GOOD HARBOR
CONSULTING, LLC

Prepared Testimony of
Kiersten Todt Coon
Vice President, Good Harbor Consulting

Information Policy,
Census, and National Archives Subcommittee Oversight and
Government Reform Committee

"Cybersecurity: A Review of Public and Private Sector Efforts to Secure our Nation's Internet Infrastructure"

2154, Rayburn House Office Building
Tuesday, October 23, 2007
2:00PM

4100 N. Fairfax Drive • 3rd Floor, Suite 301 • Arlington, VA 22203-1629
Tel: 703.812.9199 • www.goodharbor.net

INTRODUCTION

Good afternoon Chairman Clay, Ranking Member Turner and Committee Members. It is a pleasure to testify before you today on our nation's ability to secure its Internet infrastructure. I am currently a Vice President at Good Harbor Consulting and have worked on the issue of infrastructure protection in previous positions at Business Executives for National Security (BENS) and as a Professional Staff Member on the Senate Committee on Governmental Affairs (now Homeland Security and Governmental Affairs). In this capacity, I was one of the drafters of the legislation that created the Department of Homeland Security. Of particular relevance to this hearing, I was responsible for drafting the language to establish the infrastructure protection directorate.

I would first like to commend this Subcommittee for astutely identifying and choosing to examine a significant gap in this nation's ability to protect itself. This country and the world have come to depend on the Internet for nearly all the critical operations of business and government. Significant disruption to the Internet will wreak havoc on our ability to function. We have a responsibility to develop and commit to a comprehensive plan to prevent, detect, respond to and recover from a cyber attack on the Internet or a similar systemic failure.

BACKGROUND

As the *National Strategy to Secure Cyberspace* correctly stated, "cyberspace is the nervous system supporting our nation's critical infrastructures." We know that the majority of Internet infrastructure is owned and operated by the private sector. Therefore, any plan developed by the government for protecting this nation's infrastructure must be a result of public/private collaboration.

The government acknowledges this need. In December 2003, the President updated a national directive for federal departments and agencies to identify and prioritize critical infrastructures and key resources. This directive recognized that since most critical infrastructures are owned and operated by the private sector a public/private partnership is crucial for their protection.

However, little progress has been made on this issue. It is not enough to provide guidance on what needs to happen; rather, we must identify the roles and responsibilities within the public and private sector during a disaster.[1] The models for cyber security public/private collaboration that exist outside of the government are reasonable. However, within the Department of Homeland Security (DHS), there is a notable lack of cooperation and information sharing between the public and private sector on these issues. We lack a clear definition of the parameters of this issue, a concrete understanding of the risks that exist, an institutional awareness of the points of failure and solutions that address these issues.

[1] For example, the Cyber Annex of the current National Response Plan, which recommends creating a committee, leaves it up to the government to determine who from the private sector should be included, at what point the private sector should be included and at what level the private sector should be included.

CURRENT ENVIRONMENT

The recent exponential increase in our reliance on the Internet puts information infrastructure at the center of fundamental business and government operations, thereby making them more vulnerable. According to a recently released Business Roundtable (BRT) report entitled, "Growing Business Dependence on the Internet, " the World Economic Forum estimates a 10 to 20 percent probability of a breakdown of the critical information infrastructure in the next ten years. Additionally, it estimates a resulting global economic cost of approximately $250 billion. The pervasiveness of the Internet in business and government functions means that a cyber catastrophe would be devastating.

The consequences of Internet failure would significantly affect the economy. According to the BRT report, in a study of 66 security breaches between 1996 and 2001, the Congressional Research Service (CRS) found that there was a 2.1% decline in stock value for affected firms once they released the information – and a 2.8% reduction in value for those companies highly dependent on the Internet. CRS found that the impact is much greater if an Internet failure lasts longer than a day or two – with a reduction in stock price of 2.7%, relative to the rest of the market on the day of the attack, but a 4.5% drop three days later. For perspective, a 4.5% drop in the DOW Jones today would result in a reduction of approximately 600 points.

Additionally, an Internet failure can compromise our national security – an issue that has been demonstrated by recent events. The vulnerabilities within our information infrastructure must be addressed; previous breaches and disruptions demonstrate the loss that is likely if comprehensive public/private action is not taken quickly. In order to identify how to strengthen our infrastructure, we must first identify critical points of failure.

POINTS OF FAILURE

Infrastructure: Routers and End Systems

Routers

We currently rely upon a small number of key service providers (usually referred to as Tier 1 providers). These providers are the backbone of the Internet and if they were successfully attacked, there would be widespread disruption. Our routing infrastructure is robust enough to handle a single, non-malicious router failure; traffic would flow in an alternate way. However, our routing infrastructure cannot sustain the loss of an entire line of routers (i.e., the loss of all Cisco routers on the network because of a lifecycle attack).

End Systems

There are two classes of end systems – home-users and enterprise. Home-users are highly vulnerable to attack; they are the most prevalent users of the Internet and consume the majority of Internet bandwidth. Access to the servers, usually by enterprise users, is critical in a time of

crisis; if these systems are vulnerable and compromised, key response personnel will not be able to access the information they need to respond to the event.

The current challenge with which we are faced is that *all* information – both critical and non-critical – is transmitted over our information networks and treated equally. Additionally, more information is being transmitted over these networks than ever before. We can expect that in the very near future, most internet users will be streaming data-rich video into their homes, using the web for online games, performing all banking and financial functions, practicing telemedicine and having voice conversations.

As we increase the amount of information running over the Internet without strengthening the systems, we are burdening the critical infrastructure upon which our country depends for daily functioning and crisis management. As with any infrastructure, we must strengthen it to accommodate the changes and increase in use. We must also adapt its capabilities to manage its most urgent and critical functions.

When this nation is confronted with a pandemic like the avian flu, our information networks, as they currently operate, will experience disruptions and outages that will paralyze us and prevent us from executing an effective emergency response. Additionally, these overburdened networks will prevent key personnel from accessing critical systems remotely. For example, if quarantine measures are instituted in specific geographic areas in response to an outbreak, will government services be able to continue to operate through remote access by key personnel?

Response Capability Challenges

An efficient response capability is critical and necessary because we will not be able to guard, successfully, against all threats. Currently, we do not have a backup system in place that can be activated in the event of a widespread Internet failure. Additionally, we have not developed scenarios for potential attacks on our Internet infrastructure or responses to Internet infrastructure compromises. Although we continue to discuss the realm of risk that exists, we have not defined specific risks or their parameters. Experts disagree on the magnitude of risk and what needs to be done and we routinely use this lack of consensus as an excuse for inaction. Until we reach a reasonable consensus on these issues, we will not be able to prepare thoroughly for imminent attacks.

RECOMMENDATIONS

Infrastructure

Routers

- We must have diversity in the service providers we use; we should develop multiple sources for routing to reduce our risk of losing a router. An individual is advised to diversify his/her stock portfolio to reduce risk of losing one's life savings; we should

employ a similar tactic of router diversification to reduce the risk of losing core components of our Internet infrastructure.

- We need robust architecture within and among routers and service providers. This architecture should be constructed in such a way that if a service provider goes down, we don't lose it – similar to the way a ship is constructed. If water enters a compartment of a ship, the ship has the ability to contain the leak and continue to operate. We must be able to shut down a malfunctioning or contaminated component of the router system without losing the entire router.

End Systems

The Internet was designed as part of a research and development project within the Department of Defense for the purpose of openly sharing information. The challenge with which we are now confronted is the ability to impose the secure exchange of information on top of an open sharing environment. We must upgrade our networks and develop a system that prioritizes Internet traffic. In a time of crisis, we must be able to ensure that critical information is being delivered with priority speed and that it is not encumbered by non-critical information, which is being sent simultaneously.

We should create a three-tiered system that allows our networks to identify and prioritize in the following order: 1) critical communications supporting government operations, business and first responders; 2) routine business information; and, 3) non-critical information. Such a system will also allow us to categorize the critical traffic for those individuals who need to access it and to stop non-critical traffic in order to make more bandwidth available for the purposes of response and recovery activities.

In its report issued in June 2006, the Government Accounting Office (GAO) recommends establishing such a system for prioritizing recovery of Internet service similar to the existing Telecommunications Service Priority Program. The report states that we need to prioritize Internet traffic, but that prioritization currently faces numerous technical challenges and is not supported by legislation. We need to address these challenges and work with Congress to reach a solution.

Response Capabilities

Backup Systems

Because we cannot protect ourselves against every possible threat, we must develop sufficient response capabilities. Just as an early diagnosis of cancer can save a life, early detection and effective response to a malicious Internet event can prevent significant disruption.

One capability we must develop to ensure a resilient infrastructure is developing a backup system. If we experience a life cycle attack – where a piece of malicious code infects every router – we would need to have the ability to reboot the Internet. We should be maintaining backup parallel systems that can replace the active systems in a time of crisis. We must also

have reserve network protocols and set aside clean backup systems that can bring up the critical portion of the Internet (which could be easily identified with a tiered network system) quickly.

Scenario Planning
We should develop a playbook for scenario planning which pushes us to identify and conceive possible responses to a serious attack – responses geared toward systems administrators all the way up to the President. A significant attack would likely affect the infrastructure of one of the top three critical industries: power/utility, banking and telecommunications. Each of these industries is developing its own solutions for safeguarding the infrastructure upon which its business depends. However, as a nation, we need to think through how appropriate players in *both* the public and private sector will respond. The creation of scenarios will enable us to develop response options before an incident occurs and identify:

- Needed resources
- Additional R&D activities
- Existing engineering options

By not defining or agreeing upon the risk that exists, we prevent ourselves from following through on preparedness activities. It is not enough to establish that a risk exists; we must be able to define roles and responsibilities and assign accountability so that we have ownership of the issue.

NATIONAL CYBER RISK ASSESSMENT

One of the first steps we need to take in preparing ourselves for an information infrastructure failure is to set risk standards. However, we can't set risk standards if we don't know, concretely, what the risk is. Moreover, if we don't understand the consequences, we cannot develop priorities, policies, solutions and investment levels. One of the primary challenges that exists within DHS is the Department's lack of ownership on this issue. For example, why isn't the Cyber Warning Information Network[2] the responsibility of the Assistant Secretary for Cyber Security and Communications? When confronted with a disaster of any kind, it is unclear who will take responsibility and ensure an effective response.

Consequently, I propose a National Cyber Risk Assessment to be conducted by a blue ribbon commission of experts, who would be responsible for defining the risks that exist. I recognize, of course, that incidents may occur that do not align perfectly with the proposed assessment, but the only way we can begin to adequately prepare ourselves is to commit to possible scenarios. This assessment would inform the scenarios and define the right level and type of response. Additionally, a National Cyber Risk Assessment will enable us to assign ownership and response roles.

[2] The expansion of the Cyber Warning Information Network (CWIN) was recommended in Priority I of the National Strategy to Secure Cyberspace to play a coordinating role with the US-CERT to provide crisis management. To date, CWIN has not received appropriate funding or attention.

The Office of Management and Budget (OMB) should provide the funding, resources, direction, oversight and leadership for a National Cyber Risk Assessment and will be responsible for ensuring the recommendations from the commission are executed.

PUBLIC/PRIVATE PARTNERSHIPS

The phrase "public/private partnership" has lost its meaning. We use it so often without any result that it has become a cliché. Effective models for partnering the public and private sector exist, but failure has come from a lack of execution that has prevented the assignment of responsibility or accountability. However, public/private collaboration is necessary in developing efforts to secure our nation's infrastructure because ownership of this infrastructure resides primarily in the private sector.

The challenge that currently exists is that the private sector, as cited in the Business Roundtable Report referenced previously, believes that government has the primary role for restoring business operations following a major Internet disruption. In contrast, government believes industry sectors have recovery plans that will restore service.[3] What is evident is that both have a responsibility, but neither is adequately prepared.

CONCLUSION

Experts and observers postulate that we do not have to be worried about hackers taking down the Internet because hackers would not intentionally bury their playground. But our greatest risk does not come from hackers. I would like to leave you with the assertion that it comes from foreign governments that can ably and quietly use the Internet infrastructure for espionage and other nefarious purposes. The threat is particularly strong from governments that have developed their own internal Internet (such as China) and would therefore not be severely affected by a worldwide Internet disruption. Recent events have demonstrated that these scenarios are not possibilities, but realities.

Our national security, the health and well-being of our community and the daily functioning of our society depends on the security and resiliency of our infrastructure. We have a responsibility to define the information infrastructure risk that exists; we have a responsibility to plan for that risk appropriately, through dynamic and well-defined public/private partnerships. We have a responsibility to act and we must act now.

Thank you for the opportunity to testify before you today. I look forward to answering your questions.

[3] The 17 sector approach to infrastructure protection has thwarted cross-pollination of information sharing and methods across sectors. As industry and government examine effective partnering, it should examine and reconsider this model.