Written Statement of
Donald (Andy) Purdy, Jr.
Director (Acting), National Cyber Security Division
Information Analysis and Infrastructure Protection Directorate
U.S. Department of Homeland Security

Subcommittee on Federal Financial Management, Government Information, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

July 19, 2005

Good morning Chairman Coburn and distinguished members of the Subcommittee. My name is Andy Purdy, and I am the Acting Director of the National Cyber Security Division (NCSD) within the Department of Homeland Security. I am delighted to appear before you today to share with you the work of the NCSD and those with whom we are partnering to secure our national cyberspace and critical information infrastructure. In my testimony today, I will provide an overview of NCSD, our operating mandates, our mission and goals, our priorities, and the programs in which we are engaged to meet those missions and goals. Much of the information in my testimony today is reflected in the recent Government Accountability Office (GAO) report 05-434, which focused on cyber security responsibilities and in our response.

Introduction: DHS and Cyber Security

As you may know, Secretary Chertoff has proposed a new Assistant Secretary for Cyber Security and Telecommunications as part of his six point agenda for the Department, announced on July 13th. As it currently stands in DHS, the core cyber security activity is located in the Information Analysis and Infrastructure Protection (IAIP) Directorate. The IAIP Directorate includes the Office of the Chief of Staff; the Information Sharing and Collaboration Office (ISCO); the Office of Information Analysis (IA), the primary gathering and analytic center for threat information and intelligence within DHS; the Homeland Security Operations Center (HSOC), the primary national-level hub for domestic operational situational awareness, common operational picture, communications, information fusion, and coordination pertaining to the prevention of terrorists attacks and domestic incident management; and the Office of Infrastructure Protection (IP). The Office of Infrastructure Protection has four component divisions, including the Infrastructure Coordination Division (ICD), the Protective Security Division (PSD), the National Communications System (NCS), and the National Cyber Security Division (NCSD). Within the Directorate, IA, IP, and the HSOC work together to share intelligence and other information as well as to coordinate our efforts to mitigate our vulnerabilities.

In today's highly technical and digital world, we recognize that attacks against us may manifest in many forms, including physical and cyber. 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 critical infrastructure makes it difficult – not to mention irresponsible – to attempt to address the protection of our physical and cyber assets in isolation.

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 approaches.

NCSD was created in June 2003 to serve as a national focal point for cyber security and to coordinate implementation of the *National Strategy to Secure Cyberspace* ("the Strategy") issued by President Bush in February 2003 that set out a national framework for addressing various aspects of cyber security. The Strategy established the following five national priorities for securing cyberspace:

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

In December 2003, President Bush further solidified NCSD's mandate as a national focal point for cyber security by issuing Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7), which calls for DHS to "…maintain an organization to serve as a focal point for the security of cyberspace…."[1] HSPD-7 also established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Furthermore, HSPD-7 laid out how DHS should address critical infrastructure protection, including "…a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources.[2]

To meet this mandate, IP embarked on the development of the National Infrastructure Protection Plan (NIPP) that will serve to address critical infrastructure protection in the seventeen (17)[3] identified critical infrastructure sectors and key resource sectors. The interim NIPP issued in February 2005 encompasses a risk management framework for public and private sector stakeholders to work together to identify critical assets in each of the sectors, prioritize them, conduct vulnerability assessments in each of the prioritized sectors including identification of interdependencies among them, and provide priority protective measures that owners and operators of those assets should undertake to secure them. The final NIPP is expected to be released later this year.

HSPD-7 outlines "Sector Specific Agencies" (SSAs) for each of the critical infrastructure sectors, with DHS serving as the overall coordinator for the NIPP program. The private sector-

[1] Homeland Security Presidential Directive 7, December 17, 2003; http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html; Para (16).
[2] Homeland Security Presidential Directive 7, December 17, 2003; http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.
[3] The NIPP identifies the following Critical Infrastructure Sectors and Key Resources: Food and Agriculture; Public Health and Healthcare; Drinking Water and Wastewater; Energy; Banking and Finance; National Monuments and Icons; Defense Industrial Base; Information Technology; Telecommunications; Chemical; Transportation Systems; Emergency Services; Postal and Shipping; Dams; Government Facilities; Commercial Facilities; Nuclear Reactors, Materials, and Waste.

led Sector Coordinating Councils (SCCs) and/or Information Sharing and Analysis Centers (ISACs) work with each SSA; and the SSA's are the chairs of the respective Government Coordinating Councils(GCC), which represent the government agencies that have a role in protecting the respective sectors. DHS SSA responsibilities include the Information Technology Sector and the Telecommunications Sector. Specifically, NCSD coordinates the Information Technology Sector, and the NCS coordinates the Telecommunications Sector. Reflecting the increasing convergence between these two communications sectors in today's market, NCSD and NCS work together closely to coordinate all efforts to protect the nation's critical cyber systems and the telecom transport layer. In addition to its IT sector responsibility, NCSD is responsible for providing cyber guidance to all sectors to include the information infrastructure vulnerabilities they may have as well.

Given today's interconnected environment and DHS's integrated risk-based approach to critical infrastructure protection, NCSD's mission is to work collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. To meet that mission, NCSD developed a Strategic Plan that establishes a set of goals with specific objectives for each goal and milestones associated with each objective. The Strategic Plan goals, which are closely aligned with the *National Strategy to Secure Cyberspace*, HSPD-7, the interim NIPP, and the Cyber Annex to the National Response Plan, are as follows:

1. Establish a National Cyberspace Response System to prevent, detect, respond to, and reconstitute rapidly after cyber incidents;
2. Work with public and private sector representatives to reduce vulnerabilities and minimize severity of cyber attacks;
3. Promote a comprehensive awareness plan to empower all Americans to secure their own parts of cyberspace;
4. Foster adequate training and education programs to support the Nation's cyber security needs;
5. Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace; and
6. Build a world class organization that aggressively advances its cyber security mission and goals in partnership with its public and private stakeholders.

To meet these goals, NCSD is organized into four operating branches: (1) U.S. Computer Emergency Readiness Team (US-CERT) Operations to manage the 24x7 threat watch, warning, and response capability that can identify emerging threats and vulnerabilities and coordinate responses to major cyber incidents; (2) Strategic Initiatives to manage activities to advance cyber security in critical infrastructure protection, control systems security, software development, training and education, exercises, and standards and best practices; (3) Outreach and Awareness to manage outreach, cyber security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders; and (4) Law Enforcement and Intelligence to coordinate and share information between these communities and NCSD's other constituents in the private sector, public sector, academia, and others, and also to coordinate interagency response and mitigation of cyber security incidents. Together, these branches make up NCSD's framework to address the cyber security challenges across our key stakeholder groups and build communications, collaboration, and awareness to further our

collective capabilities to detect, recognize, attribute, respond to, mitigate, and reconstitute after cyber attacks.

Cyber Security Priorities: Response and Risk Management

The *Strategy* and HSPD-7 provide NCSD with a clear operating mission and national coordination responsibility. To carry out the mission and those related responsibilities, NCSD has identified two overarching priorities: to build an effective national cyberspace response system and to implement a cyber risk management program for critical infrastructure protection. Focusing on these two priorities establishes the framework for securing cyberspace today and a foundation for addressing cyber security for the future.

Priority 1 – Cyber Incident Management: A National Cyberspace Response System

A core component of NCSD and our effort to establish a National Cyberspace Response System is the US-CERT Operations Center. US-CERT was established in September 2003 as a partnership between DHS and the public and private sectors to address cyber security issues. Beginning as an initial partnership with the Computer Emergency Response Team Coordination Center (CERT/CC) in Carnegie Mellon University's Software Engineering Institute, 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 from the cyber consequences of physical attacks or natural disasters.

US-CERT has four major programs of activity. First, US-CERT is DHS's 24x7x365 cyber watch, warning, and incident response center, and provides coordinated response to cyber incidents, a web portal for secure communications with private and public sector stakeholders, a daily report, a public website (http://www.us-cert.gov/), and a National Cyber Alert System, which provides timely, actionable information to the public on both technical and non-technical bases. Second, US-CERT conducts malicious code analysis, provides malware technical support, and conducts cyber threat and vulnerability analysis. Third, US-CERT manages a situational awareness program that includes the Einstein Program for monitoring network activity in the federal agencies, currently operational at three agencies, with five pending deployments within the next four to six months; and, an Internet Health and Status service used by 50 government agency computer security incident response teams. Fourth, US-CERT manages programs for communication and collaboration among public agencies and key network defense service providers. In line with NCSD's close working relationship with NCS, US-CERT works closely with the National Coordinating Center for Telecommunications (NCC) to address and mitigate cyber threats including response and recovery. U.S. CERT also maintains a presence in the HSOC to ensure coordination throughout DHS.

As noted, NCSD has initiated a number of activities specifically to assist federal agencies in protecting their cyber infrastructure. NCSD established the Government Forum of Incident

Response and Security Teams (GFIRST) to facilitate interagency information sharing and cooperation across federal agencies for readiness and response efforts. GFIRST is a group of technical and tactical practitioners of security response teams responsible for securing government information technology systems. The 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 basis; and
- Improve incident response operations.

GFIRST meets on a regular basis and held its first annual conference in April 2005 with more than 200 participants from federal, state, and local governments. The conference was a major success for US-CERT, and GFIRST has established further lines of communications across organizations. The technical workshops and speakers stimulated many technical interchanges regarding cyber first responder activities. In another step forward, GFIRST held its first classified threat briefing with DHS IA, the Central Intelligence Agency, Department of Defense, and National Security Agency in June 2005.

US-CERT utilizes a secure collaboration platform, which is being intergrated into the Homeland Security Information Network (HSIN), to support cyber information sharing and collaboration among the GFIRST community, and other communities, such as the ISACS. This secure platform bridges the gap between Government participants as well as participants from the ISAC and other private sector partners.

In addition to GFIRST, NCSD worked with DOD and DOJ to help form the National Cyber Response Coordination Group (NCRCG) to provide a federal government approach to coordinated cyber incident response. We created a Cyber Annex to the recently issued National Response Plan (NRP)[4] that provides a framework for responding to cyber incidents of national significance. As such, the Cyber Annex formalized the NCRCG as the principal federal interagency mechanism to coordinate preparation for, and response to, cyber incidents of national significance. The co-chairs of the NCRCG are DHS/NCSD, the Department of Justice, and the Department of Defense. An additional 13 federal agencies with a statutory responsibility for and/or specific capability toward cyber security, including the intelligence community, comprise the membership. NCSD serves as the Executive Agent and point of contact for the NCRCG. The NCRCG has developed a concept of operations (CONOPS) for national cyber incident response that will be examined in the National Cyber Exercise, *Cyber Storm,* to be conducted by NCSD in November 2005 with public and private sector stakeholders.

In addition to its CONOPS and incident response mechanism, the NCRCG is reviewing capabilities of federal agencies from a cyber defense perspective to better leverage and

[4] *http://www.dhs.gov/dhspublic/display?theme=15&content=4269*

coordinate the preparation for and response to significant cyber incidents. This effort will entail the following components:

- Mapping the current capabilities of government agencies related to cyber defense relative to detection and recognition of cyber activity of concern, attribution, response and mitigation, and reconstitution;
- Identifying capabilities within the government that US-CERT should leverage to maximize interagency coordination of cyber defense capabilities;
- Performing a gap analysis to identify the surge capabilities for possible leverage by or collaboration with the US-CERT for cyber defense issues in order to detect potentially damaging activity in cyberspace, to analyze exploits and warn potential victims, to coordinate incident responses, and to restore essential services that have been damaged; and
- Consider establishing formal resource sharing agreements with the other agencies per the cyber defense coordination needs identified through the process identified above.

Finally, NCSD has been supportive of the Department of Commerce's (DOC) efforts related to Internet Protocol version 6 (IPv6).[5] The NCSD funded the IPv6 Task Force co-chaired by National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA) in conducting an economic study of issues related to IPv6 deployment. The draft report, entitled "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)" opened for Federal Register comment in January 2005, and the DOC is holding a public meeting on July 28, 2005 to solicit additional input from stakeholders who may potentially be impacted by the report findings.

In addition, the US-CERT has released six technical bulletins and advisories pertaining to IPv6 regarding current vulnerabilities that exist and potential issues concerning deployment of IPv6. While the IPv6 standard has yet to be widely deployed, there exist several potential security risks that must be properly recognized and managed. These bulletins and advisories offer technical security recommendations for firewalls, configurations, cyber incident handling, and other relevant guidance for securing IPv6 enabled systems. DHS is supportive of OMB's efforts to facilitate the migration of federal agencies to IPV6 compatibility.

With our efforts, accomplishments, and on-going programs, NCSD has made significant progress in managing cyber incidents and has taken substantial strides toward building a National Cyberspace Response System; however, much remains to be done.

Priority 2 – Cyber Risk Management: Assessing the Threat and Reducing the Risk

[5] The IP is a technical standard that enables computers and other devices to communicate with each other over networks, many of which interconnect to form the Internet. The current generation of IP, version 4 (IPv4) has been in use for more than 20 years. Through the guiding efforts of the Internet Engineering Task Force (IETF), a new version of IP, version 6, has been developed. Advantages of IPv6 over IPv4 include availability of more Internet addresses and additional user features and applications.

NCSD incorporated the risk management framework set out in HSPD-7 and the resulting interim NIPP into its effort to better assess the threats and reduce the vulnerabilities to our national cyberspace, and to mitigate and manage the consequences of a cyber attack. The NIPP Risk Management Framework entails a collaborative partnership among the private sector and federal, state, and local governments looking at people, cyber, and physical assets to identify and prioritize assets, assess vulnerabilities, and coordinate the protection of critical infrastructure and key resources.

With regard to assessing the risk, NCSD collaborates with the law enforcement and the intelligence communities in a number of ways. DHS assisted in the coordination of cyber-related issues for the "National Intelligence Estimate (NIE) of Cyber Threats to the U.S. Information Infrastructure." The resulting classified document issued in February 2004 details actors (nation states, terrorist groups, organized criminal groups, hackers, etc.), capabilities, and intent (where known). In addition, NCSD has infused cyber requirements into the Standing Information Needs (SINs) and Priority Information Needs (PINs) for the intelligence community and continues to collaborate with them through IA to characterize cyber threats for accuracy. Finally, the NCRCG includes law enforcement and intelligence agencies and has working groups addressing botnets and attribution issues.

There are four major components to NCSD's approach to reducing vulnerabilities. The central element of our approach is the cyber component of the NIPP. The other three key elements are the Internet Disruption Working Group (IDWG), the Control Systems Security Program, and the Software Assurance Program.

As I indicated, DHS is the SSA with NCSD as the lead for the Information Technology (IT) Sector and works with the Information Technology Information Sharing and Analysis Center (IT-ISAC) and the newly established Information Technology Sector Coordination Council (IT-SCC) supporting the NIPP framework. This public-private partnership is a crucial component of the NIPP framework, as more than 85 percent of the critical infrastructure is owned and operated by the private sector. In addition to its responsibility to work with the IT Sector to identify critical assets, assess vulnerabilities, and determine protective measures, NCSD is ensuring that cyber is comprehensive throughout the NIPP by providing guidance to the other critical infrastructure sectors in identifying, assessing, and protecting their cyber assets and cyber components of physical assets. This guidance includes contributing cyber elements to the NIPP Base Plan, reviewing the cyber aspects of Sector Specific Plans (SSPs), and delivering cyber CIP training to SSAs and SSP authors to help them enhance the cyber aspects of their SSPs, all of which are underway in NCSD.

Protection of critical cyber assets goes hand-in-hand with protection of critical telecommunications assets; accordingly, NCSD and NCS are working closely together to collaborate on issues related to threats, identification of critical cyber assets, vulnerability and risk assessments, and development of appropriate protective measures. Within the NIPP framework, NCSD and NCS established the Internet Disruption Working Group (IDWG) in December 2004 to address the resiliency and recovery of Internet functions in case of a major cyber incident. The Department of Treasury and the Department of Defense are also engaged, and the working group is acting to extend the partnership to representatives from the private

sector as well as international stakeholders. The IDWG reflects the convergence of telecommunications and information technology sectors in today's environment and the emergence of Next Generation Networks (NGN) that will compose the Internet of the future. An initial focus of the working group is to identify near term actions related to situational awareness, protection, and response that government and its stakeholders can take to better prepare for, protect against, and mitigate nationally significant Internet disruptions.

Future milestones for NCSD's CIP / Cyber Security Initiatives include efforts to:

- Develop IT Sector vulnerability assessment methodology and compile vulnerability assessment information;
- Define IT Sector specific metrics;
- Submit FY06 IT Sector Plan, subject to NIPP Council requirements;
- Compile FY06 IT Sector asset list and conduct FY06 asset prioritization; and,
- Develop, test, and publish cross-sector vulnerability assessment requirements as best practice.

The interdependency between physical and cyber infrastructures is hardly more acute than in the use of control systems as integral operating components by many of our critical infrastructures. "Control Systems" is a generic term applied to hardware, firmware, communications, and software used to perform vital monitoring and controlling functions of sensitive processes and enable automation of physical systems. Specific control systems used in the various critical infrastructure sectors include Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS).

Examples of the critical infrastructure processes and functions that control systems monitor and control include energy transmission and distribution, pipelines, water and pumping stations, chemical processing, pharmaceutical production, rail and light rail, manufacturing, and food production. Increasingly, these control systems are implemented with remote access, open connectivity, and connections to open networks such as corporate intranets and the Internet. These sophisticated information technology tools are making our critical infrastructure assets more automated, more productive, more efficient, and more innovative, but they also may expose many of those physical assets to physical consequences from new, cyber-related threats and vulnerabilities.

To assure immediate attention is directed to protect these systems, NCSD established the Control Systems Security Program to coordinate efforts among federal, state, and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors. As part of this Program, NCSD developed a Control Systems Strategy that incorporates five highly integrated goals to address the issues and challenges associated with control systems security. As such, our control systems activities support NCSD's overall efforts to address cyber security across critical infrastructure sectors over the long term, as well as the US-CERT's capability in the management, response, and handling of incidents, vulnerabilities, and mitigation of threat actions specific to critical control systems functions.

NCSD also established the US-CERT Control Systems Security Center (CSSC) in partnership with Idaho National Laboratory (INL) and other DOE National Laboratories[6], the British Columbia Institute of Technology, and the private sector in June 2004. Since its establishment, the CSSC has made considerable progress and some of its major accomplishments include:

- Established the US-CERT CSSC assessment and incident response facility located at INL and a US-CERT Support Operations Center for Control Systems;
- Established relationships with more than 25 potential industry partners and completed several agreements that established initial assessment, analysis, and vulnerability reduction plans within various industry sectors;
- Created the Gross Consequence Matrix to determine the industries of most concern, and a list of specific sites from the National Asset Database where Control Systems could cause a negative consequence due to failure or attack;
- Created a quantitative control systems cyber risk/decision analysis measurement methodology; and,
- Established the Process Control System Forum (PCSF) (in partnership with DHS's Science and Technology Directorate) to accelerate the development of technology that will enhance the security, safety, and reliability of Control Systems, including legacy installations.

Future milestones for NCSD's Control Systems Security Program include efforts to:

- Develop a comprehensive set of control systems security assurance levels for owners and operators;
- Sponsor government/industry workshops to increase awareness among control systems owners and operators of potential cyber incident impacts and vulnerabilities;
- Develop, populate, and validate control systems security scenario assessment tools to provide response teams a web-based application to assess impacts;
- Assess a minimum of three core systems and provide solutions to vulnerabilities and recommendations to protect against cyber threats; and,
- Develop the US-CERT CSSC web page for information exchange.

The fourth major component of NCSD's cyber risk management program is our Software Assurance Program. Software is an essential component of the nation's critical infrastructure (power, water, transportation, financial institutions, defense industrial base, etc); however, defects in software can be exploited to launch cyber attacks as well as attacks against the critical infrastructure. NCSD developed a comprehensive software assurance framework that addresses people, process, technology, and acquisition throughout the software development lifecycle.

As part of the shared responsibility approach to cyber security, DHS is working to achieve a broader ability to routinely develop and deploy trustworthy software products. As such, DHS is shifting the security paradigm from "patch management" to "software assurance" by

[6] Idaho (INL), Pacific Northwest (PNNL), Los Alamos (LANL), Argonne (ANL), Sandia (SNL), Savannah River (SRNL)

encouraging U.S. software developers to raise the bar on software quality and security. In collaboration with other federal agencies, academia, and the private sector, we are:

- Sponsoring the development of a repository of best practices and practical guidance for the software development community;
- Developing a software assurance common body of knowledge from which to develop curriculum for education and training;
- Facilitating discussions with industry and academic institutions through Software Assurance Forums (held in August 2004 and April 2005). The next forum is scheduled for October 2005;
- Collaborating with NIST to inventory software assurance tools and measure effectiveness, identify gaps and conflicts, and develop a plan to eliminate gaps and conflicts;
- Completing the DHS/Department of Defense co-sponsored comprehensive review of the National Information Assurance Partnership (NIAP)[7] with the draft report to be published in September 2005; and
- Promoting investment in applicable software assurance research and development.

DHS will seek to reduce risks by raising the level of trust for all software, minimizing vulnerabilities and understanding threats. DHS will collaborate with government, industry, academic institutions, and international allies to achieve these software assurance objectives.

Moving Forward

We have studied the recent GAO report on critical infrastructure protection. We believe it has provided a fair assessment of the progress to date and agree that while considerable work has been done, much work remains to meet the challenges in this rapidly changing area. With the proposed appointment of a new Assistant Secretary for Cyber and Telecommunications Security, we are confident that we will accelerate our cyber security efforts.

Secretary Chertoff's recent release of the findings from his "Second Stage Review" of the entire Department illustrates DHS commitment to addressing leadership and organizational concerns that have been similarly raised by GAO.

We, tentatively, have identified three priority areas for collaboration with stakeholders that we will socialize with our public and private stakeholders in the next few weeks. These priority areas include information sharing, preparedness, and recovery. As part of that engagement, we will discuss our suggestion that the first priority should be to enhance preparedness collaboration by identifying the most significant cyber attack scenarios.

[7] The National Information Assurance Partnership, established in August of 1997, is a joint effort between NIST and NSA to provide technical leadership in security-related information technology test methods and assurance techniques. NIAP uses the Common Criteria to evaluate and certify commercial off the shelf (COTS) products mainly for use by DoD and NSA. There has been much discussion in past years on the effectiveness (time and cost) of the NIAP process. As a result, the National Strategy to Secure Cyberspace recommended an independent review of the program be conducted to make recommendations for its improvement.

In connection with the interim National Infrastructure Protection Plan, we have begun our efforts to assess cyber threats and vulnerabilities, and identify significant interdependencies. These efforts will be fully implemented as the Sector Specific Agencies start implementing their portion of the NIPP. In partnership with NCS and other agencies we are working through the Internet Disruption Working Group to address the resiliency and recovery of internet functions in the case of a major cyber incident. We are working with the government, private sector, and academia to promote the integrity and security of software. We have planned a major exercise for later this year to test the Cyber Annex to the National Response Plan. Through this effort, we will pull together appropriate entities in the Federal government and appropriate private sector stakeholders to test our capabilities and, subsequently, to improve our incident management process.

We have also organized a Performance Metrics Team with internal representatives from all key substantive areas to ensure that each NCSD objective has associated metrics. We will seek private sector engagement in the development of metrics, including for cyber security preparedness. The Team will evaluate each objective to ensure the milestones and associated metrics are meaningful and capable of measuring performance and will develop measures to fulfill these needs.

We are committed to achieving success in meeting our goals and objectives, but we cannot do it alone. We will continue to meet with industry representatives, our government counterparts, academia, and state representatives to formulate the partnerships and leverage the efforts of all, so we, as a nation, are more secure in cyberspace.

Again, thank you for the opportunity to testify before you today. I would be glad to address you in the coming months on our progress and would now be pleased to answer any questions you have.