CYBER SECURITY®
INDUSTRY ALLIANCE

Prepared testimony of
Paul B. Kurtz
Executive Director
The Cyber Security Industry Alliance

Before the Subcommittee on Telecommunications and the Internet of the House Committee on Energy and Commerce

Wednesday, Sept. 13, 2006

Introduction:

Chairman Upton, Congressman Markey and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Paul Kurtz and I am Executive Director of the Cyber Security Industry Alliance (CSIA).

CSIA is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. The organization is led by CEOs from the world's top security providers who offer the technical expertise, depth and focus needed to encourage a better understanding of security issues. It is our belief that a comprehensive approach to ensuring the security and resilience of information systems is fundamental to global protection, national security and economic stability.

Before joining CSIA, I served at the White House on the National Security Council and Homeland Security Council. On the NSC, I served as Director of Counterterrorism and Senior Director of the Office of Cyberspace Security. On the HSC, I was Special Assistant to the President and Senior Director for Critical Infrastructure Protection.

You have asked me to comment on a very broad topic – to look at the importance of cyber security not just as it relates to our critical infrastructures, but across America's economy and for all consumers. Later today I will testify before the House Homeland Security Committee on a narrow but important piece of your much broader inquiry – cyber security and recovery of our critical infrastructure – so I particularly appreciate the chance to begin that dialogue at the 50,000 foot level you posit.

Right now no one in government is really looking at the macro-level. The fact is that cyber systems are our newest and most pervasive infrastructure. They drive and organize every facet of our collective and individual lives from national and economic security to personal health and well-being – and yet we do not have a strategic national capability to assess how well the most critical systems are protected, and what the consequences are if they fail. Currently, there is little strategic direction or leadership from the federal government in the area of information security. Ensuring the resiliency and integrity of our information infrastructure and protecting the privacy of our citizens should be higher on the priority list for our government. CSIA believes the government has a responsibility to lead, set priorities, and coordinate and facilitate protection and response.

DHS has a central role in protecting critical cyber infrastructure from massive attack, but government must consider economic consequences and impact to our citizens in a more comprehensive and systematic way.

Clearly DHS has a vital and central role – HSPD 7 designates the Department of Homeland Security as a focal point for infrastructure protection, including cyber security. [We'll get to how well, or poorly, they are doing in just a moment.] But it is myopic to assume DHS has exclusive government responsibility for the entire continuum of security across all information infrastructures, and for all threats. DHS should, indeed ***must*** be accountable for coordinating the protection of our most critical infrastructures from serious attack or devastation. But when we think about the potential impacts of cyber threats and attacks on our overall economy, or for consumers as a whole, we must acknowledge that we have a strategic national interest in cyber security that is much broader than the mandate of DHS or the immediate challenges it faces. We face various forms of cyber attacks and efforts to exploit faulty software code every day. Businesses routinely fight against unauthorized intrusions, whether for sport, industrial espionage, or more nefarious reasons. Companies incur significant costs to keep up with ever-more sophisticated efforts to compromise their systems, ultimately we all bear these costs. And every day, thousands of citizens have their sensitive personal information compromised through data breaches, phishing campaigns, Internet fraud and other cyber crimes. As a result, consumers do not have trust and confidence in online services and e-commerce, with significant economic results for many industries.

The truth is that a major cyber disruption could prevent companies from operating critical systems, possibly for sustained periods of time. This means that planes may not fly, goods and services may not be distributed, power and gas may not be available, and all of this would have a potentially devastating impact on our economy and our citizens.

Most importantly, DHS must consider and articulate how it will work with the private sector to respond to and recover from a massive failure of information technology systems – whether from a cyber attack or a natural disaster. In preparing for how to respond to a significant cyber event, the unanswered question affecting all is: What is a suitable role for DHS as well as other key federal agencies, including DoD and the FCC, in facilitating recovery and reconstitution from a cyber "incident of national significance"? The Federal government must engage in a serious inquiry of the following questions:

- What is an "incident of national significance" and what is the process for determining such an event and its legal significance?

- What obligations do private sector entities have to obey directives from DHS, or other agencies?
- Who would resolve conflicting demands for scarce cyber resources?
- What enforcement power does DHS, DOD, and the FCC have to help the nation recover from a cyber disaster?

These are tough questions, and raise complex policy issues which extend beyond DHS.

We must take a holistic view – the United States needs a Strategic National Information Assurance Policy

The bottom line is that protecting our cyber infrastructure is not just DHS's problem. In large measure, because our cyber infrastructure is almost exclusively owned and operated by the private sector, the front line defense is the investment made by infrastructure providers on behalf of their customers. But, in addition to DHS, many key departments and agencies have key roles in protecting our cyber infrastructure:

- **The Department of Commerce has a key role.** The Department of Commerce advocates for technological innovation and has responsibility to develop and promote measurements, standards, and technology to enhance productivity, trade, and the quality of life. This includes conducting research to advance the U.S. technology infrastructure and supporting the development of technologies for broad national benefit.[1] The Under Secretary for Technology Administration has the lead in developing and promoting information security standards and in leading research and

[1] http://www.technology.gov/Index.html

development efforts to enhance privacy and security. There is much more Commerce could do. For example, Commerce currently does not measure consumer or business confidence in the information infrastructure or the costs of attacks or disruptions. Commerce, in partnership with DHS, could support increased adoption of insurance. Currently, many insurance companies are reluctant to enter this market because of a lack of actuarial data.

- **The Federal Trade Commission has a key role.** The FTC's Enforcement Division conducts a wide variety of law enforcement activities to protect consumers online, including: (1) ensuring compliance with administrative and federal court orders entered in consumer protection cases; (2) conducting investigations and prosecuting civil actions to stop fraudulent, unfair or deceptive marketing and advertising practices; and (3) enforcing consumer protection laws, rules, and guidelines.[2]
- **The U.S. Department of Justice has a key role.** The Computer Crime and Intellectual Property Section (CCIPS) within DOJ's Criminal Division is responsible for combating computer and intellectual property crimes worldwide. CCIPS' Computer Crime Initiative is a comprehensive program designed to combat electronic penetrations, data thefts, and cyber attacks on critical information systems. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.[3]

[2] http://www.ftc.gov/bcp/bcpenf.htm
[3] http://www.justice.gov/criminal/cybercrime/ccips.html

- **The Federal Communications Commission has a key role.** Charged with regulating interstate and international communications, the FCC has established the following objectives:
    - To evaluate and strengthen measures for protecting the Nation's communications infrastructure.
    - To facilitate rapid restoration of the U.S. communications infrastructure and facilities after disruption by a threat or attack.
    - To develop policies that promote access to effective communications services by public safety, public health, and other emergency and defense personnel in emergency situations.[4]
- **The Department of Defense has a key role.** DoD gives highest priority to securing its national security systems. The Defense Information Systems Agency (DISA) provides a seamless, secure and reliable web of communications networks, computers, software, databases, applications, and other capabilities to meet the information processing and transport needs of DoD. DISA also ensures the integration and interoperability of command and control, communications, computers and intelligence systems.[5]
- **The Office of Management and Budget has a key role.** The government has a critical need to ensure critical Federal IT systems are resilient; after all, our citizens rely on our government not to let them down. Under the Federal Information Security Management Act (FISMA), OMB is responsible for developing and overseeing the implementation of government-wide policies, principles, and standards, as well as

[4] www.fcc.gov/homeland
[5] http://www.disa.mil/main/about/missman.html

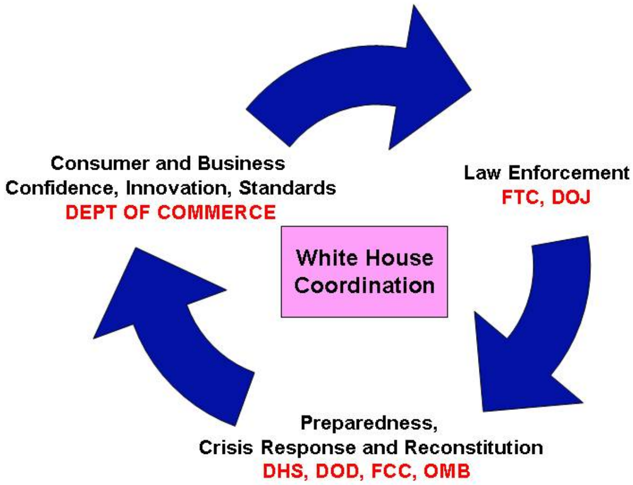
providing guidance for the federal government's information technology security program.[6]

- **White House Coordination.** The President's staff must ensure seamless coordination across Federal agencies and ensure sufficient attention and fiscal resources are allocated to the issue.
- **Congress has a key role.** Congress must exercise its traditional role. This Committee, for example, has worked hard to enact effective legislation to protect sensitive personal information; Congress should act before the end of the session to pass data security legislation.

A graphical depiction of this discussion is noted below:

Information Assurance

Federal Agency Roles and Responsibilities Cycle



Clearly, as a nation we have a strategic national interest in making sure that we understand the risks across all our cyber infrastructures and who is accountable for their resilience to attack.

[6] http://www.whitehouse.gov/omb/egov/

We urge policy makers to consider the need for a strategic national information assurance policy, developed in consultation with industry, operating across all of government. The policy would address many of the questions I have posed.

DHS needs to specify steps to prevent and/or minimize a massive cyber attack or telecommunications disaster

My remaining testimony will reflect on DHS's effectiveness to-date, because the bottom line is that cyber security is receiving inadequate attention from DHS. Of particular urgency is the need for DHS to specify how it and the private sector would coordinate actions if a massive cyber attack were to occur.

Last week in his updated national strategy for counterterrorism, President Bush declared that "America is safer but we are not yet safe." The reality of physical terror occurring in the United States has riveted our attention since the attacks on September 11, 2001. Prevention of any physical incident of horror has since been priority one.

The President's reminder for vigilance clearly applies to threats against our physical well-being, but his admonition should also apply to cyber security. Since 9/11, responsibility for coordinating federal efforts on national safety shifted to the Department of Homeland Security. DHS has predictably reacted to a myriad of security challenges by focusing first on immediate physical threats and natural disasters. This focus is understandable, but it has also impeded progress toward stronger national cyber security. As a result, the United States remains unprepared to defend itself against a massive cyber disruption or to systematically recover and reconstitute information systems after such an event. However, by realistically refining the

Department's role in national cyber security, DHS can escalate cyber security efforts along with efforts to prevent physical terror in America.

National coordination of cyber security is the purview of the Department of Homeland Security, and its related leadership position is Assistant Secretary for Cyber Security and Telecommunications. This new position was established in July 2005 by Secretary Chertoff specifically to elevate the importance of cyber security in relation to DHS's main focus on physical security. Unfortunately, fourteen months later, the Assistant Secretary position is unfilled, which reflects the low priority DHS still has toward cyber security. No one is in charge to lead efforts to protect information infrastructure against cyber attacks or to lead response and recovery.

For example, currently members of the IT sector are working with DHS on a sector specific plan as required under HSPD-7 and the National Infrastructure Protection Plan. While we have made progress, there has been little to no senior-level attention to the plan at DHS, as well as several other agencies. The plan seeks to hammer out many of the questions I posited earlier.

DHS has not specified how it will work with the private sector to a cyber incident of national significance

The Cyber Incident Annex of the National Response Plan, published January 6, 2005, states that the federal government plays a significant role in managing intergovernmental (federal state, local and tribal), and, where appropriate, public and private coordination in response to cyber incidents of national significance. DHS is well aware that the private sector "runs the show," which may account for its encouragement of public-private partnerships. However, the

Government Accounting Office recently reported that progress on those initiatives is limited, some lack time frames for completion, and relationships between these initiatives are unclear.[7]

Consequently, DHS needs to articulate a chain-of-command for each step of recovery and reconstitution. For example, the DHS's U.S. Computer Emergency Readiness Team (US-CERT) may be aware of a network attack, but the North American Network Operators Group (NANOG) is the operational forum for backbone/enterprise networking.

In addition to chain-of-command, DHS needs to articulate an emergency communications system that works even when standard telecommunications and Internet connectivity are disrupted. Emergency communications entail more than simply establishing a resilient mechanism allowing people to talk. It also requires advance identification of the right people from appropriate organizations who speak the "same language" for establishing rapid recovery and reconstitution of national systems.

These are but a few of the details that must be articulated and agreed upon in advance if the nation is to truly prepare for recovery and reconstitution from a cyber disaster. Ostensibly, DHS would have a leading role in planning.

These issues should be answered in the DHS's 400-plus page *National Response Plan*. Unfortunately, the plan does not articulate clear answers on how federal agencies work with each other, with other government entities, or with the private sector in responding to a

[7] "Challenges in Developing a Public/Private Recovery Plan," GAO-06-863T (July 28, 2006).

national disaster. Instead of one coordinator, there are at least six: Homeland Security Operations Center, National Response Coordination Center, Regional Response Coordination Center, Interagency Incident Management Group, Joint Field Office, and Principal Federal Official. The *National Response Plan*'s discussion of cyber security is contained in the "Cyber Incident Annex." The Annex mentions many other federal departments and agencies with "coordinating" responsibility for cyber incident response, including Defense, Homeland Security, Justice, State, the Intelligence Community, Office of Science and Technology Policy, Office of Management and Budget, and State, Local, and Tribal Governments. The agency tasked with maintaining the *National Response Plan* is FEMA.

As I draw toward the end of my testimony, I wish to comment on one other topic that also requires close coordination of the government and private sector – namely, the need for a cyber early warning system that provides the nation with situational awareness of attacks. DHS has sponsored some mechanisms toward this end, such as US-CERT, and Information Sharing and Analysis Centers (ISACs) that share some cyber alert data from the private sector with the federal government. As noted by the Business Roundtable, however, the nation lacks formal "trip wires" that provide rapid, clear indication that an attack is under way.[8] This mechanism would be akin to NOAA's National Hurricane Center, which usually can provide a day or so of advance notice before a dangerous storm lands ashore. Cyber attacks provide far less notice to prepare and react. DHS should lead the establishment of an efficient national cyber warning

[8] Business Roundtable, "Essential Steps to Strengthen America's Cyber Terrorism Preparedness" (June 2006); see also Section 15 of Homeland Security Presidential Directive 5, "Management of Domestic Incidents" (Feb. 28, 2003), and the *National Strategy to Secure Cyberspace* (Feb. 2003).

system because the private sector is most likely to first detect an attack, and data correlation and follow through coordination closely involves the government.

Summary of Recommendations

In summary, CSIA offers the following recommendations for the Subcommittee's consideration:

Consider the need for a government-wide strategic national information assurance policy. Cyber security is too important to be left to piecemeal and bifurcated approaches. There needs to be more active engagement by the White House to lead in developing a coherent national information assurance policy across all agencies.

Urge Congress to enact comprehensive data security legislation this year. Sensitive personal information should be protected whether it is being held by a commercial enterprise, non profit organization or government entity. Millions of Americans are looking to the government for help in safeguarding their personal information.

Increase Attention to Cyber Security. DHS has inadvertently exposed the nation to another vector of attack by providing inadequate attention to cyber security. The Department should reassess its priorities and shift some attention from an almost exclusive focus on physical security.

Appoint a Leader. There is no leadership at DHS in terms of a person who is solely responsible for cyber security. DHS should swiftly fill the open position of Assistant Secretary for Cyber Security and Telecommunications to close the leadership vacuum.

Plan to Prevent or Minimize a Major Cyber Disaster. DHS should shift this energy to articulating a smaller set of priorities focused on preventing and/or minimizing the likelihood or severity of a massive cyber attack or telecommunications disaster.

Plan to Work with the Private Sector to Recover from a Major Disaster. The existing DHS "plan" for recovery cites more than a dozen federal departments and agencies with "coordinating" responsibility – not including state, local and tribal governments. DHS needs to clearly articulate a chain-of-command between government and the private sector for recovery from a major cyber disaster.

With that, I appreciate the opportunity to testify today and am pleased to answer your questions.