. Chairman. I take it that you mean you are simply postponing your own opportunity?

Mr. THORNBERRY. There may be another chance.

Mr. COX. I hope you do not yield your time entirely.

I want to join in welcoming our witnesses, and thank you very much for your leadership in the Department, for being up here today, and for keeping us apprised of what you are doing. As you know, we are keenly interested, in fact most members of the subcommittee have been keenly interested in cyber as a priority since we were developing the Homeland Security Act in Congress. And we want to make sure that it gets all the attention that it deserves, and I know that you are doing that.

Let me begin by asking just what I hope is a trivial question. I am just trying to do the math in the testimony: That the $79 million dollar request for cyber; of that, 75 percent is going to the program, 59.3. Then there was another 8.7 that goes to outreach and public awareness, and 7 million that goes to vulnerability assessments and reduction. That leaves, by my math, 4 million unaccounted for, and I just wondered where it went.

Mr. LISCOUSKI. Sir, if you would permit me to get back in writing on that so I can do the math myself, I am sure we can provide to you the balance of where that $4 million is.

Mr. COX. It may be undistributed overhead. I don't know.

Mr. LISCOUSKI. I could look through this, but I would prefer to get back to you in writing, if I may, sir.

Mr. COX. Okay. Given the important role, as you outlined, Mr. Liscouski, in your testimony for the Computer Emergency Readiness Team, the CERT, the component of your efforts, how should we assess the other watch centers within DHS? There are several of them. If we are interested in consistency and overall cyber spec reporting, shouldn't we be concerned? Or should we welcome the fact that we have, for example, the IP National Communications System operating a 24/7 telecommunications watch center; we have also within IP Cybersecurity Division operating a 24 by 7 cyber watch center; we also have within IP the Infrastructure Coordination Division operating a 24/7 watch for physical and cyber reporting. We have within IA a 24/7 Homeland Security Op Center with a dedicated cyber watch desk. We have Mr. Cooper, in your shop, a Cybersecurity Incident Response Center. And, we have at Secret Service a 24/7 watch operation for electronic crimes.

Mr. LISCOUSKI. Sir, and thank you for the question. Let me get some clarity to the operations overall in terms of how the integration of the watch centers is being performed.

The legacy organizations that came in to us from Secret Service, from NCS that—and the Fed CIRC, that represent some of the watch centers you just articulated. With respect to the Fed CIRC, the NCC, the ones we have created with the HSOC, I will just quickly try to outline what those capabilities and mission requirements are and tell you how they are integrating.

The HSOC, the Homeland Security Operations Center is a 24 by 7 watch center that on behalf of DHS or at large it provides situational awareness across all of our enterprise, across the entire United States, integrates information to ensure that we understand from all hazards what is going on at any given point in time. Information piped into that HSOC is analyzed, understood in the context of is it threat information, is it incident data? And then we share with the respective elements of DHS to ensure that the appropriate actions are followed upon.

In the context of other situational awareness types of watch centers, the ICD, the Infrastructure Coordination Division, is ultimately responsible for the coordination of activities as it relates to infrastructure protection and monitoring what is going on across all of our infrastructure components irrespective of incidents.

The distinction there is ICD is going to be creating—I will add one more acronym to you— the NICC, the National Infrastructure Coordination Center, which is going to be the amalgamation of all these watch centers. This is just an evolutionary process to the comment of not breaking it as we are building it. We do not want to denigrate the capability we have with existing watch centers as we are building the one amalgam capability that is going to respond to our situational requirements, very large infrastructure protection, which will mean the incorporation of the NCSD's watch center, the NCC, the National Communication Coordination Center, and other elements for infrastructure coordination, all under the ICD.

The interconnectedness between the Homeland Security Operation Center and the NICC is paramount for us. We are looking to augment the capabilities of the HSOC. We have NCSD and as well as other infrastructure protection components on the HSOC which are responsible for doing incident management real-time.

The reach-back capability to determine what the impact of an incident may be is going to be through the Infrastructure Coordination Division and, through that center, the NICC. And it is really reflective of the complex nature of all of our infrastructure components. Instead of creating one gigantic coordination center, we are really looking to leverage the capabilities that we have established through DHS to ensure that we have got the right expertise coming to the table at the right times to provide the answers as necessary.

So it is not a redundant capability, sir, it is clearly an augmentation of the capability, depending on what function they are serving at a given point in time.

Mr. COX. But I heard in what you said that you also are anticipating further consolidation.

Mr. LISCOUSKI. That is correct, sir. We are consolidating the watch centers, the national, the NCS, the National Communications System. The NCD's watch center will be incorporated into the NICC. That is correct.

Mr. COX. How is my time, Mr. Chairman?

Mr. THORNBERRY. The gentleman's time has expired.

Mr. COX. All right. I thank the CHAIRMAN.

Mr. THORNBERRY. Although the Chair is trying to be lenient.

The gentlelady from California.

Ms. LOFGREN. Thank you, Mr. Chairman.

I have had a chance to—although I didn't have a chance to read your testimony, Mr. Cooper, I did have a chance to review your comments to the House Government Reform Committee in October of last year. And in that testimony, you had given your first draft of the Department Enterprise Architecture Plan, and you provided what I think you called a Quick Hit Project that you thought could be accomplished within 6 months. And some of those quick hits were integrating watch lists, network integration, developing external information sharing strategy, completing a feasibility study on integrating Immigration and Customs case management systems, and a number of others.

Now, we don't have teams of people auditing your department, but I don't believe we yet have a unified watch list data base. And the Inspector General has told us that the lack of an agreed-upon IT infrastructure prevents the Office of Information Analysis Risk Assessment Division from communicating with State, local, and private sector partners, and that inhibits the exchange of information. And the IG also says that there is concern that the IAIP lacks connectivity to access sensitive data bases maintained in other Federal agencies, which hampered their efforts to conduct business. And, you know, you can't always believe what you read in the press, but Information Week has reported that your office has had problems handing over and receiving secured e-mail.

Can you provide us with an update and where we are on all the quick hits that you were going to get done by now?

Mr. COOPER. I can give you an initial update, and I would like to also provide information in writing on all of the quick hits represented in the first release of enterprise architecture. But let me address a couple that I think are very, very relevant to the points that you made.

With regard to an integrated watch list and with regard to information sharing, the Secretary and the Deputy Secretary have already initiated an information sharing program that is now under way within the Department. The business owner is General Frank Liboutti, who is our Under Secretary for Information Analysis and Infrastructure Protection. Under his guidance, he has named a program director, and a team has been established that has already begun work in addressing how we will move forward to better improve our connectivity and our ability to put in place a two-way exchange of information with all of our stakeholders, both internal and external.

Ms. LOFGREN. Can I interrupt to try to understand?

Mr. COOPER. Yes, ma'am.

Ms. LOFGREN. So this information sharing effort is only within the Department? Does it include the FBI and those agencies that are outside the Department?

Mr. COOPER. Yes, ma'am. It will address the full national scope.

Ms. LOFGREN. It will but it does not currently?

Mr. COOPER. It does not currently. We are in the early stages of formation, and the team exists and is now working through the various requirements for the different communities with which we must interact.

Ms. LOFGREN. When do you think that will be done?

Mr. COOPER. Our expectation is to hit the deadline set for us by Under Secretary Liboutti, and that means that we will have a significant amount of this in place operational and done by the end of this calendar year.

I also want to highlight that in the quick hits we have in place and operational what we are now calling our Homeland Security Information Network. We built off a program called JRIES, Joint Regional Information Exchange System, that is operational. It is in place. And we are rapidly expanding membership in that system and as part of our Homeland Security Information Network. In the next several months, we will expand from the current about 50 participating State, local, and Federal partners who are already connected to probably about five times that number in the next several months. And, again, I will be more than happy to provide detailed program plans related to information sharing and building upon what is already operational.

Ms. LOFGREN. I see that I am just about to run out of time. But I would like to get, I am sure every member of the committee would want, a report on each one of the quick hits and the current status. Before—I guess my time has completely expired, so I will yield back to the chairman. I expect we will have a second round.

Mr. THORNBERRY. I thank the gentlelady.

The gentleman from Nevada.

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

Gentlemen, welcome to the committee. We are happy to have you. Your information has been extremely helpful to us.

Cybersecurity is not new. It is something that not only your agency but other Federal agencies have been working on for decades in some cases. If you could help us better understand how agencies like the NSA, National Security Agency, NGA, National Geospatial Intelligence Agency, the CIA, the DOD, all of those other agencies' efforts have been or have not been, I don't know what the answer will be, integrated into your effort in cybersecurity. How do you leverage their experience, their efforts, their work product over these many years to help you?

Mr. LISCOUSKI. Thank you, sir. And there is a couple of different perspectives on the roles and responsibilities within those agencies and how they would integrate and how we partner up.

DHS has got a protective mission and the protective mission we have in terms of looking at how we should best protect our critical infrastructure, the partnerships that we have got there clearly within the Intelligence Community and the NSA and the DOD specifically are we actively leveraging those. We have got a very strong partnership with NSA across a number of fronts. Up until just recently, until a recent transfer, the Deputy Director of the NCSD was in fact an NSA detailee, and it provided tremendous opportunity for us to leverage the experience that they have over the years of being able to gain an understanding of how to best protect those systems, and we are actively looking or looking forward to his replacement to come on board very shortly. Similarly, within DOD, who also has a protective mission for their dot-mil domain, we partner up with the Joint Task Force For Computer Network Operations. We have a very robust exchange of information between our US–CERT and their operations center. We have got very good personal relations as well as operational relationships with that agency.

On the offensive side, clearly within the domain of that realm, I speak at a very high level here, we are able to partner up with CIA and other Intel Community efforts to understand how they best look at their offensive mission to understand how we best need to look at our defensive mission based upon what the capabilities are out there.

On the intel side, in terms of the threat assessments, as you may know, through our Information Analysis Office we use them as the portal back into the Intelligence Community. We regularly drive requirements into the Intel Community to better understand how we can best protect our networks and our Nation's infrastructure from cyber threats.

So it is really a multifaceted approach. I would say it is highly integrative from the standpoint of either through people, exchange of people, or through active exchange of information.

Mr. GIBBONS. Very quickly, who establishes the standards by which you integrate and take advantage of all of these multiple operations? Is there a common standard which is being established, and are you part of that? Do you control it, or is some other agency in control of the standard and definitions about how this cybersecurity program that you just described takes place?

Mr. LISCOUSKI. Well, we have got the benefit of the Homeland Security Presidential Directive 7, which was signed by President Bush on December 17th of 2003, which provides us the framework for integration of all of the—real large for infrastructure protection, not just for cyber, to ensure that we have appropriate roles and responsibilities laid out for that protection. We are actively engaged in framing out not just the strategy but the implementation of that strategy. It is a work in progress as we develop the plan we are implementing. But we are able to negotiate with respective sister agencies in the Federal Government as well as State and local and the private sector to understand how we have to, again from the total infrastructure protection picture, flesh out the responsibilities. Who is going to do what? What programs are necessary to be done? Where the gaps are? And, most importantly, from the perspective of outcomes, how do we measure the outcomes to ensure that we have effectiveness? That falls under the auspices of HSPD–7. I have direct responsibility for that. I have got a program office in my office to do this, and we are actively engaged in fleshing it out.

Mr. GIBBONS. One final quick question. What degree does the DHS enterprise architecture plan to marry up with the Federal enterprise architectural efforts as well?

Mr. LISCOUSKI. I will defer to Mr. Cooper for that. But I will just, as a segue into that, is we are wholly dependent on Mr. Cooper's efforts to provide us the backbone enterprise architecture for our operations.

Mr. COOPER. It is aligned. Even before the Department was formed, we actually began working with the Federal enterprise architecture framework to both work with Dr. Haycock, who was guiding the charge under Norman Ranscript of the Office of Management Budget, and we have continued that relationship since. So it is very much alive.

And in those business areas that are critical to Homeland Security, we become, if you will, the lead agency. So as the work we do to populate the business processes, the informational requirements and then supporting technology, that flows into the Federal enterprise architecture.

Mr. GIBBONS. Thank you, Mr. Chairman. My time has expired.

Mr. THORNBERRY. I thank the gentleman.

The gentlelady from the Virgin Islands.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman, and I would like to welcome our two witnesses, also.

Mr. Cooper, do you feel that your office has the sufficient authority to drive IT integration within the Department of Homeland Security, even though you don't have direct line authority over divisional chief information officers? And, if not, is there anything that we can do to strengthen that position, the position you hold within the Department of Homeland Security?

Mr. COOPER. What I have done is to have created a Department of Homeland Security CIO Council, which is comprised of all of the named or titled CIOs who came into the Department with their respective agencies that now comprise the full Department. Additionally, I have asked the Chief Financial Officer and the Chief Procurement Officer to participate with us as full members of that council. Together, we have been participating in the investment review process of the Department. That is under the guidance of the Under Secretary for Management and Under Deputy Secretary Loy. I believe that in concert we have been appropriately bringing forward the proper recommendations, the proper decision-making framework so that we can make adjustments, if necessary, in some of the alignment that we inherited with regard to legacy applications and/or infrastructure investment. We will continue to learn, we will continue to grow, we will continue to refine these processes as rapidly as we can.

Mrs. CHRISTENSEN. And to what extent also does your office interact with other Federal agencies outside of DHS?

Mr. COOPER. I personally participate in the Federal CIO Council. So there are regular meetings. I am also a member of the Executive Committee of the Federal CIO Council. We draw upon the Federal CIO Council for a lot of that interaction. Additionally, our Chief Technology Officer and our Deputy Chief Information Officer are also members of that committee. So the three of us participate very actively.

Mrs. CHRISTENSEN. Do you provide standards for the other agencies that are outside?

Mr. COOPER. My office actually does not provide standards for other Federal agencies. But let me give you a real example of how it works. We, like other Federal Cabinet agencies, receive the direction and guidance that are set by Mr. Liscouski's area of responsibility, and we then apply, as all Federal CIOs would do, we apply that guidance and those standards, those accompanying standards within the Department of Homeland Security.

Mrs. CHRISTENSEN. Assistant Secretary Liscouski, last week we had a briefing from two of the private infrastructure organizations, the financial and telecommunications sectors. Could you tell us how your office interacts with the private sector? And early on, in the early days of the Department there seemed to be not an easy relationship, or there were problems that needed to be resolved. Could you talk about the relationship within your office and those private sector agencies?

Mr. LISCOUSKI. Yes, ma'am. We have a very aggressive outreach program with the private sector, and you are accurately portraying the relationships in the beginning. The legacy relationships that we inherited from the PDD–63 effort that ultimately authorized the establishment of the ISACs, the Information Sharing Analysis Centers, didn't allow for sufficient leadership and engagement at the private sector level to allow them to mature to a level of capability that would ensure that we had robust information sharing going both horizontally across information or industries as well as vertically back up to the government.

The first couple of months we were engaged with the private sector, we actively looked at that model to see how we could best leverage it, and the first part of that was to determine the validity or the value of those information sharing analysis centers. And I can tell you from my private sector experience, I looked hard at the efficacy of that effort.

To be candid with you, when I looked real hard at it. I saw there was a lot of opportunity there that we could leverage very well into a success story by enabling and empowering the private sector through the ISACs to develop their horizontal relationships, how they integrate and how they collaborate information. And that was the road that we embarked upon to ensure that we could establish that.

We have got a very good story to tell. I hope you heard that last week between the FS ISAC specifically.

Mrs. CHRISTENSEN. What exactly is your current relationship with the ISAC Council?

Mr. LISCOUSKI. Well, we have got an excellent relationship with the ISAC Council. They have stepped up to the leadership plate and they have provided what has been necessary and has been previously missing with the private sector, and that is the private sector leadership going back down into the private sector. They are actively engaged with my office both through the Infrastructure Coordination Division, which is responsible for managing ISACs and funding ISACs, as well as directly through my office I actively engage with them minimally once a month on a council level and much more frequently on an individual level. So I think we have got a very robust and a very successful story to tell as it relates to our private sector partnership there.

Mrs. CHRISTENSEN. Thank you. I think my time is up.

Mr. THORNBERRY. I thank the gentlelady.

The gentlelady from Washington, the Vice Chair of the committee.

Ms. DUNN. Thank you very much, Mr. Chairman, and welcome, gentlemen. It is very interesting as we begin to tie some of these responsibilities together to get a clear view from your point of view on how things are working.

Secretary Liscouski, in your written testimony and in your testimony before our panel today, you identified a couple of major steps in your management methodology that were interesting to me. One was the identification of critical infrastructure. Another was the assessment of vulnerabilities. I am especially interested in knowing how you work together with local government bodies and State government bodies and the private sector, what kind of input they have into these assessments, and whether they have a direct pipeline to you to know what you decided on.

Mr. LISCOUSKI. Yes, ma'am. Thank you, and I appreciate the question.

As I pointed out, our partnership with the private. sector—and coming from the private sector, my bias is that we have to work closely with the industry to determine what they believe their priorities are, and we have to normalize those priorities with what we believe are our national level priorities.

We accept ready input from both the private sector, the associations and, importantly, the State and local and tribal governments to ensure that we have got their perspective on what has to be protected and how it can best be protected. We develop common vulnerabilities assessments, common best practice methodologies, which are vetted through our State and local and tribal contacts as well as the private sector to ensure that we have got, in terms of our achieving infrastructure protection at large, consistent, effective, sustainable, and measurable capabilities and results across all of our critical infrastructures.

Now, as a general statement, I will tell you that we are succeeding in that very well. The methodology that we have outlined is that, at a national level, is scalable right down to an individual company level. It is the type of methodology which is being adapted to ensure that we help the industry at the single entity level as well as those that are highly interconnected to ensure that we can identify those vulnerabilities, the assets that need to be protected, the vulnerabilities, and the appropriate levels of programs.

The reason integration is so important to us, not just within the Infrastructure Protection Office as it relates cyber and physical, but clearly as it relates to State and local involvement, is because these efforts cannot be done unilaterally. The private sector cannot afford to protect itself nor does it have the wherewithal to protect itself that the State and local governments do in their law enforcement and protective authorities. So all the programs that we have developed and designed have been in collaboration and coordination with all those stakeholders to ensure that we have both a rational approach and an effective approach, and one which is dynamic enough to be molded against the current threat at any given point in time.

As you know, it is a very dynamic threat environment, so it is a work in progress. Clearly, the engagement we have with the private sector, we are constantly being fed with new technologies and new ideas on how to best implement programs that can be effective. At the end of the day, it is the private sector who is responsible for ensuring that they are doing what they need to be doing to protect that critical infrastructure. So we have a significant effort there.

Ms. DUNN. The State and local governments are satisfied with the relationship they have with you?

Mr. LISCOUSKI. At a general level, I would say they are, but as everything, I think there are different opinions.

We have clearly a lot of room for improvement across the board. We are not satisfied with where we are today. We are in the very early stages of building this program. It is a long-term approach, but I think we are satisfied with the approach we are taking.

Over the recent holiday threat period, we were actively engaged, and I am sorry to see Mr. Gibbons go because I had the opportunity to be out with Mr. Gibbons in Las Vegas during that period of time in which we had very robust meetings with the private sector, State and local governments. To be candid with you, I wasn't quite sure what kind of reception we were going to get, but we worked through many very difficult issues and came up with some very successful solutions to a response of that holiday threat period; and I think it is representative of the types of efforts we have out there that do tell a good story.

Ms. DUNN. That is good.

I think it is very useful that both of you have been in and out of the private sector, so you understand the value of what they can contribute and the kinds of communications that they need in order to be part of this whole thing. I think it makes us all stronger.

Let me ask you, Mr. Cooper, one question. The enterprise architecture team that you have started is going to come up with a plan to connect networks within the Department of Homeland Security.

At the same time, you have new programs being started up, like U.S. VISIT. Do you believe that you are in contact with them to the extent that you know what sort of information-sharing requirements they have and is it working well together?

Mr. COOPER. Yes, ma'am. I am actually a member of the executive advisory committee of U.S. VISIT in that specific example and also participate in the advisory committees of all of our major programs. We are deliberately looking for major programs to leverage whatever capability is being established. For example, within U.S. VISIT, as we roll out new biometric capability at the borders and ports of entry, that requires some new underlying infrastructure. We are actually leveraging that new investment as part of the U.S. VISIT program to ensure that infrastructure enhancements that we are making become the foundation of the direction that our infrastructure requires and—as represented in our enterprise infrastructure architecture.

We are doing the same thing with Customs and Border Protection's ACE program. We are leveraging the legacy Immigration and Naturalization Service's Atlas program for which there is appropriated funding to better establish infrastructure, and we are working to coordinate all of those investments within our enterprise architecture activities.

Ms. DUNN. Are you going to be able to get the FBI and CIA to come together so the U.S. VISIT can use their information in a way that is consistent?

Mr. COOPER. I am confident we will do that. I am afraid where we might have a difference of opinion is the timing that it might take.

Mr. THORNBERRY. So the question is, are any of us going to be alive when it happens?

Gentleman from North Carolina.

Mr. ETHERIDGE. Thank you, Mr. Chairman, and let me thank you gentlemen for being here this morning.

Mr. Cooper, I know—I think a question has been asked in one way on the testimony previously before the Government Reform Committee, and let me go back to that and ask my question a little different way, to some extent on the same subject as it relates to the 18 projects. Let me talk about two of them and one very specifically, I think, because right now, as you are trying to pull these together, and I guess I am very interested in particular—first, as you talk about the State and local industry needs survey, what do you hope to gain and what is its status is what I would like to know.

And let me go to another one that is very specific that I know my office and, I assume, many offices have problems with. This is an ongoing problem of getting information out of the Citizens Immigration Services, or CIS, because for my constituents they are constantly blaming the computer system. We call them, and they keep saying it is the computer system's problem. Well, garbage in, garbage out. You know what I am talking about in computer language.

And I am very interested in hearing about the feasibility study on integrating immigrations and Customs case management systems. Specifically, don't we need to fix the immigration computer problems first before we integrate those with Customs? Because if we don't get them fixed and integrate them, we are compounding the problem. I hope you will help me understand that so I can share that back with my staff who are quite upset about it.

Mr. COOPER. I understand. Let me take them in reverse order of your question. Let me go ahead and address citizenship and immigration services.

First, I do agree and the approach we are taking is exactly as you described. We have done a couple of things very actively. First we have—.

Mr. ETHERIDGE. Can you give me a time line as to when we will have it fixed?

Mr. COOPER. I will give you our current working targets of timing. The first thing that I had done is I have worked directly with Director Aguirre and his staff. We have named a CIO in Citizenship and Immigration Services. That individual is already on board and working directly with his staff and directly with the program folks to first, as you properly point out, to fix the problems with both the process as well as the underlying information technology that supports those processes.

They will address, first, developing and reengineering any of the processes that they find to be inefficient or lend themselves to optimization. Only until that work is done will we then move forward to integrate with other component parts of the organization.

So we are following your advice. We are fixing the problems first, streamlining process, understanding requirements, understanding the information necessary to support those processes; then automating within CIS, then integrating. And there is opportunity to integrate in that case management arena.

We have also ongoing an integrated consolidated case management effort that is at the very beginning so that the CIS folks, who are developing the work that I am just describing to you, are also part of a larger interdepartmental working group. And then, in turn, we also have reached out to other Federal agencies, like the Department of Justice or the Department of Energy, who have automated solutions in place to then evaluate, might there be an already existing solution that we could reuse that we could bring to bear? And the goal is to optimize, streamline and modernize, but don't necessarily build all this stuff from scratch because we are suddenly a new department.

Does that give some guidance.

Mr. ETHERIDGE. The time line?

Mr. COOPER. Here, again, we are moving forward. The time line to address the backlog is 6 months, the target that Director Aguirre has given us to direct the backlog and a lot of the cases kind of pending, from roughly this time period.

Another way of thinking about that is that our goal is to address this and have real solutions on the ground and to have cleared that backlog as fast as we can. But Director Aguirre's direction to me and to my team is help us do this by the end of the fiscal year.

Mr. ETHERIDGE. October 1?

Mr. COOPER. Six months, that is the target, this fiscal year.

Very quickly, in the State and local information sharing, that type of thing, as part of the program that I mentioned to you that

Under Secretary Libutti is guiding, as part of that, I actually have been working along with several of our other colleagues and leaders within the Department, particularly the office of State and local government.

We actually have been reaching out through the National Association of State CIOs and through a number of larger city CIOs, my office and me personally. We have been exchanging information. We have been working to better understand the requirements for information sharing from State and local and tribal government and from members of the first responder community. We are doing that not only through my office, but when we have something like Project Safecom which is also reaching out on the interoperability issue. That is how we are gathering requirements. We are then taking those and applying them and sharing them within the Department and working together within the Department and State and local partners to put solutions on the ground.

Mr. ETHERIDGE. I know my time is up. Is that sharing a two-way sharing?

Mr. COOPER. It is a two-way sharing. In fact, we require them to guide us. We can't see the requirements from the Federal environment. We are dependent upon them to provide local requirements.

Mr. ETHERIDGE. In a lot of cases, they are really our eyes and ears for those people who don't have the data.

Mr. THORNBERRY. I thank the gentleman for his good questions. The gentleman from New Jersey.

Mr. ANDREWS. Thank you, Mr. Chairman. I would like to thank our witnesses for their testimony this morning and for their service to our country. I know they do it at some considerable sacrifice.

The first thing I thought about last August when I heard about the blackout that was rolling across the northeast United States was whether it was an accident or whether it had been deliberately caused.

Let's assume—and happily all the evidence from that is that it was an accident. Let's assume that, this morning, a utility company in Wisconsin found evidence that someone was hacking into their system with an apparent attempt to bring down the system and bring down the grid. How would you find out about that?

Mr. LISCOUSKI. We learned a lot from the blackout, sir, and the processes we established with NCSD and through IP in general, particularly as it relates to situational awareness during that blackout period served us very well. For instance—.

Mr. ANDREWS. Not to interrupt, but if that happened this morning, who would tell you?

Mr. LISCOUSKI. What we learned in the blackout period was the processes we put in place at that time were exactly the same processes we would learn from an event similar to the hypothetical you just provided. We work with FERC, NERC in particular, which is the North American Electrical Reliability Council, which establishes the ISAC management point for our relationships with all the private sectors that relate to the electric utility companies. They have a very robust capability and the communications across the grid to pick up on incidents. Most likely, that would be the first indication for us reporting back from the private sector back into the ISAC, directly back into DHS about any activity like that.

Mr. ANDREWS. Would the utility company be required to tell you this, or just do it as a matter of good practice?

Mr. LISCOUSKI. There is a requirement—and I am getting a little bit out of my lane here as it relates to the regulatory requirements set forth by both the FERC and the NERC, FERC in particular; but I believe that there is a requirement to report those outages, but I can't specifically cite the authorization for that regulation.

Mr. ANDREWS. I know this is probably an unknowable answer, but give me your best guess.

How long would it take between the discovery of the intrusion by the utility company and report of the intrusion to responsible authorities within your division?

Mr. LISCOUSKI. There are a lot of dependencies on that chain—in the chain of that reporting. The first indication would be the robustness of that particular enterprise that might be under attack to detect an attack. In some cases, it might be a failure that might be the first indication of an attack. Where there is more robust capability, they are doing network monitoring and there are standards that have been supplied by NERC for implementation for cybersecurity, particularly resulting from the blackout example that would allow a utility company to be able to detect what is going on and therefore report it.

It depends upon the magnitude of the type of attack, their capability to detect that.

Mr. ANDREWS. I think I just heard you say that your ability to know would be very dependent upon the robustness of the detection system the utility company has in place. So if they had a weak system in terms of detection, you all might miss it all together?

Mr. LISCOUSKI. It really depends upon the type of attack. If it is a very specific attack against a specific company, a utility company or any other company that might be on the Internet, specifically targeting them, there are a couple of points we might be able to get information from, a, from the ISP which might be monitoring network activity that might see an increase of traffic to a specific IP address that might result in a denial of service for instance. The IP could report it to us, the target company could report it to us; it really depends upon the scenario. It is not easy to come up with a cut and dried answer to say, yes, it can happen, or no, it can't happen.

Mr. ANDREWS. Let us assume that the information was accurately reported and let us further assume that there were tools at your disposal that would stop the spread of the problem, that you could wall off other parts of networks and other parts of systems to protect other parts of the power grid. And let us assume that your best experts in your department said that is what you ought to do.

Do you have the authority to tell people to do that or not? Do you have the authority to tell the other people in the utility system that they have to follow those prescriptions or not?

Mr. LISCOUSKI. Taking the example, in partnership with the Department of Energy with whom we have—and the FERC with whom we have a strong relationship in the protection of critical infrastructure, by extension, I would say we have the authority to initiate that activity.

The actual execution of that authority would be with those respective regulatory agencies that have that specific legislative authority. But in terms of taking an action and prescribing a specific action, going back to the earlier conversation I had about the HSPD7, we are exactly in the middle of framing out those roles and responsibilities and how we would broker those relationships.

Mr. ANDREWS. What I think I just heard you say was that if you detected the attack and if you had a clear recommendation as to what to do about it from your experts that you would have to have some cooperation from the Department of Energy to execute the solution, right?

Mr. LISCOUSKI. I think it is more appropriate at the FERC level.

Mr. ANDREWS. You would have to have some cooperation from FERC and there are other regulatory bodies that might have some flow in this, too. The Nuclear Regulatory Commission might have a hand in it?

Mr. LISCOUSKI. They might.

Mr. ANDREWS. I raise these questions not just to paint an interesting hypothetical, but I think we have a lot of technological issues, and we have a lot of very smart technological people to address them; but I think fundamentally we have a management problem, an analytical problem. And the analytical problem is, who is in charge when we have a crisis?

I don't pretend to have an answer, and I don't advocate the answer that government be in charge of private enterprises in these circumstances. I don't want to see that. But we need to think through, "we," the committee, the administration, everyone, these protocols, because we don't have a lot of time to make these decisions. And even if we have honed the technology to the point where we know what is going on, and we have some good ideas what to do about it, we have created confusion or dysfunction—you haven't—as to who is in charge of what.

Mr. LISCOUSKI. I don't think that is the appropriate characterization. I think we have good leadership. I think DHS, the brilliant part about the creation of this department is it does pin leadership responsibilities on the Secretary in working through the relationships we have with sector-specific agencies. It may not appear to be a direct line of authority, but there is a clear line of communication that—we got activity going, and we have plenty of examples over the recent threat periods of how we have exercised that authority in cooperation.

Mr. ANDREWS. Can the Secretary order utility companies to do what your folks would say they should do?

Mr. LISCOUSKI. I feel pretty confident we can exercise the necessary actions we would need to get to get the appropriate action at that level. We have a cyber IIMG, Interagency Incident Management Group, that was stood up subsequent to the live wire exercise that took place this past fall in which the lesson there was that we need a cyber response. We quickly created that capability.

I am confident, sir, that we have the leadership that we need. Do we need to refine that and figure out how we do it better? Absolutely.

Mr. ANDREWS. I realize my time is up. I am not in any way impugning the leadership capabilities of people in these jobs nor am I doubting our competence to do them. What I am wondering about is because of the relative infancy of this department whether a—knowing bureaucratic turf battles to be what they are, if we were find ourselves mired in a bureaucratic turf battle at a time that we had to make some very quick decisions, I think it behooves us to answer those questions in advance so people know clear lines of authority.

Mr. LISCOUSKI. We are actively engaged in looking at those lines of communication. I would be happy to come back and talk to you about that. I wouldn't want you to leave this committee room thinking that we haven't thought about that or we haven't taken activity on that.

Mr. ANDREWS. I certainly don't think. I think we collectively need to think more about it and establish clear lines of authority.

Mr. THORNBERRY. Gentleman from Rhode Island.

Mr. LANGEVIN. Thank you, Mr. Chairman.

And, gentlemen, thank you for being here. I would like to touch on a couple of areas that have already been touched on this morning, first, dealing with JRIES and the second dealing with outreach to private industry.

First of all, can you tell us about the relationship between JRIES and RISSNet? Those people who may not be familiar with it, that is the Regional Information Sharing Network used by law enforcement. It is a highly effective tool for intelligence sharing and obviously it is a proven entity.

It was my understanding that JRIES was supposed to partner with RISSNet, but evidently that has not happened. And, in fact, from what I understand, RISSNet has been sidelined by DHS. So I would like to ask why it seems that you are pushing aside a proven system for a brand new one.

Second question for Secretary Liscouski: Last week I had a meeting with the IAIP directorate's enterprise architect Jonathan Houk and a company from my district, Ibis Consulting, to discuss how DHS is tapping the vast amount of expertise residing in the private sector. And I was pleased to hear that he is trying to leverage industry resources as much as possible in setting up IAIP's enterprise architecture, which is still obviously in the planning stages.

But aside from Mr. Houk's efforts, I would like to hear more on how effective DHS has been in forging industry partnerships. And I would like to hear more from you and Mr. Cooper about DHS's policies and guidance concerning industry outreach, if you would take the RISSNet question first.

Mr. COOPER. Let me address that for you, sir.

You are correct in that there was a period of time where the communication between the two programs was not occurring and was not anywhere near as effective as I think both groups and DHS want it to be. Much more recently, myself included, we have gotten that back on track and the RISS.Net team has met with the JRIES team and the program director to reengage and to actively build upon the work that RISS.Net has already done and to rapidly map into our homeland security information network, which is now what JRIES is evolving into as far as a label. It is a broader scoping. And that change in title properly reflects the broader scoping on behalf of DHS. So I do acknowledge that there was a temporary delay. We didn't have the effective communication. We believe very strongly that now has been corrected and I know that as of last week, there had been more recent meetings between the RISS.Net team and the JRIES team to move this forward.

Mr. LANGEVIN. I am encouraged to hear that.

Mr. LISCOUSKI. Sir, with respect to the private sector outreach program, we have it in many dimensions. Let me address the cyber one since that is the focus of this panel or meeting this morning.

Mr. Yannis has taken a very aggressive approach in establishing private sector partnerships. The first event that he participated in was the cyber summit back in December in which we were actually able to announce and get him engaged in the private sector outreach program. But subsequent to that, there have been a number of initiatives that he is engaged in. There is a US–CERT, private sector partnership program. They are on daily watch calls with the private sector either directly with private sector entities or through the ISACs. The task forces that have result from the cyber summit are also reporting back and are actively engaged with the NCSD in providing information and recommendations about how they can influence best practices throughout the industry.

Across infrastructure protection, we have traditionally have had—traditionally, in a year, if you can establish a tradition in the year, we have had active engagement with the NSTAC, the National Security Telecommunications Advisory Council, which is a presidential council established through the NCS; the NIAC, National Infrastructure Advisory Council, which was established through the legacy organization of the CAIO. Those are things we are actively engaged with.

The Homeland Security Advisory Council, which was established by the Secretary, has its own subcouncil, the Private Sector Advisory Council, with whom we are actively engaged. They represent, really, leadership of industries at the top level, at the CEO level, with whom we both exchange ideas and get influence from, again, the ISACs themselves across all the infrastructure components.

The private sector component is one in which I personally take an active leadership role, ensuring that we have got the right things going on there. We look for every form possible to ensure we get both feedback as well as getting our message out there. And importantly, when we get the feedback, it is, what do they believe they need to be doing to better protect our critical infrastructure; and we take that feedback into our thinking about how do we develop programs, realistic, going back to the consistent, effective, sustainable and measurable types of approaches we try to take.

I could, frankly, better take the remaining time here to talk about the different types of relationships and I would like to address something specific if you have it.

Mr. LANGEVIN. Can you talk about your interaction with small business? Very often they are the innovators and entrepreneurs that are out there at your basic level that have a product they believe can fill a niche. This is what happened with Ibis Consulting, and I put them in touch with the right people.

But how easy is it for small business to reach someone at DHS and get some type of an answer or an action?

Mr. LISCOUSKI. There are two parts to that question.

From a protection standpoint, we actively reach out to small businesses through our partnerships with our private sector outreach office, Mr. Al Martinez–Fonts, who you may know is a Special Assistant to the Secretary. His office is responsible for ensuring that we don't let any business fall through the cracks if they are not represented by a specific infrastructure sector themselves, so leveraging partnerships with U.S. Chamber of Commerce, for instance, or other industry groups to reach out to those small businesses to get the word about how to best protect themselves.

I was a small business owner and I am a staunch believer in what they add to the economy. That is the growth engine for the economy. We are very interested in protecting them. In terms of outreach and ways they can actually do business with us, I will defer to Steve, but the reality is we have a number of mechanisms by which companies can reach DHS.

Mr. COOPER. We have specific focus on small—and medium-sized businesses. My office works very closely with Kevin Boshears, who is the Director of our Office of Disadvantaged and Small Business Utilization; and we have actually, with his guidance, established some programs to flow and to make introduction connections with small businesses, in particular with my office.

I have named a Special Assistant For Industry Liaison, Tom Bold, and Tom has developed a program that then, in addition to Kevin's guidance to us, we have established a Web site that allows small businesses, medium-sized businesses—any business, but we are trying to focus on small and medium-sized businesses—to make their products and, services with specific areas they believe that they can help us address some of the business problems and challenges that we face, known to us.

We have—I personally, along with my team, have met with more than 3,000 businesses in the past year. We are trying to meet as many and talk with as many people as we can. We feel very, very strongly, and I have publicly spoken about the fact that we inside the Department don't have all of the technology-enabled answers. We are dependent upon a very cooperative, collaborative partnership with industry, particularly small—and medium-sized businesses where a lot of the innovation does occur.

Mr. LANGEVIN. I am encouraged by your answer.

Mr. THORNBERRY. I thank the gentleman.

Mr. Liscouski, let me try to see if I can ask a series of questions related to the national strategy to secure cyberspace, which the administration issued just before the Department really was up and running. But it still seems to me that to offer a good blueprint on the issues we need to be concerned about with regard to cybersecurity; and what I would like to do is go through some of the things they said we need to work on and have you just at least give us the name of a program or an effort. We can't get into the details of this stuff, or we will never get anywhere, but I am trying to get a feel, over the last year, how much progress have we made.

The first priority, as you know, is the National Cyberspace Security Response System. That is the first priority in the national strategy. And then they talk about public-private architecture for responding to national level cyber incidents. The first specific under that is analysis, tactical, strategic, and vulnerabilities.

Are we doing those things? Are we analyzing those cyber attacks?

Mr. LISCOUSKI. We are, sir.

Mr. THORNBERRY. Do you do that or does IA do that; or does the Cyber Division, which is under you, do that? It says "analysis," so how does that work?

Mr. LISCOUSKI. Let me take the first part of what we are doing, and I will tell you how we are doing it. There are a number of efforts that we have got under the priority one; the first—and no order of ranking here, just to give you the amalgamation.

There is the critical infrastructure—I am sorry, Computer Incident Interagency Management Group that I referred to earlier, first part of our response system. There are the alerts that we put out through the cyber alert system, as well as the efforts we are taking to build our national watch capability. We have got a—one effort dedicated to network flow analysis and situational awareness, and we have got our C1 project, which is our secure and survivable communications.

But who does the analysis that is aggregated among these types of efforts is a combination of—we work closely with our information analysis colleagues. The unique thing is, you know, about IAIP as we are joined at the hip. We both are resources for each other. In the context of threats, IA has the responsibility of providing us with threat information and that can then be mapped over to vulnerabilities. The technical expertise to understand how those threats can manifest themselves and those vulnerabilities, particularly in the cyber world, is found in the NCSD.

So analysis occurs across the soft center of IAIP if we look at where really the heart of what the IAIP organization is providing in terms of value to DHS.

I don't mean to be overly complicated about this, but there is analysis on both sides of that equation. So as it relates to priority 1, we have a very distinct role from the NCSD's perspective providing that response capability as well as an analytic capability.

Mr. THORNBERRY. Number two under that same priority is warning, and you just referred to some organization, but that is kind of an operational role; it seems to me that is a little different from infrastructure protection. I presume that is the same thing. Cyber Division is doing all of that analysis and the operational things and yet they are under infrastructure protection. I think that is kind of a unique situation for cyber, but also raises some questions.

Mr. LISCOUSKI. It is not unique for cyber. We are doing a similar way for telecommunications under the NCS. Similarly, within our protective security division, we are doing an analysis on threat information as it relates to mapping that threat information into vulnerabilities. As I point out, this is a very—you can't cut that Gordian knot. It is robustness of analysis going on both sides of the equation.

The one way that he might look at it is, threat information is sort of incident specific. Vulnerability analysis in terms of how vulnerabilities may be exploited might be end results specific. For instance, oftentimes we look at if we want to create—if a terrorist group is interested in creating a mass casualty type of event, they have a number of different ways they can use that: biological event, chemical event, bombing, using aircraft as missiles. We all know the results and we look at different ways we can affect that type of outcome.

The analysis that has to go on to exploit vulnerabilities in those particular modalities of attack are things that our organization is responsible for doing. The intent and who has got the capability of doing those things clearly resides on the side of the information and analysis.

Mr. THORNBERRY. Under, still, priority one, one of the things we need, the strategy says, is recovery mechanisms and continuity plans in Federal cyber systems. Are those under way?

Mr. LISCOUSKI. Yes, sir, they are. The partnerships we have in cross-infrastructure components, but cyber in particular, is intended to be able to recover from an attack as quickly as we possibly can, reconstitute ourselves. That is an integral part of our protection program.

One of the things a good recovery capability does is it devalues the target. One of the protection priorities we have is not just hardened targets, but to quickly recover from an attack should an attack occur. That effectively devalues the target if we can recover quickly.

Mr. THORNBERRY. I am not going to go through all of these items. I will skip ahead for a second to priority two, which is threat and vulnerability reduction.

Among some of the specific items listed there are securing the mechanisms of the Internet including key Internet protocols, Internet routing, and management of the Internet. How are we working with the private sector to do those things that were specifically set out in the strategy?

Mr. LISCOUSKI. We have a number of initiatives currently under way in which we are looking at both the vulnerability of the Internet as well as ways that we need to enhance the security of the Internet. One of those efforts, the GEWIS program, which was the Global Early Warning Information System, started out as an effort that the NCSD has enhanced significantly and gained ownership of, is looking broadly across the Internet at the network analysis activity that needs to be examined to ensure that we can see attacks coming over the horizon and take protective actions as necessary.

Mr. THORNBERRY. I think what we might like to do is submit some of these other types of questions for the record, going through the various elements of the strategy, again not looking for detail, because that is way too much, but I do think it is important for us and for all of those interested in this topic to have some idea that at least there are initiatives under way for the various areas, and some of them are not even in your bailiwick. But the initiatives that are under way, we need to know that they are under way.

I yield to the gentlelady.

Ms. LOFGREN. I realize we are out of time and we have a series of votes. I have a lot of questions which I will submit and look forward to the written response.

But I did want to make sure that I understood Mr. Cooper's answer to Mr. Etheridge, because I wrote it down and want to make sure I was not mistaken.

Did you say that by the end of this fiscal year we will meet the President's 6-month goal on processing immigration?

Mr. COOPER. I am indeed saying that we are going to do everything that we possibly can to meet that goal. That is our direction, that is where I am placing additional information technology resources to help do that.

Ms. LOFGREN. Thank you very much.

Mr. THORNBERRY. The chairman may have additional questions, particularly for Mr. Liscouski, who has another hearing. Maybe Mr. Cooper might be more flexible if we need to come back.

Mr. COX. We don't need to come back. I intend to go to the floor for the vote, but I would take a few minutes before we leave.

Mr. THORNBERRY. We have the gentleman from Florida here.

Mr. MEEK. I will yield to the chairman and I will submit my questions for the record.

Mr. COX. I appreciate your courtesy.

On the subject of our overall strategic objectives, I am impressed and pleased that the number one strategic objective is preventing cyber attacks against America's critical infrastructures. When I look at the priorities as they are laid out, I find that the first priority is the response system. The second priority is threat and vulnerability reduction, which has as its analog the second of the two, the second of the three overall objectives for DHS itself.

Likewise, priority 3 is awareness and training. That gets to protection. Priority 4 is securing government cyberspace. That, of course, is defensive. And within priority 5, as it is outlined, even though it is described as international cooperation, there is a bit about intelligence sharing and so on.

But, you know, the main purpose of the Department of Homeland Security is to deal with the problem of T and T, terrorists and technology, the weapons of mass destruction plus terrorists, the possibility that mayone day be upon us. That is the worst thing that could happen to the country and, therefore, the first thing that the Department of Homeland Security needs to concern itself with.

Such things as pulse weapons directed at our country, therefore, mark what ought to be the top priority in prevention there is clearly superior to dealing with it after it happens, just as with any other weapon of mass destruction. So I wonder if I could inquire first whether you have it in mind to place increasing emphasis on the prevention piece, because while it is occasionally mentioned, I see that we are focused, for understandable reasons, elsewhere because it is more tractable; and specifically whether it is possible to initiate more meaningful collaboration between the National Cyber Division and the Department of Defense.

Mr. LISCOUSKI. Yes, sir. From our perspective, these programs all roll up into a good preventive and protection approach. You can take apart elements and see that they contribute to protection. But every single one of these, from a response and recovery capability awareness, threat and vulnerability reduction, all really do constitute good protection programs. So I would, if I understand your question correctly, validate this approach in terms of what it accumulates—.

Mr. COX. What I am trying to do is distinguish protection from prevention. We have prevention, protection response. I see a lot of protection, a lot of response, and I need to understand more about what we are thinking about doing in the prevention area.

Mr. LISCOUSKI. In the context of prevention and again, I don't want to be definitionally based here, but as it relates prevention, typically the law enforcement component of interdicting, detecting and interdicting what is going on. Detection as it relates to prevention is clearly within the domain of what we do. The actual activity related to interdicting or reducing an adversary's ability to attack us is not something that my organization is charged with.

Mr. COX. On the other side of IAIP, in the other half of Frank Libutti's brain, we have the essence of the prevention piece of DHS, and it would seem to me that that would apply just as thoroughly to cyberspace as anything else.

Mr. LISCOUSKI. The full circle here—and again, this is trying to cut the Gordian knot, but we look at prevention in the context that you just provided it to occur at the target level. And the things that we can control in the world, that we do to protect—if I could take some time here for a moment—there are protective activities we engage in which increase awareness of group capabilities and tactics that could be affected against a specific target.

We go out and train the private sector on what to look for, the observables of preincident indication of activity of a terrorist attack. Those observables, while they may be disparate pieces of information not directly related to an imminent attack, but potentially future planning of an attack, are things we can pipe back into our IA folks to assist in the prevention role.

That is the value add that we have in the ability of providing information from the private sector that we directly gain on preincident information that we collect, that we share with our information analysis component that gets put back into the intelligence community to affect good prevention methodologies and good prevention activities. It is finding out—and the unique thing about this and the unique thing about what DHS does, particularly as it relates to IP, is that we deal in the target community; and as a result and as opposed to looking at just the criminal activity or the terrorist activity that goes into targeting the private sector, we are dealing with the targets that are the focus of those terrorist groups.

So if we know what to look for and we can train people in what the observables are, that observable information can significantly enhance prevention activities as it relates to law enforcement and the intelligence function.

As I pointed out earlier, it is a pretty complex process, but I think it is an extremely articulable one as it relates to what our role is and how we play together in this space. It happens in the cyber world routinely; as we found out, probing or potential exploit probes, things that can be detected in the cyber world contribute to that sort of knowledge as well. Terrorist groups, we know, use cyber activity to probe physical targets to see what the penetration capabilities are. That information gets collected similarly as observable—physical things that are observable get reported back to us.

I don't know if that responds to your question or not.

Mr. COX. It amply responds given the time that we have. I appreciate very much your willingness to speak to the point.

I thank the chairman. Please keep in mind my suggestion about deeper cooperation with DOD. I think that that could be helpful.

Mr. LISCOUSKI. I could respond to that, too.

We actively engage with DOD and we are looking at all levels between NORTHCOM as well as the Assistant Secretary of Defense Paul McHale. We have a good partnership there.

Mr. THORNBERRY. I thank the chairman.

I would like to ask both witnesses if we can have an agreement that because our time has been cut short, that you all will make an effort to respond to our written questions, try to within 2 weeks and less than 30 days, and I will commit to you to make sure that the questions are reasonable in length and scope. If we could have that agreement with both of you, I would appreciate it.

I am going to ask one other question at the risk of missing this first vote. You are free to go Mr. Liscouski, but I don't know if anybody is going to be over there anyway because we are all voting.

But, Mr. Cooper, I want to direct this to you because one of the primary reasons that the Department of Homeland Security was created was to integrate 22 different agencies into one seamless unit. Now, the total measurement of seamlessness is not having one IT architecture and system with which the Department can operate, but it is a pretty good one. And yet, when I look at some of the specifics that you have provided on the progress you have made, you have still got ten different financial management systems, you have still got eight different contracting offices, seven different human resources.

I guess it is an area where I am frustrated, frankly, and I want to ask, is the primary difficulty you face figuring out what you want to do? Is it resolving the technical difficulties of merging these 22 different agencies? Or is it something else? Is it money? Is it getting the decisions made to force people to go use somebody else's computer system even though that is not what they have been using?

If you had to summarize the difficulty you face in making this one seamless IT department, what is it?

Mr. COOPER. I would summarize it in this way: It is a combination of people, process and technology. The technology is in fact, honestly, from my professional and kind of sitting in the role that I currently sit in, is the least controversial and the easiest to effect.

However, having said that, it is—in and of itself, the technology challenges are complex. We know how to do them, so that is the easiest.

The second is process. What we don't want to do, if you pardon the expression, is pave the cowpath. We want to reengineer some of the processes that we now use or will use to effect threat identification and management or some of the cybersecurity activity that Bob has talked about or some of the back office processes that I spoke to briefly. That is hard work.

We do have—we are making progress. I mentioned the five business area focus groups. This is under way. We were a little bit slow to get going because we had to do some education. We had to help people understand why this is an important and valuable exercise.

We have had the support of the Secretary. We have had the support of the Deputy Secretary and now we are engaging. All areas of the Department are engaging. So that, I feel comfortable that we are under way.

Again, we will move as fast as we can move with quality and with speed. It may take us longer than all of us would hope that we could complete.

The last and the toughest is people. This is about change. And that means that in some cases, the right decision or what might come out of these business area focus groups might be suggestions or reengineering that says a process used to be done in many organizational elements and now it might be more appropriate to place it in one organizational element, name that organizational element, the managing partner or the business process owner to have reach and span of control across that process across the entire Department. That is change, it is difficult, and it is about thinking differently and about doing work differently.

I don't have exact answers. It is not quite a science yet. There is a little bit of art involved.

Mr. THORNBERRY. I appreciate your analogy of changing the tires as the car is moving, because while you are doing this stuff, you still have got to guard the borders and still have to process the people coming in. And I don't want to minimize that effort.

I will say this. I think a number of us will be looking for ways to help you, maybe even push you a little bit to make sure that this does move as fast as possible. And understanding culture and people and reluctance to change, we cannot let that obstruct the ability to have a department that is functioning as well as it possibly can, because so much is riding on the success of this department.

So I don't want to make your job more difficult, but on the other hand, separation of powers is here for a reason and maybe we can help give you some extra incentive or whatever to get the job done.

But I appreciate it. I appreciate both of you being here and your answers today, and I appreciate your willingness to answer our written questions promptly. And, with that, the hearing is adjourned.

[Whereupon, at 11:50 a.m., the subcommittee was adjourned.]

APPENDIX

Questions Submitted for the Record

Questions for Assistant Secretary Robert Liscouski, From Congressman Dave Camp

1. Your office has the responsibility to communicate cyber threat information to the private sector. I am interested in understanding the different means you use to accomplish this task. What challenges do you face in communicating with large companies (the Financial Services Sector, for example) versus small business owners and private users? What are the different means you utilize to reach these different groups, especially given their varying levels of understanding of cyber threats?

The primary ways that DHS communicates cyber threat information to the private sector are: (1) through the U.S. Computer Emergency Readiness Team (US–CERT) public website at *www.us-cert.gov,* (2) through the US–CERT's National Cyber Alert System (NCAS), (3) through the US–CERT Portal, and (4) through the Information Sharing and Analysis Centers (ISACs) in each of the critical infrastructure sectors.

The US–CERT public website is our primary means to provide information to the public at large. It includes relevant and current information on cyber security issues, current cyber activity, and vulnerability resources. To date, the website has received over 3.8 million hits at an average of 128,000 per day. It also provides a link to the National Cyber Alert System (NCAS).

NCAS is an operational system developed to deliver targeted, timely, and actionable information to Americans to allow them to secure their computer systems. Information provided by the NCAS is designed to be understandable to all computer users, technical and non-technical, and reflects the broad usage of the Internet in today's society. The NCAS provides a communication mechanism through website access and e-mail alerts for providing general guidance for users and the ability to reach millions of Americans at once with a variety of cyber security information materials on both a technical and non-technical level. There are currently over 270,000 unique subscribers to the various alerts provided by the NCAS, and our challenge is to increase its outreach to as many Americans as possible. We are working closely with the National Cyber Security Alliance on expanding the Stay Safe Online campaign, coordinating closely with the Federal Trade Commission on their information security campaign, and working with other trade groups and industry associations with key cyber security awareness and outreach programs.

In addition to the public website, US–CERT maintains an active secure online portal that enables the cyber security stakeholder communities including government and the private sector to communicate and collaborate on cyber security efforts. Groups that utilize the US–CERT portal include the Chief Information Security Forum (CISO Forum), the National Cyber Response Coordination Group (NCRCG), DHS's Office of Infrastructure Protection, the Government Forum for Incident Response Security Teams (GFIRST), the Multi-State Information Sharing and Analysis Center (MS–ISAC), and the US–CERT staff. One challenge to reaching the private sector communities has been creating a trusted protocol for sharing information. That challenge is being addressed in through the NCSD/US–CERT Outreach and Awareness efforts.

In the case of vendor-specific vulnerability or threat information, we communicate directly with appropriate and expert representatives in the individual company when that is possible. The recent Cisco vulnerability is a key example of how we communicated—and collaborated—with the private sector on a very specific vulnerability. The ability to communicate with specific companies in such cases is crucial. The appropriate contacts are being developed through the NCSD/US–CERT Outreach efforts and through participants in the US–CERT Portal. Outreach targets include the spectrum of the critical infrastructure sectors (through the ISACs, industry associations, etc.), software developers and researchers, academia, government, the information technology (IT) vendor and operator community, and others. DHS works with various vendors to understand, assess, and inventory vulnerabilities so that when threat information is transmitted, it includes specific instructions on how to mitigate or eliminate the vulnerability, and what resources exist to obtain help.

The ISACs were established as a primary mechanism for two way information sharing with the critical infrastructure sectors. Many critical infrastructure sectors have developed procedures to widely disseminate their alerts, warnings and advisories, to both large and small companies, throughout their sector. These sectors involve trade associations, representing smaller companies, who receive information from the ISAC and who then re-transmit that information to their members.

2. How do you utilize Information Sharing and Analysis Centers (ISACs) to share and receive threat information? How do you recommend strengthening or improving the relationship between ISACs and DHS for this purpose?

DHS/IAIP's Infrastructure Coordination Division within the Office of Infrastructure Protection maintains an on-going relationship with the ISACs and is the focal point for all ISAC relationships for critical infrastructure issues. Threat information gained from the Intelligence Community through DHS's Office of Information Analysis alerts, warnings, and advisories applicable to the critical infrastructures and key resource industries are delivered directly to them through standard agreed upon procedures. DHS/IAIP also provides to them regularly scheduled daily situational briefings, and periodic classified briefings as needed as well as special briefings when there is a major change in the threat level. IAIP also meets periodically with the ISAC Council a cross-sector body representing a large number of the ISACs, to improve information sharing practices and strategies. Such meetings help to sustain the relationship with the ISACs by proactively identifying gaps that need to be mutually addressed.

DHS is constantly strengthening its relationship with the ISACs. One of its most critical programs is the implementation of a National Infrastructure Coordination Center (NICC) to serve as an operational nexus for all of the ISACs. The NICC allows representatives from the ISACs, industry groups, and key companies within each sector to share and receive situational awareness information. These sector experts work both within their areas of expertise and across sectors to maintain constant situational awareness of the status of the critical infrastructure. The NICC provides a centralized mechanism for sharing information with the ISACs and the private sector in response to an event or crisis. The ISACs will also be expanded to ensure that one exists for each critical infrastructure sector and key segments within each sector. DHS continues to work with industry to evaluate ways to reach the full breadth of each critical infrastructure sector, either through improvements in the ISAC mechanism or additionally through sector coordinating groups.

In addition to these regular, ongoing efforts, the Homeland Security Information Network, once functional, will facilitate real-time communication between DHS and the private sector through the ISACs or other sector groups as they form. DHS is also working with the ISACs on a number of exercises, on a national, regional, and sector basis that will help determine where communication and collaboration improvements can be made.

Questions From Congressman Sherwood Boehlert

1. Mr. Liscouski, in a September 2003 letter to Governor George Pataki, you requested New York's initiative and leadership in the Multi-State Information Sharing and Analysis Center (MS–ISAC) and promised that DHS would assume a more 'formal' role in the MS–ISAC, once established. New York State and Mr. William Pelgrin, Director of Cyber Security and Critical Infrastructure Coordination for the state, have been proactive and effective in coordinating and leading the Multi-State Information Sharing and Analysis Center. Mr. Pelgrin's efforts have resulted in the MS–ISAC involving 49 states and the District of Columbia and a business plan, submitted to DHS, which highlights roles, responsibilities, budgets, and additional steps needed for the MS–ISAC. Now that it has been established, what funding and support do you plan to provide the MS–ISAC as you work to formalize the relationship between DHS and this critical initiative that you requested?

DHS recognizes and appreciates Mr. Pelgrin's efforts to develop and expand the Multi-State ISAC. As part of this effort, we had requested that he engage other like entities within the states, which had information sharing initiatives on-going, such as NASCIO, and integrate their efforts. That work is in progress. We are currently reviewing Mr. Pelgrin's business plan that was developed prior to the implementation of new capabilities within DHS, such as the National Cyber Security Division, the US–CERT, and the announcement of the Homeland Security Information Network (HSIN) by Secretary Ridge in March 2004. All of these new capabilities are intended to assist and enhance the core capabilities of the ISACs and bring them up to a common level of effectiveness. The Multi-State ISAC will receive the benefits of all these new capabilities including the ability to share information and collaborate on cyber security issues on a 24x7 basis and to further integrate information sharing within and across State and local governments through the HSIN/US–CERT portal.

The Multi-State ISAC and Will Pelgrin have been extremely supportive of the US–CERT and our initiatives to increase national cyber security situational awareness. The NCSD has participated on a number of Multi-State ISAC monthly conference calls throughout 2004 and plans to continue to support the mission of the Multi-State ISAC to provide valuable cyber security vulnerability and incident information to the State level. Moving forward, NCSD plans to work along with the Multi-State ISAC to mutually improve cyber security on both the state and federal level. As such, DHS has entered into a contract with the MS–ISAC to provide $400,000 in FY04 funds, which the MS–ISAC is currently using for various outreach efforts such as conference, the webcast series, and other activities. DHS is exploring an increase in the funding for the MS–ISAC in FY05.

FROM CONGRESSMAN MAC THORNBERRY AND CONGRESSWOMAN ZOE LOFGREN

1. Coordination for Threat Assessments

a. How is the National Cyber Security Division (NCSD) working with the Information Analysis Directorate (IA), which has responsibility for information analysis of the threat?

The Office of Information Analysis (IA) is DHS' portal to the Intelligence Community and is responsible within DHS for all aspects of the intelligence cycle for cybersecurity, such as issuing additional collection or analysis requirements to the rest of the Intelligence Community. NCSD works with IA on the substance of the collection and analysis requirements.

Operationally, the NCSD works with IA through daily threat assessment meetings and on an as-needed basis in the case of a specific threat. One example of this coordination was the participation of NCSD in partnership with IA to develop the National Intelligence Estimate (NIE) "Cyber Threat Against the Information Infrastructure." This classified document is an update of the 2000 NIE of the same title. In addition to the regular meetings NCSD participates in daily conference calls with the National Security Agency/NSIRC, the Central Intelligence Agency, and the Department of Defense's Joint Task Force Global Network Operations (JTF–GNO) to discuss classified cyber activity of note.

b. How does the NCSD interact with the Terrorism Threat Integration Center (TTIC) for classified assessments? How are these assessments used and what NCSD products have resulted from TTIC derived information?

NCSD interacts with the Terrorism Threat Integration Center (TTIC) indirectly through the DHS Homeland Security Operations Center (HSOC). NCSD shares the staffing of a 24x7 Infrastructure Protection desk at the HSOC that has direct reach back to the US–CERT, and the HSOC and TTIC work closely together on information for both physical and cyber threats. Additionally, NCSD interaction with the TTIC is accomplished through DHS/IA, law enforcement and intelligence community detailees on staff in IAIP and is developing a comprehensive threat, risk, attribution assessment, and response capability.

With regard to classified assessments, NCSD participated in National Intelligence Estimate's cyber threat assessment in conjunction with IA and other members of the law enforcement community.

To date there are no specific NCSD products that have been produced from TTIC-derived information.

c. Who within DHS has the authority and mission to correlate cyber threat and vulnerability for an overall assessment? When, how, and with whom will this information be shared?

As a focal point for cyber security issues related to reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks, DHS' National Cyber Security Division (NCSD) has the authority and mission to correlate cyber threat and vulnerability information. The NCSD performs this correlation within the Division in a collaborative effort between the US–CERT

Operations branch and the Law Enforcement/Intel branch as the lead entities but also in collaboration with other Divisions in the Office of Infrastructure Protection. In addition, as part of the National Infrastructure Protection Plan (NIPP), NCSD is responsible for: (1) conducting risk assessments and determining the necessary protective measures for the information technology industry, and (2) providing guidance to the sector specific agencies with responsibility for other critical infrastructure sectors on how to incorporate cyber-related vulnerabilities into their vulnerability assessments.

NCSD regularly shares information with key stakeholders within DHS, including the Homeland Security Operations Center (HSOC) through existing daily conference calls or targeted communications, IAIP, and other components as appropriate as well as with interagency partners through the NCRCG, GFIRST, and the Chief Information Security Officer (CISO) Forum. As information is cleared through classification procedures, NCSD also shares information with the private sector through appropriate channels, including the ISACs, the HSIN/US–CERT Portal , and the US–CERT NCAS. The public at large can also access information provided through the NCAS as well as the US–CERT public website. In the event that a cyber threat rises to the level of national security, the public will be informed through the Homeland Security Advisory System (HSAS).

2. Coordination for Cyber Advisories and Warnings

a. What organization within DHS is responsible for managing and issuing cyber advisories and warnings?

Through its mission to serve as a national focal point for cyber security issues and to implement the National Strategy to Secure Cyberspace, NCSD is responsible for managing and issuing cyber advisories and warnings. Those advisories and warnings are issued to the public and our partners through the NCAS and to specific entities on an as-needed basis in the case of a targeted vulnerability or threat. Information that is less sensitive and for wider distribution is disseminated through the US–CERT public website and the US–CERT secure online portal, as appropriate.

b. How will DHS integrate cyber advisories and warnings into the existing Homeland Security Advisory System (HSAS), given that cyber has a unique audience, particularly when those people who must respond to an attack are not the traditional First Responders used for physical national disasters?

NCSD provides information for use in the HSAS to be activated as appropriate. However, the nature of cyber attacks is that there are varying degrees of cyber activity at any given time that warrant advisory to the cyberspace stakeholder community that does not meet the criteria for raising the national alert status through the HSAS. Therefore, US–CERT utilizes the NCAS to notify the entire national, and international stakeholder community about activities that may warrant specific protective measures but that do not rise to the national security level of the HSAS. US–CERT is reaching out to key partners for incident response at various levels of sensitivity or urgency through the NCAS, the US–CERT secure online portal, the NCRCG, and the US–CERT public website to communicate with cyber “first responders” and other stakeholders.

In the event of a cyber incident of national significance (or an incident with both physical and cyber implications), the NCSD/US–CERT and/or NCRCG will provide analysis and recommendations to the IIMG or to the Secretary to help inform a decision about whether to raise the national alert level,

c. How is the cyber threat and warning mission being integrated into the Homeland Security Operations Center (HSOC)?

US–CERT communicates regularly with the HSOC on cyber security issues, including participation in daily conference calls and regular e-mail and other correspondence. In addition, the NCSD shares the staffing of a 24x7 Infrastructure Protection desk at the HSOC that has direct reach back to the US–CERT for coordinated action as appropriate.

d. How will DHS work with other countries when responding to a cyber attack, given that most attacks have effects on information systems around the world?

Cyberspace transcends traditional borders and we recognize our international outreach is crucial to protecting ourselves. As such, DHS is active in a number of multilateral and bilateral activities addressing cyber security issues such as early warning, response, and information sharing. NCSD and US–CERT are reaching out to other countries to form strategic partnerships that we will be able to leverage in the case of a cyber attack. US–CERT is a member of the Forum for Incident Response Security Teams (FIRST), an international coalition of government, commercial, and academic organizations that aims to foster cooperation and coordination in incident prevention, prompt rapid reaction to incidents, and promote information sharing among members and the community at large. FIRST is one way that US–CERT works with computer security incident response teams (CSIRTs) in other countries when needed to share information, best practices, and experiences. US–CERT also communicates and collaborates with other CSIRTs directly.

For example, NCSD and US–CERT participate in the cyber security efforts of the Asia Pacific Economic Cooperation (APEC), the Organization for American States (OAS), and the Organization for Economic Cooperation and Development (OECD). Their respective programs seek to raise awareness about cyber security, provide technical assistance and capacity building for emergency response teams, help develop trusted relationships between response teams, and to build a global "culture of security."

On an operational basis, the NCSD and US–CERT are developing closer ties with the so-called "Five-Eyes" countries (United States, United Kingdom, Canada, Australia, and New Zealand), as well as other countries with key operational capability and interest through information sharing and cooperative mechanisms. The objective is to forge trusted relationships with our counterpart organizations abroad and develop the basis for a coordinated response in a cyber incident or attack. We seek and have created opportunities to build those relationships in a number of international forums and activities. The most recent example was the multilateral conference on cyber security that DHS/NCSD co-hosted with the German Ministry of the Interior in Berlin in October 2004. Government policy makers, managers of CSIRTs with national responsibility, and law enforcement representatives from fifteen countries in Europe, Asia Pacific, and the Americas participated in the conference. The conference focused on developing a framework for cyber information sharing and incident response, and included a tabletop exercise to examine international communication and collaboration channels as well as interactive sessions on international information sharing and incident response. The participants agreed to an initial framework for cyber information sharing and incident response by identifying points of contact cyber information sharing actions in the short term and, and are forming a cooperative mechanism to build a more mature framework in the longer term.

3. Framework

a. Is DHS developing a cybersecurity framework for public and private use and what is the status?

The cyber security framework for the nation is the *National Strategy to Secure Cyberspace* issued by President Bush in February 2003. The Strategy put forth a framework of five priorities for all stakeholders in protecting our nation's information infrastructure and provided a roadmap for both the private and public sectors to undertake toward a more secure cyberspace. DHS is well on our way to implementing the Strategy with our counterpart agencies throughout the government and are actively partnering with the private sector to work collaboratively and create a set of public milestones to measure progress. We have consolidated and are leveraging existing programs and have identified new ones toward meeting the mandate of the Strategy.

b. What elements are being included in this framework? At a minimum, please include an update for benchmarks, standards, best practices, common criteria and other elements as appropriate.

The elements of the framework are set out in the Strategy's five priorities:

Priority I:A National Cyberspace Security Response System

Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program

Priority III: A National Cyberspace Security Awareness and Training Program

Priority IV: Securing Government's Cyberspace

Priority V:National Security and International Cyberspace Security Cooperation

Key elements of our program to meet the mandate of the Strategy are as follow:

US–CERT—established a 24x7 cyber watch and warning operation with a secure online portal for collaboration, information dissemination, and information exchange;

US–CERT Outreach—establishing regular communication and collaboration mechanisms such as US–CERT Portal, US–CERT public website, NCAS and other activities to reach critical infrastructure sectors, software developers, academia, government entities, and other stakeholders.

Strategic Initiatives—identification of cyber security programs for the long term, including software assurance, research and development, exercises, training, and education.

Law Enforcement and Intelligence Coordination—NCSD works with key parties in the law enforcement and intelligence communities to leverage information and coordinate response to cyber security threats and events.

NCSD has identified a set of goals, corresponding objectives, and programs and initiatives to further these goals that map to the five priorities of the National Strategy. NCSD is working to develop a set of specific milestones to measure progress toward the goals articulated in the following strategic framework:

PRIORITY	NCSD GOALS
I. National Cyberspace Security Response System	#1 Prevent, predict, detect, and respond to cyber incidents, and reconstitute rapidly after cyber incidents
II. National Cyberspace Threat and Vulnerability **Reduction Program**	#2 Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks #4 Coordinate with the Intelligence and law enforcement communities to identify and reduce threats to Cyberspace
III. National Cyberspace Security Awareness and Training Program	#3 Educate and encourage Americans to secure their cyberspace thought a National awareness and training campaign
IV. Securing Governments' Cyberspace	#1 Prevent, predict, detect, and respond to cyber incidents, and reconstitute rapidly after cyber incidents #2 Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks
V. International Cyberspace Security Cooperation	#1 Prevent, predict, detect, and respond to cyber incidents, and reconstitute rapidly after cyber incidents
Common to All Priorities	#5 Build an effective organization

NCSD has various opportunities and obligations to report to Congress on its programs and activities and will continue to do so as requested and on a timely basis.

c. How will progress and compliance with voluntary standards and the framework be measured and certified, particularly in the private sector, which owns and operates most of the critical information infrastructure?

The private sector has a large role in increasing our nation's cyber security, and they are acting upon that responsibility. Private sector associations formed the National Cyber Security Partnership (NCSP) and are expanding it to include over 20 associations. NCSD is participating in meetings of the NCSP and others to encourage the articulation of a set of priority milestones for implementation of the priorities of the National Strategy that can track progress by the private sector and government.

d. What incentives will be provided, or are needed, in order to have government and industry adopt this cybersecurity framework?

Much of the Strategy calls for information sharing between the private and public sectors. Historically, companies and other entities have had concerns about the confidentiality of information shared with the federal government, either independently or through a mechanism such as the ISACs. Congress enacted the Critical Infrastructure Information Protection Act as part of the Homeland Security Act of 2002 to facilitate sharing of the most valuable information about capabilities, threats, vulnerabilities, and deterrence programs possible. The law granted an exemption for voluntarily submitted critical infrastructure information from the Freedom of Information Act (FOIA) and state sunshine laws. To implement the law, DHS has created and led a working group to develop regulations and procedures for receipt, disposition, and use of Protected Critical Infrastructure Information (PCII). In February 2004, DHS created the PCII Program Office, which has developed rigorous safeguarding and handling procedures to manage the information flow and prevent unauthorized access to information submitted under the PCII program.

Separately, the market demand for cyber security presents a significant incentive for both government and industry to adopt the approach laid out in the Strategy.

e. The National Institute of Standards and Technology (NIST) has been active in developing cybersecurity requirements for industrial control systems. Are these activities being included in DHS efforts to develop cybersecurity standards? How will DHS capitalize on these activities to decrease the vulnerability of privately owned critical infrastructure?

Yes, the National Institute of Standards and Technology (NIST) efforts to develop cyber security requirements for industrial control systems have been included in DHS' efforts to develop cyber security standards, particularly in NCSD's effort to develop a control systems framework.

The control systems framework will build upon the work already completed by the NIST-sponsored Process Control Security Requirements Forum (PCSRF) and developed in compliance with the ISO 15408 requirements definition language (Common Criteria) to allow for international acceptance.

PCSRF has already developed a system protection profile for industrial control systems? components that serves as an appropriate starting point for this effort. Work continues on the profile, and once the reference components are defined, a vulnerability analysis will be conducted to enumerate the relevant operational security requirements for each class of component. These requirements will then be mapped to a set of security controls based on specific assurance levels and the criticality of the site in terms of impact on critical infrastructure, economic impact and/or potential loss of life due to an environmental manifestation of a successful cyber attack on a control system. Once this definition is complete, specific recommendations will be made to implement the appropriate security controls in each environment.

Currently there is a lack of specific guidance in the standards that are being developed for operational control systems implementations. NCSD will continue to work with the standards bodies and industry to define any specific sector operational requirements, and then to offer rigorously defined security requirements and specific recommendations for security and/or mitigation back to the standards bodies and to industry.

In addition to the framework, DHS has invested funds to augment the existing testing capability of the National Supervisory Control and Data Acquisition (SCADA) Testbed officially launched in May 2004 and run jointly by the Idaho National Environmental and Engineering Laboratory (INEEL) and Sandia. The National SCADA Testbed is aimed at SCADA systems only and aimed strictly at developing the capabilities to test energy sector systems. DHS' test center operates hand-in-hand with the SCADA Testbed, but the DHS effort is focused on the non-energy sectors and is trying to work with other existing private and public testbeds as to leverage their efforts and avoid duplication. The DHS Control Systems Security and Test Center (CSSTC) and the National SCADA Testbed was officially opened in August 2004.

Finally, with regard to control systems, NCSD is developing a control systems risk/impact decision tool that the US–CERT will be able to use for analysis and vulnerability evaluation for control systems.

4. Management

a. How is DHS distinguishing cybersecurity roles and responsibilities internally, e.g., NCSD, CIO, TSA, Secret Service, NCS, and others?

By virtue of the mandate provided in HSPD #7, NCSD has been given the mandate to "facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations." As such, NCSD is a national focal point for the public and private sectors on cyber security issues and it is responsible for coordinating the implementation of the *National Strategy to Secure Cyberspace.* NCSD recognizes that each of these entities may bring unique capabilities, responsibilities and/or authorities to bear on cyber security issues, and as such, NCSD must act as a coordinating body to ensure that these entities are acting in concert.

When dealing with the internal DHS information systems, the DHS CIO has the responsibility and authority to implement and assure the security of such systems. NCSD ensures that the office of the CIO is kept informed of the latest cyber threats and is provided with timely, actionable information to take steps to protect DHS systems from emerging malicious code occurrences.

The National Cyber Response Coordinating Group (NCRCG; previously known as the Cyber Interagency Incident Management Group) will coordinate interagency preparedness and operations to respond to, and recover from, cyber incidents and attacks. The role of the NCRCG is discussed in the Cyber Annex to the National Response Plan. The group brings together senior officials from DHS, law enforcement, defense, intelligence, and other government agencies that maintain significant cyber security capabilities. The combination of these officials/agencies provides the capability to analyze and coordinate a national level response to any incident that affects cyber assets. In addition to the ability to focus portions of their agencies? resources, they possess the necessary statutory authority to act.

The National Communications System (NCS) is responsible for coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances. National security and emergency preparedness (NS/EP) telecommunications services are those that are used to maintain a state of readiness or to respond to and manage any event or crisis that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the NS/EP of the United States. Both the NCS and NCSD report to the Assistant Secretary for Infrastructure Protection, which allows for close coordination on those cybersecurity issues that impact each organization.

The draft National Response Plan (NRP) is a set of defined processes that will bring together several DHS functions for cyber security. The Cyber Incident Annex of the NRP, as developed by NCSD in coordination with the NCRCG, establishes procedures for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to, and recovery from cyber Incidents of National Significance impacting critical national processes and the national economy. For physical incidents, Emergency Support Function 2 (ESF #2)—with NCS as coordinating agency—would coordinate Federal actions to restore backbone connectivity for the Internet and provide priority service to NS/EP users. The draft National Response Plan includes tie-ins between ESF #2 and the Cyber Incident Annex to ensure these functions stay coordinated, which has been operationalized by cross-membership across the NCS, NCRCG and the Interagency Incident Management Group (IIMG).

Various DHS components, including Immigration and Customs Enforcement (ICE) and the Secret Service have statutory responsibility for investigating cyber crimes. DHS through NCSD has assumed a supporting role in this area. Among the efforts that have been undertaken are, the support and administration of the Cyber Cop Portal, the co-sponsorship (with the Department of Justice) of the first statistically valid survey of cyber crime in the US, and the initiation of a number of joint meetings to address the issue of cyber attack attribution.

The Cyber Cop Portal is one of the oldest and most widely used mechanisms for sharing information in the electronic crimes community. It consists of over 5,300 members from all 50 states and over 40 countries. Its growth and use brought it to the point where it could no longer be maintained as a voluntary part time project, and it was in danger of being shut off. NCSD has decided to sponsor and administer the portal.

NCSD has agreed to provide funding and support to the DOJ Bureau of Justice Statistics to assist in the first ever statistically valid survey of cyber crime in the United States. The effort will involve questionnaires to over 36,000 US businesses covering all critical infrastructure sectors. The results of the survey will provide law enforcement and policy makers with a better understanding of the problem and how to allocate resources.

One key component in the ability to effectively respond to cyber attacks is attribution, determining the source of the attack. This is also one of the most difficult aspects of cyber attack investigations. The solution to the problem is not found in any one community of interest, but across a broad spectrum of disciplines (Intelligence, Counter Intelligence, Law Enforcement, private industry, etc.). Under the auspices of the NCRCG, and in conjunction with DOJ, a number of attribution meetings have been held or are being planned. These meetings are designed to develop an overall picture of the state of attribution throughout the various communities, and then to develop a plan to improve it. The plan is due during the second quarter of FY05.

b. What measures have been taken to elevate the importance of cybersecurity within the overall mission of DHS and to improve public awareness of cybersecurity issues? Specifically, should cybersecurity be a part of "READY.GOV" public web site to make Americans more aware of cybersecurity needs?

Cyber security is a priority issue for DHS and the mission for NCSD. We are improving public awareness of cyber security issues through the US–CERT public website and the NCAS launched in January 2004 as well as through our engagement in the National Cyber Security Alliance's Stay Safe Online campaign, our Outreach and Awareness branch, and our partnership with the MS–ISAC to reach state and local government. The US–CERT public website provides information on cyber security issues, cyber activity, and cyber vulnerabilities. NCAS is our primary mechanism for communicating with the public on cyber alerts, security tips, and other useful notifications. We are pursuing ways to reach as many Americans as possible through the website, awareness campaigns, and the NCAS as well as other public awareness efforts.

DHS is currently expanding the Ready campaign and is developing Ready for Business and Ready for Kids. Ready for Business is designed to help small to medium business owners safeguard their business operations in the event of a terrorist attack or other emergency.

Preliminary messages for the campaign center around three key themes: Ensuring Business Continuity, Safeguarding and Preparing Your Employees, and Safeguarding your Computer Systems (cyber security). The third theme will help businesses owners understand better the need for cyber security and also how to achieve it. It will encompass topics such as how to prevent computer viruses, how to detect computer viruses, how to preserve and back-up computer data, and how to prevent hacker intrusion.

DHS is working with the Advertising Council to develop content and messages that will inform and motivate business owners to take action. The messages will be distributed through a variety of vehicles that will target business owners and operators.

c. Some have suggested that the NCSD should be elevated within the DHS organization—either as a direct report to the Secretary Ridge or to the Under Secretary for Information Analysis and Infrastructure Protection. What is the Department's view of such a change?

The Department is working closely with the Homeland Security Council to evaluate this and other policy and organizational options related to elevating and expanding the current role of the NCSD.

5. Wireless Funding

a. The National Communications System program budget for Wireless Priority Service is $78M. The office of the Chief Information Officer (CIO) includes funding for wireless activities at $100M. How are your office, the CIO, and Science and Technology Directorate working together on developing these programs?

In summary, each program has a very distinct mission employing different technologies. DHS/IAIP recognizes the need to continually assess opportunities to insure integration of communications as well as efficiencies of programs. DHS has established forums for the review and ultimate execution of such a strategy and is coordinating all of its programs efforts. The IAIP NCS is an inter-agency body responsible (through E.O. 12472) to support the President in providing priority telecommunications services across federal, state and local entities that assures the greatest opportunity to communicate during all crises. The NCS Wireless Priority Service (WPS) program was directed by the National Security Council and subsequently authorized by the FCC. WPS is a National Security/Emergency Preparedness (NS/EP) priority service program utilizing based in the commercial/public cellular networks for designated Federal, State, Local and critical infrastructure owner leadership. The DHS CIO office focuses on managing the wireless assets for the department with a significant focus on the private Land Mobile Radio (LMR) network users of the federal entities transferred to DHS. They are also engaged with DOJ in leveraging its capabilities and development of LMR interoperable communications for the Federal law enforcement community. In terms of coordination, the NCS programs, through exhibits 300, are reviewed and approved by the DHS CIO office. The CIO office also has established a wireless management working group which IAIP NCS participates in regularly to review technology issues and evolution as well as identify areas that will create efficiencies of all programs. A primary long term objective, in addition to assuring interoperability of DHS assets, is to integrate WPS capabilities with all wireless solutions as technology enables.

IAIP, DHS' CIO Office and the S&T Directorate, along with other Directorates, also work together on common interoperability challenges through the Department's new Office of Interoperability and Compatibility. This Office, housed within the S&T Directorate, was created to coordinate the multiple interoperability efforts and needs of the Department as well as look to leveraging the vast range of interoperability programs and efforts within the Federal government. Additionally, the DHS S&T Directorate manages the SAFECOM Project charged with partnering with state and local governments to improve the interoperability of federal, state and local LMR communications for first responders. In this area as well, IAIP support to DHS S&T through participation and review of Project SAFECOM activities, includes assuring that the WPS can effectively interoperate with Project SAFECOM solutions as technology dependency eases to a more open environment.

b. Describe how First Responders will be able to benefit from the results of these efforts.

First Responders are increasing their dependence on wireless communications for command and control during emergency operations. The WPS program provides government and private sector leadership, such as incident commanders, with priority access to the public cellular infrastructure. The WPS link improves the commander's ability to receive reports from and give instructions to First Responder teams and other supporting organizations. Without the WPS link, command and control could be degraded because of cellular call-congestion in the vicinity of the incident/ emergency for all government and private sector leadership.

Deployment of WPS across the wireless industry is essential to a full public network based emergency capability for response as well as COOP and COG needs. WPS is the cellular augmentation of the Government Emergency Telecommunications Service (GETS). It is anticipated that in the future technology will enable the integration of these capabilities with the interoperable Land Mobile Radio (LMR) private systems employed by the broad based first responder community.

QUESTIONS FROM CONGRESSMAN JIM TURNER

1. When the National Cyber Security Division (NCSD) was created in June of last summer, the Department announced it would build upon the existing capabilities of several agencies with cyber responsibilities transferred to DHS, including the National Communications System (NCS). The NCS, however, has remained separate from the NCSD. Yet, the NCS remains responsible for several cybersecurity initiatives, including the "Network Security Information Exchanges (NSIE)" and the "Cyber Warning Information Network." The proposed budget continues to keep the NCS activities separate from the NCSD. Isn't it counterproductive to have so many core cyber functions outside the National Cyber Security Division? Wasn't the creation of the National Cyber Security Division intended to provide a focal point for cyber security threat and vulnerability assessment, as well as information sharing, within the Department?

The June 2003 DHS announcement forming the NCSD was not intended to suggest that NCS would be fully absorbed into NCSD. The NCS is an interagency organization formed under Executive order 12472 to support the President in the provision of National Security/Emergency Preparedness (NS/EP) Telecommunications meeting the need of the federal government under all wartime and non-wartime crisis conditions. This is a critical mission that now addresses infrastructure protection issues in addition to its traditional COOP/COG focus.

The NSIE referenced in the question is a government and industry effort initiated under the auspices of the President's National Security Telecommunications Advisory Committee (NSTAC) and is managed through the NCS National Coordinating Center for Telecommunications (NCC). It addresses a very broad range of security issues potentially affecting the telecommunications infrastructure. Cyber security is only one component of these issues and the NCSD sits on the NSIE to address these matters. Also referenced in the question is the Cyber Warning Information Network (CWIN). When first envisioned, this private network was focused on the cyber arena, as the development of the US–CERT became firm and with further analysis, IP recognized that this capability had far more utility than originally intended. CWIN is intended to provide information and warnings across all infrastructures to our State, local, and industry partners. CWIN has been transferred to the IP Infrastructure Coordination Division (ICD) where it will support the cross-sector needs for all IP divisions.

In order to facilitate coordination between these elements, Infrastructure Protection is currently building out a watch center facility, the National Information Coordination Center (NICC) that will include NCSD, US–CERT, NCS, and ICD. Colocating these groups on in a single watch center facility will facilitate the fast and efficient sharing of information. Initial move in to this facility is scheduled for the first quarter of 2005.

2. The IAIP budget includes a $1.9 million increase for conducting cyber exercises such as "Live Wire," which was a simulation of a terrorist attack on computer, banking, and utility systems. There are, however, existing cyber exercises that are up-and-running. Over two years—since before the Department was created—the city of San Antonio planned and conducted "Operation Dark Screen," a cyber terrorism exercise that involved both the public and private sector and was designed to help the city defend and respond to a cyber attack. Even within the Department, the Secret Service is reaching out to the private sector and supporting table-top exercises to

address the security of private infrastructures. What is the IAIP Directorate doing to integrate and coordinate with existing cyberexercises such as these? How much of the requested $1.9 million will go towards these existing exercises that have been tested and proven? In addition, what is DHS doing to ensure that our local communities and towns, who will provide the cyber-first responders in the time of crisis, are prepared? Isn't it true that there is no individual entity or individual within IAIP responsible for coordinating all of the cyberexercises being put on by the government and, as a result, there may be duplicative efforts?

Whereas the first responder and emergency management communities have been exercising at national, regional, and local levels for many years, the cyber response community is quickly catching up. The U.S. Government has an active program of exercises to assess preparedness and processes in the event of an attack on the Nation. DHS has established a National Exercise Program Office (NEP) to coordinate scheduling and participation in the exercises sponsored by various agencies. The IAIP Directorate is coordinating its exercise planning with the NEP, which is the responsibility of the DHS Office of Domestic Preparedness. The IAIP Under Secretary's Office has an Exercise Management Program (EMP) that maintains regular contact with members of the exercise community and coordinates with the NEP to facilitate the Directorate's participation in exercises. NCSD's coordination efforts entail scheduling cyber security exercises with NEP as well as integrating cyber scenario components into other planned exercises as appropriate. These coordination efforts with NEP assist in minimizing the duplication of exercise efforts.

NCSD's involvement in the NEP is guided by two principles: (1) while cyber is only one element of a multifaceted NEP, cyber elements must be closely coordinated with other elements of that program to ensure efficient use of limited resources and the most effective return on exercise investments; (2) cyber exercise elements must not be sidelined or relegated to an "afterthought" category within the NEP.

In October 2003, numerous federal agencies participated in *Livewire,* the first ever national-level cyber exercise to baseline our capabilities for responding to national cyber attack. The exercise involved more than 300 participants representing more than 50 organizations across the federal, state, and local governments, as well as the private sector. Cyber attack simulation scenarios were developed to stress cyber interdependencies across America's critical infrastructures and baseline government agencies' abilities to collaborate across the public and private sectors. Information gleaned from *Livewire* and similar exercises aimed at ensuring security of critical infrastructures are being used to improve our national incident response processes.

While *Livewire* brought together a number of players for a large-scale event simulation, other exercises target specific areas or agency concerns. For example, the United States Secret Service's (USSS) Electronic Crimes Task Forces (ECTFs) have been running smaller regional and sector-specific tabletop exercises over the past eighteen months. These exercises are designed to help coordinate efforts in a targeted geographic area and are tailored to a specific regional infrastructure, such as the energy industry in Houston, TX, the high-technology industry in San Francisco, CA, and the banking and finance industry in Charlotte, NC. In February 2004, the National Defense University ran its *Dark Portal* exercise and in August 2004, a cyber security workshop co-hosted by NCSD and the National Security Council was held at the National Defense University. This tabletop workshop exercise included members of the National Cyber Response Coordination Group (NCRCG), as well as multi-agency key decision makers in the U.S. Government cyber security realm.

NCSD has sponsored several exercises that test cyber readiness in various geographic locations and critical infrastructure sectors across the Nation. In September and October 2004, a series of regional exercises were held in Seattle, WA (Blue Cascades II) and New Orleans, LA (Purple Crescent II). Both exercises were successful in highlighting dependencies between cyber and physical infrastructures and interdependencies among critical infrastructures. These exercises also identified and tested the coordination and cooperation among federal, state, and local governments with the private sector in the case of attacks (both cyber and physical) on the critical infrastructures in those regions of the U.S. In addition, each of the exercises illustrated the need to continue to provide outreach and cyber education to local emergency management and physical security professionals as well as identify and improve shortfalls in emergency preparedness.

DHS EMP serves as the lead organization in the development, facilitation and participation of a week-long, cabinet-level national exercise ("TOPOFF3") to be held in the summer of 2005. These national exercise programs occur every two years and involve the same basic set of participants. The exercise for TOPOFF3 represents a joint physical and cyber scenario, with NCSD leading the development of the cyber component for the exercise. It will test not only response to attacks, but also continuity of government and operations, emergency response at the state, regional and local levels, and containment and mitigation of chemical, nuclear, and other attacks, etc. NCSD is also working with DHS to ensure a more prominent cyber component in the follow-on TOPOFF series of exercises for 2007 and beyond.

The lessons learned from these and other exercises will form the backdrop for an NCSD-sponsored National Cyber Exercise planned for November 2005. Planning activities are currently underway with initial groundwork already laid for this effort. In September 2004, a key stakeholder meeting was held to discuss the scope and objectives with critical infrastructure sector lead agencies. NCSD is in the process of planning the Initial Planning Conference (IPC) for the National Cyber Exercise that will include representatives from various government agencies and the private sector. The IPC will allow the opportunity for the stakeholders to establish clear and concise goals and objectives for the National Cyber Exercise as well as to discuss and develop possible scenarios.

The objectives of the National Cyber Exercise are to:

1. Sensitize a diverse constituency of private and public-sector decision-makers to a variety of potential cyber threats including strategic attack;
2. Familiarize this constituency with DHS' concept of a national cyber response system and the importance of their role in it; and
3. Practice effective collaborative response to a variety of cyber attack scenarios, including crisis decision-making.
4. Provide an environment for evaluation of interagency and cross-sector business processes reliant on information infrastructure.
5. Measure the progress of ongoing U.S. efforts to defend against an attack.
6. Foster improved information sharing among government agencies and between government and industry.
7. Identify new technologies that could provide earlier warning of attacks.
8. Define the roles and responsibilities of government agencies and industry.

Questions for Chief Officer Steven Cooper, From Congressman Mac Thornberry and Congresswoman Zoe Lofgren

1. Cybersecurity Standards

Question: a. How are technical cybersecurity standards being established and enforced across the Department for information technology purchases, processes, and practices?

Technical Cybersecurity Standards are promulgated through the Technical Reference Model portion of the Department's Enterprise Architecture Program. There are also mature standards established through the Federal Information Processing Standards. The Information System Security Managers at the organizational elements are responsible for ensuring compliance with standards. In addition, regular Program and Acquisition reviews check for compliance with published standards.

The Department's long-term strategic approach for the enforcement of information technology security standards is to verify policy and standards compliance during the Security Test and Evaluation phase of the system Certification and Accreditation (C&A) process. DHS is currently in the process of establishing an enterprise C&A application that will maintain an online repository of all C&A documentation and enforce the use of Department mandated C&A methodologies. This application will generate comprehensive system test procedures and processes to fully map system compliance with DHS policy and standards. The current status of implementing this C&A tool is that DHS has completed the Requirements Definition phase and product evaluation phase, and have an operational pilot system which has given phenomenal results. We expect to have a Department implementation in the near future.

The Department also verifies proper implementation of policy and standards by conducting NIST 800–26 reviews of security controls in accordance with Office of Management and Budget Memorandum M–03–19. These reviews are ongoing.

Question: b. Who sets cybersecurity requirements for the Department and how are they communicated to the technology developer or purveyor?

DHS follows cybersecurity standards requirements established by the Committee for National Security Systems for its classified systems, and the Office of Management and Budget, and National Institute of Standards and Technology guidance for it unclassified systems. Additionally, mission specific requirements are promulgated through the internal Management Directives, as well as through the Technical Reference Model of the Department's Enterprise Architecture. These have been provided to industry in general, and are also specifically called out when appropriate in contracting vehicles.

Question: c. How are cybersecurity standards requirements being incorporated in calls for proposals, grants or other contracting mechanisms?

The DHS Science and Technology (S&T) Directorate is in the process of establishing a DHS-internal Cyber Security Standards Working Group. Within the S&T Directorate, the working group will include representatives from the Standards and Cyber Security R&D portfolios, as well as representatives from S&T's Chief Information Officer (CIO) group. Outside of S&T, invitations to serve on the working group have been extended to the DHS Office of the CIO, the National Cyber Security Division and the National Communications System in the Information Analysis and Infrastructure Protection Directorate, and the United States Secret Service. This group will collectively identify what cyber security standards requirements should be incorporated into S&T's R&D portfolio investment plans.

Question: d. In what areas of cybersecurity do you see a need for new or better standards, benchmarks, and other elements of a cybersecurity framework, and what can DHS do to help implement such a framework?

With new areas of technology emerging every day as well as new applications of existing technology, there is always a need to refine existing standards and promote new ones. The emergence of MPLS has opened many new questions and the means to securely implement reliable, secure wireless networks continues to be a challenge, as does the management of geospatial data and Law Enforcement Information. DHS works closely with the Federal cooperative process through bodies such as the National Institute of Standards and Technology and the Committee for National Security Systems to ensure the success of these efforts.

Question: e. Does the office of the Chief Information Officer (CIO) use any cybersecurity standards and processes recommended by the National Cybersecurity Division (NCSD), National Institute of Standards and Technology (NIST), and National Security Agency (NSA) to secure the DHS enterprise architecture?

To the best of our ability, all relevant standards from national bodies such as NIST, NSA and NCSD are applied throughout DHS. This includes relevant FIPS and similar standards for procurement and internal processes such as self assessments and Certification and Accreditation are explicitly standards based.

Question: f. How does NCSD provide actionable cybersecurity information to the CIO to consider in its enterprise architecture implementation?

DHS participates in the interagency US CERT process. As a member of USCIRC, DHS like all participating agencies, gets alerts, warning and mitigation tools in a timely manner. In addition, there is a constant and constructive exchange of information between the National Cyber Security Division and the Office of the CIO for timely notifications of relevant issues. Actionable items—such as those that may significantly compromise confidentiality or availability are given the highest priority for incorporation into the Department's security architecture which is integral to the Department's Enterprise Architecture.

2. Purchasing Power

Question: a. What specific actions has DHS taken to improve its FISMA report card in order to become government model for secure information systems?

DHS has implemented a COTS enterprise product to provide automated support for 800–26 assessments, manage FISMA metric reporting, as well as Department-wide Plans of Actions and Milestones (POA&M). This product is being used to generate a Digital Dashboard showing Organization Element performance metrics and overall DHS performance metrics, and access to this system has been made available to the OIG to ensure veracity of FISMA data reported by Organizational Elements. Access to the Digital Dashboard will be made available to senior management in the near future to ensure that senior managers are directly involved with the Department's Information Security Program. In the past few moths we have implemented several enhancements made to FISMA reporting product for improving reporting of 800–26 and C&A metrics. This enhancements include a) 800–26 integrity checking; 2) computed metrics for 800–26 assessments and C&A; capability to upload assessment and C&A artifacts; 4) better tracking of C&A deliverables. We have purchased an Enterprise license for a C&A tool (SecureInfo RMS). This tool has been installed on an Enterprise server and all OEs are currently using the tools with DHS ramping up to full mandatory use. The DHS baseline policy has been mapped to this tool and use of the tool will ensure that the C&A SRTM is mapped to DHS policy. We have prepared and submitted a POA&M to OMB to achieve full ATO on all currently reported systems by the end of July, 2005. To ensure continued progress we have formed a DHS security working group to focus on FISMA reporting and FISMA issues.

Question: b. Many witnesses before the Subcommittee have suggested that a powerful tool the federal government possesses in cybersecurity is its buying power. Has DHS used this power to induce hardware or software manufacturers to provide more secure systems?

Every new information technology contracting vehicle put into place by the Department includes robust security standards. Additionally, the Department regularly engages information technology vendors to ensure that strong security is integral to product development and implementation.

3. Wireless Funding

Question: a. The office of the CIO includes funding for wireless activities at $100M. The National Communications System (NCS) program budget for Wireless Priority Service is $78M. How are your office, the NCS, and the Science and Technology Directorate working together on developing these programs?

The Wireless Management Office (WMO), within the DHS Office of the Chief Information Officer, is mandated to lead and coordinate the Department's programs, projects, and initiatives that involve the wireless transport of information, including voice, data, and multimedia. The WMO's mission, "To be the model program office, providing state-of-the art wireless capabilities to preserve our freedoms and protect America," serves to focus and provide direction for the program's activities and services to ensure the effective use of wireless technologies across the Department's organizational elements. As part of its mission, the WMO integrates its activities with the National Communications System (NCS) and the wireless initiatives of S&T to meet evolving homeland security requirements. The WMO is primarily focused on wireless communications to support internal DHS missions. The NCS is responsible for directing the Wireless Priority Service program which supports commercial, private sector wireless capabilities.

The WMO is working with NCS and the DHS S&T Directorate in implementing program activities through groups such as the Wireless Working Group (WWG). The WWG is a coordination body established to ensure DHS-wide approaches to wireless communications are developed and implemented in an integrated manner. The WMO chairs the WWG, which is composed of 80 representatives from all of the DHS organizational elements with wireless communications as part of their mission. The majority of the WMO's coordination with the NCS and DHS S&T occurs through its participation on the WWG to collect DHS organizational elements wireless requirements, coordinate resource utilization, and ensure organizational elements play an integrated roll in centralized DHS wireless concepts (e.g., system designs, user requirements, operational concepts, procurement contracts). This collaborative approach is consistent with the Department's customer service strategy and allows for on-going feedback and confirmation that the WMO is adequately addressing the needs of its customers and stakeholders.

Question: b. Describe how First Responders will be able to benefit from the results of these efforts.

The activities of the WMO, in partnership with DHS S&T and the NCS, directly benefits first responders at all levels of the government by equipping them with the wireless capabilities to fulfill their missions of protecting the homeland. By building strong relationships that foster increased coordination among first responders, enabling and enhancing their wireless capabilities, the DHS WMO—in coordination with DHS S&T and NCS—are achieving several objectives to the benefit of first responders, including—

- Implementing integrated, nationwide tactical communications capabilities for DHS organizational elements and other public safety first responders
- Providing technical assistance and implementation of wireless enhancements
- Advancing the use of emerging wireless technologies among first responders

These objectives are being met through several major initiatives supported by the WMO and coordinated with DHS S&T and the NCS.

Integrated Wireless Network (IWN): The mission of the Integrated Wireless Network (IWN) project is to provide a consolidated, nationwide approach to reliable, seamless, interoperable wireless communications to support federal agencies and officers engaged in the conduct of law enforcement, protective services, homeland defense, and disaster response within the Departments of Homeland Security, Justice, and Treasury. The IWN will serve as the day-to-day tactical communications network for the DHS, Justice, and Treasury user community, as well as for those within DHS and Treasury, replacing outdated and antiquated legacy communications systems. As a result, the IWN, in every sense, will serve as the lifeline that directly supports the wireless communications capabilities of first responders.

The IWN represents an investment in voice and data communications technologies, the completed system will establish a 24 x 7 communications network, complete with support services that will include major disaster recovery and contingency capabilities (e.g. system back-up). A centrally managed and coordinated approach to this initiative ensures that common, standards-compliant technologies are procured, thereby fostering interoperability between and among federal agencies for more effective and efficient enforcement activities, as well as provisioning communications interoperability with our state and local partners for event management and crisis response.

G4*High Risk Metropolitan Areas Interoperability Project:* With the demand for improved intergovernmental communications necessitated by homeland security concerns, federal agents must increasingly interoperate with other federal, state, and local public safety entities. The project was initiated to improve federal interoperability with local first responders in the highest threat areas across the country. The project is being implemented in coordination with the interoperability efforts of the WMO, SAFECOM, and the Office of Domestic Preparedness (ODP).

WMO Sponsored Projects: The WMO is supporting several projects that are improving the wireless communications capabilities of agencies at all levels of the government.

DC Broadband Project: The District of Columbia is currently implementing a cost-effective, high-speed, wide area, wireless data network that will permit the use of interoperable, broadband, wireless data applications for public safety communications. This network will allow first responders in the NCS to use full-motion, high-resolution video monitoring and other bandwidth-intensive monitoring tools to immediately share time-critical incident and emergency event information.

This will enhance regional and federal first responder capabilities. It will also provide accurate interoperability usage profiles and results, collect data on network performance (data throughput, coverage, latency, and effective of spread spectrum technologies), and implement public safety application requirements and operations improvements.

Phoenix Mesa Interoperability Project: This project provides an opportunity for the WMO to partner with state and local agencies and build upon existing communications system infrastructure. The WMO plans to leverage this existing system by installing federal very high frequency (VHF) trunked repeaters at select locally-owned radio frequency (RF) sites. The project should result in several key benefits, including the demonstration of an innovative application that can be replicated across the country, providing potential long-term cost savings for IWN implementation, and serving as a model for coordination and partnerships among federal, state, and local agencies and first responders.

The primary goal of the project is to demonstrate the feasibility of local and federal agencies utilizing common infrastructure while operating within different frequency bands. To accomplish this goal, the WMO partnered with the cities of Phoenix and Mesa, Arizona, who were two of the first cities in the country to implement a regional TIA/EIA–102 Project 25 800-megahertz trunked system. The installation of these repeaters will enable the WMO to use existing system assets such as shelters, towers, connectivity, and network management infrastructure.

SAFECOM: Linking federal tactical communications to local, state, and tribal public safety first responders is critical to ensuring seamless, wireless communications at the scene of the incident and improving officer safety. In 2002, as part of the President's Management Agenda, the White House established SAFECOM as the umbrella program within the Federal Government to oversee all communication interoperability initiatives and projects. Through SAFECOM, the Federal Government is addressing public safety communications issues in a more coordinated, comprehensive, and effective way.

The WMO is working with SAFECOM to improve wireless communications interoperability among federal, state, and local public safety first responders. The WMO does so by recognizing and supporting the crucial role of SAFECOM to the benefit of first responders to include—

- Creating and adopting standards
- Recognizing interoperability and communications issues
- Identifying current initiatives that address interoperable communications issues, and
- Developing coordinated strategies to leverage work, while decreasing the unnecessary duplication of efforts.

Collectively, the programs are providing the vital link to improve vertical interoperability among over 100 federal agencies with public safety response to over 44,000 local and state first responders.

Federal Partnership for Interoperable Communications (FPIC): The FPIC works to advance federal wireless communications interoperability across federal first responders by fostering intergovernmental cooperation. The FPIC pursues this mission by advancing the following goals to the benefit of the federal wireless community: providing technical and operational advice to SAFECOM and federal departments and agencies; educating federal users about wireless communications equipment, security, and operations standards and best practices; and coordinating wireless communications interoperability efforts within the Federal Government.

As members of FPIC, the WMO and SAFECOM work to improve federal wireless communications first responders through standing committees and working groups. Standing committees—such as the Standards, Security, and Spectrum Standing Committees—coordinate ongoing FPIC activities. Working groups are established to consider, investigate, and/or act on a specific activity or subject area of interest to members. The FPIC may establish partnerships with state/local organizations, associations, departments, bureaus, agencies, or individuals as appropriate. In this way, projects of mutual concern to all of the wireless public safety community can be addressed in a cooperative manner.

Question: 4. To what degree do the DHS enterprise architecture plans integrate with the federal enterprise architecture effort? How is DHS working with other departments to establish cybersecurity standards?

Support for Federal Initiatives

EA is one of the means by which visibility into IT assets can enable the federal government to find business and financial efficiencies. Our alignment to the Office of Management and Budget (OMB) Federal Enterprise Architecture (FEA) continues throughout all of our Enterprise Architecture (EA) efforts. Our FEA and e-government initiatives are discussed below.

Support for the Federal Enterprise Architecture

Our EA planning project was driven by the concepts and products of the OMB FEA Reference Models. We have aligned the various EA artifacts with the five FEA Reference Models: the Business Reference Model, the Data and Information Reference Model, the Service/Component Reference Model, the Technical Reference Model, and the Performance Reference Model. And, more importantly, we have embraced the two FEA foundation concepts: Line of Sight for program effectiveness and Component and Service Based Architectures for effective reuse and repeatability.

Business Reference Model. The FEA Business Reference Model drove the development of our business model. Several of the Business Reference Model Lines of Business are directly applicable to DHS (in particular, Homeland Security and Disaster Management). For all other business activities within the DHS business value chain level, there is a one-to-one link to the Business Reference Model Lines of Business. The EA Business Model includes a matrix that shows the relationship between our business activities and the Business Reference Model Subfunctions. It is important to note that every business activity in the EA Business Model is mapped to a Business Reference Model Sub-function. As a result of this alignment, OMB should be able to readily identify functional commonality of DHS with other federal agencies.

Data and Information Reference Model. The Data Reference Model consists of a layered model for decomposing collections of information, from Subject Areas down to Data Objects and their properties. We adopted this approach and classified the information required to support the homeland security business activities at the Subject Area and Data Object levels. Further decomposition and description of the data objects will be performed in the next phase of the EA process. Our Data Architecture aligns with the Data Reference Model concepts by providing a common, consistent way of categorizing and describing data to facilitate data sharing and integration.

Service Component Reference Model. The DHS EA project has fully embraced the FEA Service/Component Reference Model's component-based approach to the reuse of applications, application capabilities, components, and business services across the federal government. OMB created the Service/Component Reference Model specifically to identify service components and their relationship to the technology architectures of federal agencies. We leveraged the Service/Component Reference Model in two important manners: (1) the structure of our Application Architecture is a set of interworking components that has direct ties to the Service/Component Reference Model, and (2) our Technology Architecture applies a set of technology patterns that is derived directly from the technology aspects of the reference model.

The Application Architecture has been constructed to leverage reusable components that can be acquired once and used to provide services to many applications. It shows the structure of this component reuse. From the set of component architecture diagrams, it can be seen that there is a significant opportunity to apply this reuse concept throughout DHS (and across other government agencies). The result should be considerable cost savings, as well as greatly improved interoperability and flexibility of applications.

The Technology Patterns of our EA are repeatable solutions to recurring technical challenges. These patterns employ technologies described in the DHS Technical Reference Model (discussed below) and provide capabilities as described in the FEA Service/Component Reference Model. For example, the Business Intelligence/Data Warehouse technology pattern of our EA aligns with the Business Intelligence Service Type of the FEA reference model.

Technical Reference Model. The initial formulation of the DHS Technical Reference Model began with the taxonomy as well as the technical services, protocols, and interfaces specified in the FEA Technical Reference Model. The DHS model extends and refines the FEA model where necessary to reflect the additional functional and technology requirements of DHS. In deriving the DHS model from the FEA model, we have also made adjustments to better align the technology categories with the physical layering of services that exist in vendor and open source products. The Domain level (Tier 3) categories of the DHS model have all been mapped to the FEA model, so that comparisons can be directly made with the technical reference models from other agencies.

Performance Reference Model. Although this FEA reference model was still under development during our EA planning project, an initial attempt was made to align our Business Model with the intent of the Performance Reference Model, based on draft materials provided by OMB. Specifically, the Business Model includes a table that defines the outcomes or measurement categories and corresponding indicators (metrics) for each cross-cutting, corporate activity defined in the Homeland Security Value Chain. Measurement categories are defined for each activity in six areas: Mission and Business Results, Customer Results, and Process and Activities, People, Technology, and Other Fixed Assets. This guidance within the DHS EA will provide specific DHS IT programs with a starting point for applying the Performance Reference Model within their Exhibit 300 submissions to OMB.

Support of E-Government Initiatives

The Target EA and Transition Strategy identified several opportunities to leverage on-going e-Government initiatives. As you may be aware, the Department is currently the managing partner for the Disaster Management and Safecom e-Gov initiatives. The Department is also actively participating in six additional e-gov initiatives. For example, there are three major organizations within the department that provide grants to state, local, private industry, academia, and individuals for a variety of reasons that participate in the e-Grants effort. We will be looking more closely at this mode of delivery and how it may leveraged into the EA program.

Finally, the target EA identifies a concept for homeland security information sharing and knowledge flow—the Homeland Security Information Sharing Architecture—based on a concept of Communities of Interest adopted from the intelligence community. Information sharing with state, local, tribal, and other federal government entities is a critical function of DHS, both as a source of information and as the “first responders” to an incident. Implementation of this information sharing architecture will provide value to homeland security community by driving results and productivity through effective information sharing.

In addition to the initiatives for which DHS has the lead responsibility, we expect to be a major contributing player or user of several others. We are committed to transitioning to projects such as e-Authentication, e-Clearance, e-Payroll, e-Travel, and HR Integration. We are actively gaining more knowledge about these initiatives so that our role in supporting them and their particular timelines and capabilities can be integrated seamlessly into our target and transition strategy.

○