Statement for the Record
Gregory Garcia
Assistant Secretary for Cybersecurity and Communications
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on
Information Policy, Census, and National Archives
October 23, 2007

Good morning Mr. Chairman and Members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss the role of the Department of Homeland Security (DHS) and our efforts both within government and with the private sector to ensure the security and resilience of the cyber infrastructure, as well as Government's role in responding to significant incidents that may disrupt the functioning of the Internet.

Protecting the Nation's critical infrastructure and key resources (CI/KR) is among DHS' highest priorities. The Nation's CI/KR sectors rely on the availability and resilience of the Information Technology (IT) and Communications Sectors. We recognize that IT and communications play a central role in the command, control, and operations of government; the economy; and other critical infrastructures. The IT industry produces the hardware, software, and services that create the foundation of networks and systems. The communications industry provides the necessary infrastructure, technology, and services that enable the transmission of information essential for the successful execution of any organization's mission.

DHS recognizes the significance of the convergence of IT and communications through the Internet. In response, DHS created the Office of Cybersecurity and Communications (CS&C) within the Department, bringing together the National Cyber Security Division (NCSD), the National Communications System (NCS), and, more recently, the Office of Emergency Communications, under unifying leadership. NCSD and NCS work collaboratively with the IT and Communications Sectors and maintain both strategic and operational programs that seek to address the challenges associated with preventing and responding to a disruption of the Internet.

As the Assistant Secretary for Cybersecurity and Communications within DHS' National Protection and Programs Directorate, I oversee our mission to prepare for and respond to incidents that could degrade or overwhelm the operation of our Nation's IT and communications infrastructure. CS&C's strategic goals include preparing for and deterring catastrophic incidents by achieving a collaborative risk management and deterrence capability through a mature partnership between Government and the private sector. This strategic goal also encompasses tactical efforts to secure and protect the Nation's cyber infrastructure from attacks and disasters by identifying and mitigating threats, vulnerabilities, and consequences. CS&C's efforts have resulted in successful and timely responses to cyber incidents, the development of technological solutions to enhance our response and communications capabilities during incidents, and trusted

relationships and partnership mechanisms that facilitate preparedness and operational response activities.

Securing our Nation's Cyber Infrastructure

Multiple entities play a role in ensuring the security of our Nation's cyber infrastructure and in responding to significant incidents that threaten the functioning of the Internet. State and local governments are often owners and operators of network infrastructure. The private sector builds, owns, and operates most of the cyber infrastructure. The Federal Government has the responsibility of ensuring that government functions continue to operate, securing their timely restoration if they fail, and limiting any impact to national security, the economy, public health and safety and public confidence. Because so many organizations have significant roles in the protection of cyberspace, the key to success is strategic partnering.

Even though the private sector bears most of the responsibility for protecting the cyber infrastructure it owns, CS&C takes an active role in protecting and increasing the resilience of our Nation's cyber infrastructure. By building interagency and public-private partnerships for infrastructure protection and by facilitating efforts to raise cyber security awareness, identify cyber research and development requirements, exchange information, and manage cyber risk, CS&C has made significant advances in improving the security posture of our Nation's cyber infrastructure.

For example, through our Einstein program we have reduced the time it takes to gather and share critical data on cyber threats and attacks facing Federal networks. We can now obtain and share information in a matter of hours rather than days. Einstein is currently deployed in 13 Federal agencies, and CS&C is actively working to obtain memoranda of understanding with other agencies for its further deployment.

CS&C has provided resources to meet the training, education, and certification needs of IT security professionals, including development of an IT Security Essential Body of Knowledge, which was recently released for public comment through the Federal Register. Our efforts have also resulted in training nearly 7,000 IT and control systems professionals in the last year on a range of topics related to vulnerabilities, risk assessments, and standards-based mitigation measures. Working with our public and private sector partners, we have also developed common procurement language that owners and operators can incorporate into contracts to ensure the cyber security of the products and services they acquire. The long term goal is to raise the level of security through the application of robust procurement requirements. Our efforts have received very positive feedback from users, and our documents have averaged more than 450 downloads per month.

Preventing and Preparing for an Internet Disruption

We have also taken steps to minimize the impact of incidents with the potential to disrupt the functioning of the Internet. For example, we are developing a Priority Telecommunications Service (PTS) for operation in the next generation network (NGN) that will provide our Nation's leadership with the capability to communicate during network disruptions. CS&C's outreach

efforts for cyber security have had real-world outcomes: over one million people have signed up for our National Cyber Alert System and are receiving alerts, bulletins, and other information on cyber threats, vulnerabilities, and incidents, further enhancing our ability to prepare for and respond to Internet disruptions.

Further, our operational response centers, the United States Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center (NCC) for Telecommunications provide the detection, warning, and response capabilities necessary to coordinate public and private sector response to Internet disruptions in the U.S. and around the world. These entities gather information, identify sources of attacks, and share information with the private sector, Federal, State, and local government entities, and our international partners to take actions to neutralize attacks and to mitigate the consequences from attacks.

These operations centers demonstrate the value of the Federal role in response to an attack on the Internet. For example, in July 2007 the country of Estonia came under a national cyber attack from botnets, an automated computer program, that were flooding the country's IT systems with traffic, causing a denial of service for many of their government sites. The Estonian government contacted the U.S. Government as a North Atlantic Treaty Organisation (NATO) member for incident response assistance. US-CERT coordinated with its Federal, international, and private sector partners to identify over 2,500 unique sources of the attacking botnets originating from 21 NATO countries. US-CERT contacted U.S. Internet security providers and major telecommunications carriers to share information regarding U.S.-based Internet Protocol (IP) addresses involved in the attack. In addition, US-CERT provided NATO countries involved in the incident with information to assist military, intelligence, law enforcement, and computer emergency response team personnel responding to the incident in their respective countries.

The Estonia attack is one of many—from October 1, 2006, through August 31, 2007, US-CERT handled over 34,700 incidents, an 88 percent increase since US-CERT first began tracking incidents in 2005. This can be attributed to not only the increased attacks on the Nation's public and private networks but also increased situational awareness levels and reporter rates.

It is incumbent on the Federal Government to enable the development of mechanisms to ensure coordination and operational information sharing across various stakeholder communities and to facilitate appropriate preparedness activities in advance of a disruption, as well as the appropriate response activities should a disruption occur. Coordination and collaboration rely on meaningful and trusted partnerships, as well as on mechanisms and procedures tested across government and with industry. I will highlight in my testimony efforts to partner with the private sector and undertake activities to protect against Internet disruptions and to build and sustain capabilities to ensure a coordinated incident response.

Collaborative Efforts to Secure Cyberspace

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of CI/KR protection into a single national program so that investment across sectors is applied where it offers the most benefit for mitigating risk. Under the NIPP framework, the availability of the Internet and its associated services are identified as a shared key resource of

the IT and Communications Sectors, reflecting the convergence of voice and data communications networks and services.

Homeland Security Presidential Directive 7 designates DHS as the Sector Specific Agency (SSA) for both the Communications and IT Sectors. DHS has identified two of CS&C's components—NCS and NCSD—as the organizations to carry out the SSA responsibility for the Communications and IT Sectors, respectively. NCSD is also responsible for addressing the cyber element across all of the sectors. In May 2007, both the IT and Communications Sectors recently released their Sector Specific Plans (SSP), which are planning documents developed jointly by industry and government through the respective IT and Communications Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC). The SSPs focus on overall sector preparedness, including managing risk to the sectors' critical functions and infrastructures that support homeland, economic, and national security.

Public and private security partners worked together to define six critical sector functions in the IT SSP that support the sector's ability to produce and provide high assurance products, services, and practices that are resilient to threats and rapidly recovered. Of the six functions, two critical sector functions are related to the Internet: 1) Provide Internet-Based Content, Information, and Communications Services and 2) Provide Internet Routing, Access, and Connection Services. The IT SSP presents an approach for assessing risk to those functions, as well as the other four critical IT Sector functions.

Similarly, the Communications SSP addresses the identification of architectural elements of the Internet and the incorporation of specific components into the sector's national risk assessment process. Both plans include similar actions to facilitate additional IT and Communications sector collaboration to assess risk to the Internet. The two sectors are currently participating in each other's SSP implementation activities, including the respective risk assessment working groups. This collaboration provides an opportunity to assess both strategic and operational risks to the Internet and develop and implement short- and long-term protective measures as well as research and development requirements necessary to prevent a major Internet disruption.

Although the availability of the Internet and its associated services is the responsibility of the IT and Communications Sectors, all CI/KR sectors rely on the Internet. Sectors must assess their dependence on the IT and Communications Sectors and the Internet. To assist in this process and to provide a forum for addressing cross-sector cyber security perspectives, DHS and the Partnership for Critical Infrastructure Security established the Cross Sector Cyber Security Working Group (CSCSWG). The CSCSWG brings together government and private sector cyber security experts together to collaboratively address systemic cyber risk across the CI/KR sectors. As one of several focus areas, the working group will analyze cyber dependencies and interdependencies to assess how the 17 CI/KR sectors depend upon IT and Communications Sectors. Through an understanding of each sector's dependence on the IT and Communications Sectors, sectors can assess how critical business operations could be impacted by disruptions or degradation of services and develop appropriate mitigation strategies.

While the public-private collaboration achieved through the IT and Communications SCCs, GCCs, and Information Sharing and Analysis Centers (ISAC), and the CSCSWG have enabled

DHS to address Internet resilience in conjunction with larger critical infrastructure protection efforts, internal efforts have also been brought to bear on the issue of preventing and preparing for Internet disruption. CS&C established the Internet Disruption Working Group (IDWG) to address the resilience and recovery of Internet functions in the event of a major cyber incident. The IDWG, co-chaired by NCSD and NCS, engaged with public and private sector and academic and international Internet security experts to examine risks and improve preparedness and situational awareness, identified measures that public and private entities can take to protect against nationally significant Internet disruptions, and worked to confront the security challenge presented by a growing reliance on IP-based communications by promoting Internet resilience. The IDWG activities resulted in recommendations and findings that CS&C has integrated into IT and Communications sector efforts.

Because a major Internet disruption could potentially occur not only from a cyber attack or major disaster but also from a sudden and substantial increase in usage, CS&C evaluated a scenario based on increased telework-related usage during a pandemic outbreak. The study focused on the viability of the telecommuting strategy, which has been identified as a key component of the national response to a pandemic influenza and on the need to identify necessary preparations should an outbreak occur. Telecommuting is increasingly relied on as an alternative method of conducting business. However, CS&C's study found that, based on the existing Internet infrastructure, the technical feasibility of widespread telecommuting has not been established. Furthermore, a surge in telecommuting traffic could cause significant congestion. Although it is believed that the network backbones would tolerate a surge usage from telecommuting and would experience minimal congestion, residential Internet access networks and enterprise networks are likely congestion points of concern with regard to the telecommuting strategy.

The pandemic study was conducted in coordination with subject matter experts in government and industry in the fields of communications, IT, cyber security, epidemiology, business continuity, financial services, and emergency response and relied on NCS' Network Design and Analysis Capability (NDAC). The NDAC, comprised of modeling and analysis tools, communications datasets and subject matter experts, supports the analysis and assessment of both data and voice networks. The NDAC has proven extremely valuable in assisting the NCS in understanding the vulnerabilities of the communications networks. As traditional circuit-switched communications networks transition to packet-switched networks, the NDAC has begun analyzing the implications for the resulting NGN. NDAC has begun to evaluate the performance of multiple NGN architectures under various scenarios, including damage and congestion. For the pandemic study, CS&C used the NDAC to analyze network congestion resulting from telecommuting which would be similar to congestion resulting from a disruption to the Internet. Lessons learned through similar studies will inform the manner in which we plan for and respond to Internet disruptions and will provide actionable recommendations for government and industry partners.

While the NDAC work focuses on understanding networks in advance of a disruption, it can also be used to model the effects of known or likely damage after a disruption has occurred. Another CS&C program, designed to mitigate the effects of a communications network disruption, is the NCS' Priority Telecommunications Service. PTS was developed to ensure our Nation's leadership could communicate in times of congestion in the public network. Through

partnerships with communications providers, PTS has developed programs which provide priority access to both the wireless and wire line networks. As these networks are transitioning to IP-based, packet switched networks, the NCS has begun development of PTS for operation in the resultant Next Generation Network. As noted earlier, this capability will ensure our Nation's leadership continues to have priority access to voice communications in times of network congestion. Additionally, the NCS is developing plans for features such as priority email and priority video teleconferencing. The NCS is determined to ensure these vital capabilities are available for our Nation's leadership as communications networks continue to rapidly evolve.

To understand the effectiveness of these planning and modeling efforts, CS&C sponsors exercises to rehearse, test, and refine key cyber processes and mechanisms for coordination and information exchange; and identify interdependencies, overlaps, and gaps in existing plans and processes. The National Cyber Exercise, Cyber Storm II, scheduled for March 2008, will include a focus on Internet disruption and related recovery. Cyber Storm II will examine the capabilities of participating organizations to prepare for, protect from, and respond to the potential effects of cyber attacks; exercise strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures; validate information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information; and examine means and processes through which to share sensitive information across boundaries and sectors, without compromising proprietary or national security interests. Cyber Storm II will also provide an opportunity to exercise Concepts of Operations and Standard Operating Procedures that have been developed or updated based on the findings from Cyber Storm I.

NCSD's Cyber Storm II planning team is working with the IT and Communications SCCs and ISACs and other subject matter experts from government and industry to contribute to the scenario development. Scenarios will include Internet and communications disruption and stakeholder-specific issues requiring a coordinated incident response. The adversary framework may ultimately include organized crime, a terrorist organization, and a nation-state, and will be refined based on the capabilities an adversary would need to conduct the scenario-specific attacks. Cyber Storm II provides a mechanism for CS&C together with a wide variety of public and private entities to improve cyber security preparedness and incident response capabilities and refine roles and responsibilities.

Delivering Capabilities to Respond to and Recover from Internet Disruptions

Cyber Storm II will also provide an opportunity to exercise response and recovery plans from the recently released draft National Response Framework (NRF), the successor to the National Response Plan. The Framework, which focuses on response to a national emergency and short-term recovery, articulates the doctrine, principles, and architecture by which our Nation responds to all-hazard disasters across all levels of government and all infrastructure sectors. The Framework incorporates a number of key recommendations from more than 700 individuals representing Federal, Tribal, State and local governments, non-governmental agencies and associations, and the private sector, who participated in the review process. As part of the NRF review, CS&C undertook an in-depth review of the NRF components, which seek to address incidents pertaining to communications and IT. These include Emergency Support Function

(ESF) #2 – Communications Annex and the Cyber Incident Annex. ESF#2, for which the NCS is a Coordinating Agency, supports the restoration of public communications infrastructure, supports responses to Cyber Incidents, and coordinates Federal communications support to response efforts.

For national incidents that are primarily cyber in nature, the Cyber Incident Annex provides the response and recovery framework. The Cyber Incident Annex, for which the NCSD is the Coordinating Agency, focuses on responding to, and recovering from significant cyber incidents requiring a coordinated Federal response ("Cyber Incidents"). The characteristics of a Cyber Incident may include incidents that impact critical government functions, threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation. The Cyber Incident Annex provides a framework for Federal Cyber Incident response coordination among Federal departments, agencies, and upon request, State, local, tribal, and private sector entities. When a Cyber Incident occurs, it could impact multiple infrastructure sectors or be targeted at a specific sector such as finance, energy, or communications. As such, a Cyber Incident could result in the activation of several or all of the ESF Annexes under the NRF. The Cyber Incident Annex is currently undergoing a public comment period to collect recommendations from government, non-governmental agencies and associations, and the private sector.

Consistent with the guidance in the NRF, ESF#2, and the Cyber Incident Annex, NCSD works with DHS' Incident Management Planning Team to develop the National Cyber Scenario Plan, one of fifteen National-level strategic plans being developed to guide the Nation's response to specific incidents. This planning effort will include input from the National Cyber Response Coordination Group (NCRCG), US-CERT, the Department of Defense (DOD), law enforcement, the intelligence community, State governments, international allies, and the private sector. Using the comprehensive capabilities of these entities, the plan will detail the roles and responsibilities and the capabilities available to the Federal Government to respond to a Cyber Incident.

The NCRCG serves as the principal Federal interagency mechanism to facilitate coordination of the Federal Government's efforts to prepare for, respond to, and recover from, cyber and physical incidents and attacks that have significant cyber consequences. The Cyber Incident Annex of the NRF identifies a role for the NCRCG, which is co-chaired by DHS, the Department of Justice, and DOD. The NCRCG is comprised of senior representatives from Federal agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from Cyber Incidents. The senior level membership of NCRCG helps ensure that during a significant national incident, the full range and weight of Federal capabilities will be deployed in a coordinated and effective fashion. For example, the NCRCG recently convened to address the denial of service attack against the Government of Estonia. Once the co-chairs were notified of the activity, and convened to discuss the situation, it was determined that an operational response was needed. This response was coordinated through CS&C's two operational arms—US-CERT and the NCC.

NCC and US-CERT are critically important to managing ongoing cyber incidents, and the two operations centers are positioned to work together to address cyber attacks, including those targeting the Internet. The NCC, established in 1984, has served as a forum in which the Federal

government and private sector communications providers interact face-to-face on a daily basis. In the NCSD's US-CERT, public and private sector entities collaborate with DHS to coordinate defense against and responses to cyber attacks across the Nation. Reflecting shifts in the Communications Sector, NCC membership has evolved over time to include satellite, cellular, cable, and IT companies in addition to the core telecommunications companies. In the event of an emergency involving the disruption of communications networks, the NCC, through its 24x7 operation, provides a forum for government and industry to coordinate incident response and recovery.

US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. To fulfill these responsibilities, US-CERT coordinates with a broad community of key private sector and government entities on topics ranging from Domain Name System (DNS) issues to core IP topics. For example, to bring greater attention to DNS and IP issues of national significance, US-CERT has been attending the North American Network Operations Group (NANOG) meetings for the last three years. Regular information sharing with public and private entities such as NANOG enables US-CERT to build situational awareness of network conditions, identify abnormal network activity, and initiate a response to prevent a more significant cyber incident. US-CERT also engages with the various sector ISACs to report, exchange and analyze sensitive information concerning cyber threats, vulnerabilities, incidents with strong and enforceable legal protections.

US-CERT works particularly closely with the IT-ISAC as the operational arm of the IT SCC. US-CERT and the IT-ISAC have instituted processes to regularly exchange information, analyze threats and vulnerabilities, and mitigate their effects. US-CERT and the IT-ISAC engage routinely through routine conference calls and other means and are working towards formalizing operating procedures. By working together in this manner, US-CERT and the IT-ISAC will ensure that the necessary mechanisms for collaboration are established and practiced.

To coordinate with government stakeholders, US-CERT also maintains robust collaborative arrangements. US-CERT works with the Multi-State ISAC to reach state and local government. The MS-ISAC serves as a mechanism for raising the level of cyber security readiness and response in each state. US-CERT also sponsors the Government Forum of Incident Response and Security Teams, which is a community of more than 50 Federal agency incident response teams that work together to secure U.S. Government networks.

US-CERT builds situational awareness of network conditions through its work with Federal departments and agencies utilizing its Einstein program. The Einstein program identifies abnormal network activity so that US-CERT and its partners can initiate a response to prevent a more significant cyber incident. Einstein enables strategic, cross-agency assessments of irregular or abnormal Internet activity that could indicate a vulnerability or problem in the system. The program passively monitors government agencies' gateways to facilitate the identification and response to cyber threats and attacks, improve network security, increase the resilience of critical electronically delivered government services, and enhance the survivability of the Internet.

These private and public sector engagements are critical to building trusted operational relationships that enable effective information sharing needed to respond in the event that a disruption occurs.

NCS and NCSD are working closely together to ensure that operational activities are coordinated, threats and vulnerabilities are jointly addressed, and the resources and expertise of each organization are brought to bear in this converged environment. CS&C is implementing a plan to co-locate the US-CERT and NCC watch and operations centers to ensure that IT and communications experts are working side-by-side to share situational awareness information and identify threats, attack vectors, and the implications of these threats and attacks across all infrastructure sectors. Towards this end, I also convened a joint industry-government task force to review the plans to further develop this integrated operational capability. The task force has completed its work and provided recommendations that I have begun to implement, such as the assignment of a program manager to implement the first phase of the recommendations, to include incorporating an IT industry representative into our operational framework.

CS&C is also working with DOD's Joint Task Force for Global Network Operations (JTF-GNO) to enhance information sharing and situational awareness between the two organizations to ensure the security and uninterrupted and unhindered access to the Internet. Joint operating procedures have been developed to describe US-CERT and JTF-GNO information sharing and response processes for addressing Federal and national Cyber Incidents. Plans include assignment of staff to the respective operations centers to increase coordination.

These efforts provide mechanisms for defending against, responding to, and recovering from incidents. Our collaboration with public and private sector entities is essential in these areas, and we must expand our work with others who share the need for cyber security. By doing so, we can promote the sharing of knowledge on active and strategic threats, awareness of exploits of specific vulnerabilities, and understanding of mitigation strategies.

Conclusion

Both Government and the private sector are taking action to address the resilience and recovery of Internet functions in the event of a major cyber incident. Effective collaboration with the private sector and other government entities provides a foundation for exchange of information and coordination of preparedness and response activities. We have established mechanisms to ensure that the Federal Government is prepared to handle the impact that an Internet disruption may have on our ability to achieve our mission and to respond in a timely manner to address and mitigate the consequences of a disruption. Similarly, the private sector has taken significant steps to manage risks to the Internet infrastructure and maintain its associated services and functions. Taken together, these efforts offer a framework for addressing Internet disruption now and in the future.

As we move forward, Government and the private sector must continue our collaborative efforts to prepare for and respond to Internet disruptions. To do this, senior business leaders across all industry sectors must be aggressive and take coordinated steps to assess their dependence on the Internet and our cyber infrastructure. Government departments and agencies must also ensure

that the Federal workforce understands its dependence on the Internet, the impact that a disruption could have, and steps that can be taken routinely to mitigate the consequences. Both Government and the private sector must have in place and regularly exercise continuity plans that can be implemented without the benefit of Internet or phone service. Ongoing assessment of the risk to the IT, Communications, and other CI/KR sectors will ensure that cyber security is an integral part of sector and organizational efforts to prepare for and respond to incidents.

I would like to thank the Subcommittee for its time today. I appreciate this opportunity to discuss this important issue.