STATEMENT

OF

GEORGE FORESMAN

UNDERSECRETARY FOR PREPAREDNESS
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON FEDERAL FINANCIAL
MANAGEMENT, GOVERNMENT INFORMATION, AND
INTERNATIONAL SECURITY

COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

July 28, 2006

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about cyber security and the recovery and reconstitution of critical networks.

Our Nation's communications and information infrastructure will support profound improvements in the security of our homeland in the next 20 years. States, communities, and our private sector partners are already finding innovative ways to prevent terrorism and protect critical infrastructure by leveraging information technology. As I outline further below, the Federal government is similarly deploying innovative programs that significantly raise the level of preparedness in this critical area.

Our vision and philosophy for the future build upon accomplishments of the past several years – critical infrastructure businesses, home users, and government at all levels have a greater understanding of the threat posed by malicious software. The communications and information technology sectors have deployed new tools to help these constituents manage cyber risks.

However, at the core of our vision and philosophy is a strong belief that the Department of Homeland Security (DHS) must increasingly guard against more virulent attacks and cyber disruptions – whether caused by a terrorist attack or natural disaster. We must prevent cyber incidents of national significance.

In this testimony, I will outline three strategic goals to execute this vision, and examples of current and future programs that will move us forward to these objectives.

Assistant Secretary for Cyber Security and Telecommunications

As a preliminary matter, allow me to outline the steps the Department is currently taking while working with the White House to actively pursue qualified candidates for the post of Assistant Secretary for Cyber Security and Telecommunications. I am personally engaged in the process of selecting the new Assistant Secretary and, in the interim, am providing program direction pending the post being filled permanently. Because of the importance of this mission, all parties want to ensure that the individual appointed to this position possesses the right combination of skills, experience, and leadership necessary to succeed.

To supplement my own personal involvement in strategy, the Assistant Secretary for Infrastructure Protection has been serving as the Acting Assistant Secretary for Cyber Security and Telecommunications. As such, he has been actively engaged in overseeing operational programs,

program reviews, governance structure, and has participated in government/industry forums to further the advancement of this important new office as well as the strategic goals that I will outline shortly.

Regardless of when this position is filled, the mission of the Department of Homeland Security (DHS), the National Cyber Security Division (NCSD), and the National Communications System (NCS) remain clear. The absence of a permanent Assistant Secretary for Cyber Security and Telecommunication has not had an impact on NCSD's or NCS's critically important work.

Strategic Vision and Philosophy

The Assistant Secretary for Cyber Security and Telecommunications position highlights the fundamental importance the Department places on communications and information technology (IT), as well as critical linkages across the economy and our critical infrastructure sectors.

Our vision and philosophy for cyber security and recovery reflects the expanding importance of our communications and information infrastructure in all walks of life. As you know, a failure to consider and deploy effective strategies could adversely affect homeland and national security, public health and welfare, and our economic security. Policies that advance a safe and secure communications infrastructure promote public trust and confidence, project stability to those who wish us harm, and foster valuable relationships between the public and private sectors.

We fully recognize the challenges inherent in our preparedness responsibilities. We are faced with difficult choices and options. We must think about risks to the communications and information infrastructure in new and creative ways. We must prioritize resources, and make hard decisions where resources are limited.

We must also continue to partner strategically with the communications and information technology sectors as well as other experts outside of the Federal government. As we focus on the potential for catastrophic cyber disasters, our partnerships are becoming more diverse and sophisticated, reflecting the different technology, business, and policy decisions that must be made. These partnerships also entail strengthening cooperation across the government and, at a minimum, finding ways to cultivate support outside of the Department where expertise clearly exists. Whether public or private, the partnerships must deliver real and measurable value in light of the catastrophic damages that can occur in the absence of smart collaboration.

Finally, we must reinforce a culture of preparedness and increasingly shift from a reactive to a proactive stance. In sum, we must prepare by promoting effective security strategies that evolve as the threat evolves.

Three Strategic Goals

In responding to these challenges, the Preparedness Directorate is executing three strategic priorities. (1) We are preparing for cyber incident of national significance; (2) we are working to forge more effective partnerships; and (3) we are working to foster a culture of preparedness to prevent cyber incidents and mitigate damage when disruptions occur.

- **First, we must prepare for a large scale cyber disaster.**

Our primary strategic goal is to prepare for high-consequence incidents. These would include, for example, a widespread disruption involving the Internet or critical communications infrastructure, whether from an attack or natural disaster.

Now, as the Department matures we are preparing for large scale cyber disasters. Our strategic intentions are ambitious and will require resolution of multiple impediments, such as:

- Identifying incidents and providing early warning;
- Deploying Federal assets and services more efficiently to mitigate damages where disruptions occur;
- Responding to the speed of attacks and disruptions, which will require new technologies and skill sets in our workforce; and
- Maximizing the use of tools that promote and integrate privacy protections as well as real-time security needs.

The Preparedness Directorate has several important programs already underway to prepare for a cyber incident of national significance. The Office of Cyber Security and Telecommunications has established an Internet Disruption Working Group (IDWG) to address the resiliency and recovery of Internet functions in the event of a major cyber incident. The IDWG is not examining all risks, but is focusing on and identifying measures that government and its stakeholders can take to protect against nationally significant Internet disruptions.

These proposed measures may yield heightened expectations, roles, and responsibilities for the United States Computer Emergency Readiness Team (US-CERT).

- **Second, we must continue to forge more effective partnership arrangements.**

Our second strategic goal is to improve the Department's partnership programs and practices. Homeland Security Presidential Directive 7, the Administration's policy on critical infrastructure protection, explicitly recognizes the importance of partnerships, which are essential for many sound reasons. In the cyber security arena, the Department is working to nurture existing partnerships and establish new relationships with three key stakeholder communities: (1) the private sector; (2) Federal departments and agencies and State, local, and tribal governments; and (3) academia.

Private Sector Partnerships. Industry owns, operates, and controls the bulk of the communications and information infrastructure, so collaborating with industry to prepare for and respond to catastrophic cyber disasters is a strategic priority.

In "The Federal Response to Hurricane Katrina: Lessons Learned," the White House pinpointed specific problems experienced by infrastructure owners in restoring communications services. The report additionally described interdependencies between the critical infrastructure sectors, such as energy and transportation, that impact restoration of communications services. Our vision for the future, and emphasis on close collaboration with the private sector, follows directly from these lessons learned.

In our partnerships, the government must deliver real value to our private sector partners, who are clearly committed to a collaborative approach. Smart, effective partnerships demand that we:

- Understand how the private sector will prepare for and respond to cyber disasters – and where the government can complement industry practices;
- Leverage state of the art technologies to improve preparedness and response and sustain privacy protections;
- Promote pools of knowledge and subject matter expertise for reconstituting communications and information infrastructure; and
- Ensure close coordination of Preparedness Directorate functions, such as those provided by NCSD and NCS,

Government Partnerships. The Department is similarly committed to enhancing partnership arrangements across the Federal government and

with State, local, and tribal governments. We will continue to explore innovative ways to leverage skill sets outside of the Department as part of our strategy for cyber-preparedness and response. We currently partner with Multi-State Information Sharing and Analysis Center (MS-ISAC), as well a key operational information technology and communications officials in the states, and we are strengthening those partnerships for recovery and reconstitution efforts.

Partnerships with Academia. The Department is serious about partnering aggressively with experts in academia. To date, the Department has included academia in partnership discussions; however, in order to lay a foundation for more effective cyber response capability, we must seek guidance from academia on a range of more complex problems. As an example, we expect to learn more from academia on such matters as challenges with insurance and risk transfer for the critical infrastructure sectors as well as business case arguments for catastrophic preparedness. These areas promote public and private sector collaboration.

Third, we must create a culture of preparedness – both to prevent a cyber disaster and to mitigate damages if widespread disruptions occur.

Our third and final strategic goal seeks to influence how we prepare for security challenges in the coming decade. As with our other strategic priorities, this goal demands a focused and disciplined approach in several areas. At a minimum, we are structuring programs to:

- **Clearly outline preparedness organizations, relationships, and expectations:** One of the Preparedness Directorate's strategic priorities is to clearly set forth all aspects of "doctrine" in accordance with legislative and Presidential direction. To create a long-term culture of preparedness, we are developing clear organizational doctrine, which memorializes strategic policies, clarifies roles and responsibilities, and defines measures of accountability.

- **Promote a shared way of life that measurably improves preparedness for a catastrophic cyber disaster:** Finally, we are focusing our energies on cyber-preparedness. Our programs in the coming years will seek to inculcate to change behavior as we continue to leverage our government partners to help continue efforts in these other areas. Awareness and education in the past decade have focused on large segments of the population, including home users and students in K-12. We hope to develop additional awareness programs that look more carefully at catastrophic cyber risk and continue to leverage our government partners to help advance our efforts in these other areas.

Organizational Framework

The three strategic goals outlined above will require clear organizational directions and programs.

HSPD-7 directs the Department to establish an organization dedicated to cyber security. The Preparedness Directorate's National Cyber Security Division (NCSD) has been that organization since it was created in June 2003. Since its inception, the NCSD has taken on the broad mandate of HSPD-7 and those provided in the President's National Strategy to Secure Cyberspace, in its mission to work collaboratively with private, public and international entities to secure cyberspace and America's cyber assets.

The NCSD is just one of the valuable preparedness resources within the Department. As part of the Preparedness Directorate, the NCSD works closely with the Office of the Manager of the National Communications System (NCS), which addresses national security and emergency preparedness (NS/EP) telecommunications. These two entities comprise what is now the Office of Cyber Security and Telecommunications. The Office of Cyber Security and Telecommunications works closely with the Office of Infrastructure Protection to ensure that the ever increasing interconnected nature of physical and cyber security is integrated throughout our overall preparedness efforts.

The National Communications System consists of 23 Federal departments and agencies with assets, resources, requirements and/or regulatory authority regarding national security and emergency preparedness (NS/EP) communications. Established pursuant to Executive Order 12472, the community is administered by DHS as Executive Agent and Manager and it supports the Executive Office of the President (the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget) in the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.

Executive Order 12472 also mandates inclusion of an industry component, the National Coordinating Center (NCC) for Telecommunications, or NCC Watch, a joint industry/Government body operating a 24 hour, 7-day a week watch center to coordinate NS/EP communications activities. The NCC Watch has a unique relationship with members of the private telecommunications sector in the

Communications Information Sharing and Analysis Center (ISAC). The Communications ISAC provides an opportunity for private sector industry to partner with government to exchange information and coordinate restoration of communications assets and services during emergencies. In this role, the NCC Watch communicates daily and shares a web-portal with NCSD (US-CERT) on cyber related issues.

To meet its mission, the NCSD is focused on leading a cyber risk management program, and building and enhancing the National Cyberspace Response System. To address these priorities, the NCSD is engaged in a public-private partnership which is incorporated into all of NCSD's programs. This is especially critical since the vast majority of our national assets and critical infrastructure are owned and operated by the private sector.

National Cyber Risk Management Program

The National Cyber Risk Management Program reflects the Department's overall strategic approach that is focused on risk management, as outlined in the National Infrastructure Protection Plan (NIPP). The NIPP incorporates the Department's overall risk management framework to assess and reduce our cyber risk, and improve our planning for response, recovery, and reconstitution of our critical networks.

- The Department released the NIPP on June 30 of this year after consultation with industry. The NIPP formalizes the collaboration between government and industry through the Sector Partnership Model with Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC) working together to address risk by analyzing consequences, vulnerabilities, and threats.

- The NIPP provides a unifying structure for protection of the Nation's 17 critical infrastructure and key resources (CI/KR) sectors designated in HSPD-7, including the Information Technology Sector and the Internet. The NIPP calls upon each sector to develop a Sector Specific Plan based on the risk management framework. DHS is the Sector Specific Agency (SSA) responsible for both the Information Technology Sector and the Communications Sector, and assists other sectors with the cyber elements of their infrastructure. The NCSD works closely with the IT Sector Coordinating Council, which was formally launched in January of this year. The IT-SCC and IT-GCC are working together on the IT Sector Specific Plan, which will be completed at the end of the year.

- In order to accomplish the risk management objectives of the NIPP, we have been working closely with the private sector to build the framework required. To facilitate the development of this partnership, the Department has established the Critical Infrastructure Partnership Advisory Council (CIPAC). The CIPAC comprises representatives from each of the critical infrastructure and key resources (CI/KR), sectors, SCCs, and GCCs, and provides a mechanism for the information exchange and collaboration between industry and government that is so crucial to understanding the risk we face. The Council also prioritizes the protective measures that need to be taken to reduce that risk.

As we develop the IT Sector Specific Plan and deepen our collective understanding of the cyber risks in other sectors, we are building the foundation for the development of a national cyber risk assessment. Working with our government and private sector partners, we are taking steps, such as developing attack scenarios and conducting red cell workshops and exercises, to identify what we are most concerned about in cyberspace, and then using that information to build our response and mitigation plans. As part of our risk management efforts, we have three priority mitigation programs.

First, as discussed above, the Office of Cyber Security and Telecommunications has established an IDWG to address the resiliency and recovery of Internet functions in the event of a major cyber incident. The IDWG is working with government, private sector, academic and international security experts to examine risks, improve preparedness and situational awareness, and identify measures that we can take to protect against nationally significant Internet disruptions. The IDWG conducted a tabletop exercise in June to examine the kinds of scenarios that would have significant impact on the Internet, understand when information exchange between the public and private sector is mutually beneficial, and to determine what roles and responsibilities industry and government should assume in responding to and recovering from such disruptions.

Second, the NCSD is collaborating with the national laboratories for its Control Systems Security Program to bring together government, industry, and academia to address the threats and vulnerabilities of the process control systems that remotely operate and control access to many of our critical infrastructure assets and systems. To support the Program, NCSD has established a US-CERT Control Systems Security Center, which is an assessment and incident response facility located at Idaho National Laboratory. The department also partners with the

industry sectors that utilize process control systems in their operations through the Process Control Systems Forum, or "PCSF". The PCSF met recently in San Diego and furthered its work to accelerate the security of control systems, provide a venue for sharing perspectives on cross-sector security issues, and facilitate solution-driven collaborative workshops.

Through the Process Control Systems Forum (PCSF), the Department also partners with the industry sectors that utilize process control systems in their operations. The PCSF met recently in San Diego and furthered its work to accelerate the security of control systems, provide a venue for sharing perspectives on cross-sector security issues, and facilitate solution-driven collaborative workshops.

The third risk mitigation effort is NCSD's Software Assurance Program that seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products and tools to analyze systems for hidden vulnerabilities. In collaboration with industry, academia, and government partners, the Department's approach to addressing software assurance identifies the following as keys to success:

- People – education and training for developers and users
- Processes – practical guidelines and best practices for the development of secure software
- Technology – tools for evaluating software vulnerabilities and quality
- Acquisition – specifications and guidelines for acquisition and outsourcing

To further its efforts, the Software Assurance Program holds semi-annual Software Assurance Forums with other Federal agencies, industry, academia, and international entities to facilitate ongoing collaboration and progress. As part of the program, NCSD has launched "Build Security In" to raise awareness and foster collaborative efforts.

The Office of Management and Budget (OMB) has recently designated NCSD as the Managing Agency for the Information Systems Security Line of Business. As part of NCSD's work with the Federal government, NCSD is currently working to establish a Program Management Office for this government-wide initiative which has an overarching goal of improving the effectiveness and consistency of systems security across the Federal enterprise. This effort will reduce costs through consolidation and standardization of resources. DHS will be working closely with partner agencies in overseeing the implementation of information systems security products and services.

In order to reduce our collective cyber risk we need to raise awareness of cyber security vulnerabilities and understand what we must do as individuals to create a collective, shared secure cyber infrastructure.

NCSD's awareness program leverages partnerships with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the National Cyber Security Alliance (NCSA), as well as our own National Cyber Alert System to reach state and local governments, small businesses, home users, and K-12 and higher education audiences. October is National Cyber Security Awareness Month. In October 2005, together with our state government and industry partners, we reached millions of Americans with a public service announcement, a satellite media tour on how to avoid identity theft in cyberspace, a national cyber awareness webcast for fourth and fifth graders, and many other activities. We look forward to making this year's campaign even more successful.

Cyber space is borderless, and as such, managing cyber risk needs to take into account international activities. NCSD has an international affairs program that seeks to address cyber security globally through cooperation and collaborative action toward building and leveraging the relationships needed to prevent, protect against, respond to and recover from cyber incidents and reduce overall cyber risk.

National Cyberspace Security Response System

There are three elements to the National Cyberspace Security Response System: the U.S. Computer Emergency Readiness Team Operations, or "US-CERT Ops"; the National Cyber Response Coordination Group, or "NCRCG"; and our regional preparedness and recovery efforts.

The first key element, US-CERT, was established in 2003 as a partnership between the Department and the public and private sectors to protect the nation's critical infrastructure and coordinate defense against and responses to cyber attacks. The US-CERT public website, http://www.us-cert.gov, the secure portal for stakeholders, and the National Cyber Security Alert System, provide timely, actionable information to technical and non-technical users. We encourage each of you to sign up for the US-CERT cyber alerts by going to http://www.us-cert.gov.

NCSD/US-CERT has an Operations component, which manages many aspects of the Cyberspace Security Response System, including situational awareness, incident handling and response, malicious code analysis, and strategic operations. Under Federal Information Security Management Act guidelines, OMB requires all Federal civilian agencies to notify US-CERT of any data breaches, unauthorized access, or

suspicious activity, including the loss of personally identifiable information within one hour of discovery.

US-CERT maintains a 24x7 secure Watch center; acts as a trusted third party to assist in the responsible disclosure of vulnerabilities; develops and participates in regional, national, and international level exercises; supports forensic investigations with recursive analysis on artifacts; provides malware (software that is designed to infiltrate or damage a computer system, without the owner knowing) analytic and recovery support for government agencies; coordinates Federal programs of computer emergency response teams and Chief Information Security Officer peer groups for sharing cyber incident information, best practices, and other cyber security information; and, collaborates with national and international computer security incident response teams both in the US and abroad. US-CERT's efforts in these and additional areas build our cyber situational awareness capabilities that allow us to prepare for and defend against cyber attacks, while also enhancing our ability to respond to the attacks.

US-CERT has established the Government Forum of Incident First Response Teams (GFIRST), a community of Federal agency incident response teams, which comprises the government's critical group of cyber first responders. GFIRST meets regularly, and we have hosted two GFIRST conferences to enhance information sharing and collaborative efforts to secure government cyberspace. US-CERT provides an Internet Health Service tool to GFIRST members through the US-CERT secure portal. IHS is a web-based application that provides members with access to several commercially available Internet and security products for use in building their situational awareness capabilities through the monitoring of their respective networks and the overall health of the Internet. In addition, as part of our Situational Awareness Program, US-CERT also leverages information technology for the automated sharing of critical information across the Federal government and analysis of traffic patterns and behavior.

US-CERT has developed a set of informational resources that it provides to our public and private sector stakeholders, including alerts, vulnerability notices, current activity reports, Federal Information Notices provided to the GFIRST community and Critical Infrastructure Information Notices provided to the private sector Information Sharing and Analysis Centers. In addition, US-CERT runs the National Cyber Alert System and the public website reference above, which provide cyber security tips, guidance, and other resource materials to technical and non-technical audiences.

The second key element of the National Cyberspace Security Response System is the National Cyber Response Coordination Group, or "NCRCG". NCSD co-chairs the NCRCG with its counterparts in the Department of Justice and the Department of Defense. The NCRCG includes 13 agencies with responsibility for and capabilities in cyber security matters and works to coordinate national response activities to incidents of national significance. The NCRCG meets monthly to prepare for cyber issues through tabletop exercises and working groups.

In addition to the IDWG's efforts and US-CERT Operations incident handling and analysis functions, the NRP's Emergency Support Function 2 (ESF-2) for Communications, led by NCS, is a critical component of advanced planning and ensuring coordinated recovery efforts. When ESF- 2 is activated, the Manager of the NCS ensures appropriate NS/EP communications support to operations conducted under the NRP. As part of ESF-2, NCSD works closely with NCS on preparing for recovery and reconstitution of critical communications networks and services. In preparation for this year's hurricane season, we have held ESF-2 training and exercise sessions with participation by many Federal agencies and organizations. We have created and published an ESF-2 Operational Plan and a Standard Operating Plan for ESF- 2 supporting agencies to enhance understanding across the spectrum of public and private sector entities that participate in recovery and reconstitution efforts. We have hired two Regional Communications Coordinators for Federal Regions IV and VI communications pre planning with state emergency planners. The NCS has also created more analytical tools for predictive and post-impact analysis.

One of the critical parts of ESF-2 is a management function to coordinate and facilitate the handling of private sector donations for recovery and reconstitution efforts in the immediate aftermath of a disaster such as Hurricane Katrina. We are working with our private sector stakeholders and state and local government partners to establish a set of requirements for such donations in order to match those needs with the products and services available.

The third key element of the National Cyberspace Security Response System is our regional preparedness and recovery efforts. Our regional efforts have greatly improved DHS's ability to incorporate the work of our government and private sector stakeholders at both the state and local levels. The Pacific Northwest Economic Region and the Gulf Coast Region are increasingly coordinating their efforts as a result of exercises held in the respective regions, and we are working with them to continue their preparedness planning for both cyber security events, and manmade or natural disasters that have a cyber impact. In addition, we are working with our industry stakeholders in the IT-SCC and IT

Information Sharing and Analysis Center) to develop plans for industry assistance in the event of an incident that requires surge support to recover and reconstitute critical IT systems. These efforts depend greatly on our partnerships with the full spectrum of affected industries, state and local government stakeholders, and the emergency response community.

Recent Success Stories

I would like to take this opportunity to highlight two recent success stories in our comprehensive cyber security efforts. First, we conducted the first National Cyber Exercise organized and sponsored by the Federal government. Conducted in February 2006, "Cyber Storm" was the largest multinational, cross-sector cyber exercise to date and assessed policies and procedures associated with a cyber-related incident of national significance, as outlined in the National Response Plan's Cyber Annex. The exercise tested, for the first time, the full range of cyber-related response policy, procedures, and communications methods required in a real world crisis.

Cyber Storm exercised the responses of over 100 public and private agencies, associations, and corporations in over 60 locations and five countries. It achieved collaboration in crisis response at operational, policy, and public affairs levels, including participation of more than 30 private sector corporations and associations in the planning, executing, and after action analysis of a federally funded and congressionally mandated emergency response exercise. As mentioned earlier, Cyber Storm exercised the NCRCG as the principal Federal mechanism for coordinating the national response to a cyber incident of national significance. Cyber Storm demonstrated the close cooperation and information sharing needs across Federal agencies, across boundaries, and between the public and private sectors.

First, the exercise reinforced the importance of defining roles and responsibilities, processes and procedures and having strong communications and coordination among the cyber community. In addition, it highlighted the importance of coordinating and integrating incident communications and public affairs outreach. Unlike a physical, self-announcing incident, a set of cyber attacks such as those imagined in the Cyber Storm scenario are not immediately apparent, either in occurrence or attribution. The correlation of multiple incidents proved challenging for our players, and only further demonstrated the importance of public-private relationships and the need to provide on-going training activities, discussions, and exercises to further build those relationships to strengthen our collective response to a cyber incident.

We are currently making improvements to our policies and procedures to address key findings, and have begun the planning process for Cyber Storm 2, which is slated for 2008.

A second accomplishment falls in the international arena. At the end of June, we successfully hosted here in Washington the second multilateral conference on the development of an International Watch and Warning Network, or "IWWN", among 15 countries in the Americas, Europe, and Asia Pacific. The country participants included representatives from their government critical information infrastructure protection organizations, their computer security incident response teams, and their law enforcement agencies with responsibility for cyber crime. The IWWN was established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities. The June conference established a clear path forward for the IWWN community to enhance global cyber situational awareness and incident response capabilities and marked the launch of a secure Internet portal to facilitate ongoing international information sharing as well as coordination during cyber incidents.

The Road Ahead

As we further develop our programs and leverage our recent successes, there are some efforts we need to undertake in the near term with our industry and agency partners to better prepare ourselves to respond to, and recover from, cyber incidents. These efforts include, but are not limited to:

- Further integration of the cyber security and telecommunications efforts in the Department and with industry to reflect increasing convergence in the sectors;
- Clearer articulation of roles and responsibilities in the public-private partnership for information sharing and incident response through coordinated concept of operations and standard operating procedures;
- Development of the IT Sector Specific Plan in the NIPP risk management framework;
- Development of a national cyber risk assessment based upon the cross sector cyber component of the NIPP risk management framework;
- Share aggregated situational awareness across the civilian agencies, the military, the international community, and the private sector; and
- Further collaboration between US-CERT Operations and the Department of Defense's Joint Task Force-Global Network

Operations to leverage our respective expertise and capabilities toward common cyber security objectives.

These efforts are being undertaken in the Cyber Storm After Action planning, the NIPP process, our international engagements, and our collaboration with industry on all of our programs. These action plans have defined benchmarks and milestones to drive and track our progress in each of these areas.

Conclusion

The National Cyber Security Division has established its mission and priority objectives, developed a strategic plan, and undertaken significant steps to implement its strategic plan across the programs outlined here. In this ever-evolving environment, we know that the target will shift to accommodate new threats, new vulnerabilities, and new technologies. We need to be flexible enough to adjust our efforts to meet these new challenges.

Our progress to date is tangible: we have a construct for public-private partnership; we have a track record of success in our cyber operations; we have established relationships at various levels to manage cyber incidents; we have built international communities of interest to address a global problem; and we have tested ourselves at a critical development stage and will continue to examine our internal policies, procedures, and communications paths in future exercises. We are building on each of these achievements to take further steps to increase our cyber preparedness and improve our response and recovery capabilities.

I would like to thank the Subcommittee for its time today and I appreciate this opportunity to bring further transparency to these important cyber security priorities.