Testimony of
Thomas E. Noonan
President and Chief Executive Officer
Internet Security Systems (ISS)

before the
Subcommittee on Federal Financial Management,
Government Information, and International Security
of the
Senate Committee on Homeland Security and
Governmental Affairs

Hearing on
"Cyber Security: Recovery and Reconstitution of Critical Networks"
July 28, 2006

* * *

Overview

Mr. Chairman, Mr. Ranking Member, distinguished members of the Subcommittee, thank you for the opportunity to appear before you today. My name is Tom Noonan and I am President and Chief Executive Officer of Internet Security Systems (ISS).

ISS is the world's leading provider of preemptive cyber security technologies for large-scale enterprises. Headquartered in Atlanta, Georgia, ISS employs thirteen hundred professionals with 35 offices in 20 countries worldwide. We operate five cyber Security Operations Centers spread across the globe – two in the United States, one in Tokyo, Australia, and Brussels – that scour the Internet for potential cyber threats 24 hours a day, 365 days a year and provide managed, preemptive protection for many of our customers. If it is on the Internet, ISS knows about it. ISS' commitment to our government and private sector customers is to utilize our security intelligence, technology and expertise to preempt the strikes that could cripple critical networks and stay ahead of the threat.

As the representative of the security technology industry on this morning's panel, I want to stress three important messages about our nation's cyber security landscape:

- First, threats to our critical infrastructure are absolutely real and, without a doubt, growing. The question is not if, but when. The explosive growth of new Internet technologies, from wireless access to Voice over Internet telephony, has engendered threats that are far outpacing the security responses of private and governmental users.

- Second, the intelligence, protocols and technologies necessary to protect against emerging cyber threats are, by and large, robust and widely available. We *have* the tools at our disposal today to safeguard our critical infrastructure.

- And finally, despite our knowledge of these threats and our overall ability to protect ourselves, we as a nation are not doing nearly enough to *preempt* the types of attacks that could debilitate our critical networked infrastructure. Leadership is desperately needed at the Federal level -- not to *replicate* existing private sector efforts, but rather, to extend the impact of those efforts particularly by encouraging the private sector to collectively increase its cooperation. This means:

  1. Appointing an Assistant Secretary of Homeland Security for Cyber Security and Telecommunications who will help secure the Federal government's own networks as well as those of the broader economy;
  2. Clearly delineating and hardening the roles and responsibilities of the many public-private entities working today to secure cyberspace;
  3. Ensuring that the Federal Government makes full use of existing industry resources to gather and analyze data on cyber security threats;
  4. Creating a national plan to restore connectivity on a prioritized basis in the event of a large-scale cyber attack against our critical infrastructure; and
  5. Providing sustained Federal funding and active Congressional oversight to ensure that the Department of Homeland Security is getting the job done.

Cyber threats are serious, and they are growing in sophistication.

First, the bad news:

Cyber threats to our nation's critical infrastructure are not the stuff of hysteria or even hyperbole; they are real. The quintessential computer hacker, once dismissed as a solitary troublemaker or a teenage malfeasant, is today a technically sophisticated criminal who is often part of a larger, confederated crime operation. The motivation, today, quite simply, is greed. The rules of criminal hacking today are shaped by the economics of opportunity, incentive and risk – just like traditional theft, burglary or extortion.

One need only look at the highly sophisticated "phishing" scams plaguing the financial services industry – in which cyber criminals impersonate financial institutions and defraud consumers of their savings – to realize that we are not dealing with hobbyists or Robin Hoods. Indeed, the explosive growth in "phishing" is emblematic of the trends we are seeing in cyber attacks: a movement away from individual actors launching viruses and worms, towards highly sophisticated, transactional forms of Internet-based theft and fraud. These run the gamut from click-through fraud – which impacts 15% of all online advertising – to wide-scale identity theft. And while financial institutions have been a prime and growing focus of these crimes, other components of our critical infrastructure, such as power and water facilities, have likewise been targeted.

This “professionalization” of cyber crime is unsettling for many reasons, not the least of which are indications that those who would seek to do harm to our nation have been working to improve their technological capabilities. Particularly unsettling is the real threat to the control systems and SCADA networks that monitor and regulate our nation’s industrial systems. Control systems are Internet connected, and are therefore susceptible to any number of malicious attacks. Under contract with customers, ISS has conducted real-world penetration tests with large power plants, oil companies, manufacturers and other users of control systems to demonstrate that these systems are indeed at risk to Internet-based attacks. Compounding the problem are Google type searches that demonstrate the degree of information available to would-be attackers on where and how to practice their procedures far away from the eyes of our government. The Internet offers criminals and other malicious organizations anonymity – the ability to commit crime remotely and in an untraceable way, or to use computer systems owned by others, as the vehicle to commit crime, house illicit materials or commit terrorist acts.

Put simply, Mr. Chairman, the fact that our nation’s critical infrastructure has yet to fall victim to a significant and coordinated cyber attack does not mean that it cannot happen. While I believe that our networks are robust and generally resilient, I nonetheless feel strongly that our critical infrastructures contain critical weaknesses that must be addressed.

Take, for example, the incidence of computer vulnerabilities: Despite the serious efforts of many technology companies post 9/11 to make their products and networks much more secure, the number of vulnerabilities that we are finding in computer systems today has actually grown -- not diminished -- since 2001. According to the Computer Emergency Response Team (CERT) Coordination Center, the number of known vulnerabilities climbed from roughly 2,500 in 2001 to nearly 6,000 in 2005. And in just the first half of this year, ISS has already documented almost 4,000 vulnerabilities. In fact, our world-renowned research and development team, the X-Force®, which tracks cyber threats and works closely with business and government to alert them of potential dangers, believes that we may reach as many as 7,000 published vulnerabilities this year – noting that this number does not include the number of known viruses, worms and spam. Disturbingly, the X-Force reports that June set a record for the most-ever disclosures of new computer vulnerabilities: 696 last month alone, meaning we are on track to find 42% more vulnerabilities in computer systems this year than we did last year. And since our critical infrastructures are essentially a complex web of interdependent computer systems, weaknesses in those systems can easily translate into weaknesses in our critical infrastructure. Case in point estimates are that 5-7% of Internet connected systems are currently compromised.

Part of the rapid increase in vulnerabilities may well be attributable to the fact that we as an industry are investigating vulnerabilities more aggressively than ever before. But that is not the whole story. The more likely answer lies in the fact that we have seen a proliferation of new technologies in recent years – wireless, Voice over Internet telephony, and instant messaging, to name a few – whose security features are weak or even nonexistent. Emerging technologies and an exponential increase in the use of the Internet to advance business productivity, along with an exponential surge in the number of software applications used to conduct business, have opened many new avenues of attack. Keeping up with a large increase in vulnerabilities is a daunting task. We have seen and continue to track a shrinking window for the time a vulnerability is discovered to the time it is exploited by criminal interests. As the old saying goes, you rob a bank because that is where the money is. The Internet is certainly no different. The Internet Economy is the Economy. Today, that is where the money is, as well as the intellectual property, trade secrets or even the pathway to physical and economic disruption that those who wish to do harm can utilize.

The United States has the know-how to protect its critical infrastructure.

But there is good news, Mr. Chairman.

Our nation already has the technological capabilities to protect its critical infrastructure. Between the myriad of industry, academic, and governmental experts, we know where our cyber vulnerabilities lie; we recognize where are the back doors and open windows exist that provide entry points for cyber criminals and malicious threats, and we have the means and know-how to close them.

Take our own case, for example. As part of our mandate, ISS makes it our business to identify threats before they are exploited, and to arm our customers – including government agencies like the Department of Energy – with the tools they need to preempt these dangers. At ISS, we recognize our responsibility to share with governments and targeted industries worldwide the vast amounts of cyber intelligence we gather daily across our global networks and put this into useable formats. ISS employs technical experts whose sole responsibility is to work with governmental authorities and affected industries to apprise them of potential cyber threats. This responsibility extends to my level, Mr. Chairman. As an original member of the President’s National Infrastructure Advisory Council (NIAC), I was pleased to contribute to the recent NIAC Intelligence Coordination Report and the NIAC Evaluation and Enhancement to Information Sharing and Analysis Report. The recommendations from NIAC to DHS contained in these reports are critical to strengthening the processes and protocols needed to prevent a serious cyber incident.

We work together, Mr. Chairman, because protecting our critical infrastructure is a job that the Federal Government cannot do on its own. The private sector collectively owns and operates at least 85% of our nation’s critical infrastructures, which means that we must be our own first line of defense. Simply put, the Federal Government on its own cannot safeguard the most porous border there is – the Internet. That is a job for all of us.

Which is why countless public-private efforts to protect cyber space have arisen, including the Information Sharing and Analysis Centers (ISACs), which transmit cyber information intelligence between the private sector to the Federal Government; the Computer Emergency Response Team (CERT) Coordination Center, a Federally-supported, privately-administered clearinghouse for information about computer vulnerabilities; myriad protocols established between Federal agencies, such as the Department of Homeland Security, security developers like our own, vendors whose software they developed and important segments of our critical infrastructures; and more advisory boards, information-sharing councils, and experts groups than you can shake a stick at.[1]

There is a point in vulnerability coordination where we can make great strides in providing protection to consumers across the globe. That point is after notification to the original equipment manufacturer (OEM) vendor and their ability to design an appropriate fix prior to public announcement. We know from anecdotal evidence that most organizations do not patch or upgrade their systems right away and that an overwhelming majority do not do so until somewhere between 30 and 80 days after public announcement. We also know that the criminal cyber attackers have new malware available within 24-48 hours after public announcement. Unfortunately, most of the security that all users have does not have a deployed fix available until about 24 hours later. Mr. Chairman, that means that many of our Internet users, government to business to consumer, are without any protection for days to months after attacks begin.

The know-how is there. The partnerships and protocols to harness this know-how are there, as well. The industry has the ability to coordinate amongst ourselves for all to benefit from better protection.

But what is missing, I am sorry to say, is genuine leadership on the part of the Federal Government to encourage us to do so.

Greater attention must be paid at the Federal level.

We as a nation can protect our critical infrastructure – in fact, we already are. But we can protect it much more effectively. And that requires Federal leadership.

By that I do not mean that the Federal Government should attempt to take charge of securing cyberspace. It is not possible, not to mention the fact that it would be an

[1] The long list of public-private efforts, as noted in the Business Roundtable's recent report *Essential Steps To Strengthen America's Cyber Terrorism Preparedness*, includes the President's National Infrastructure Advisory Council (NIAC), the National Security Telecommunications Advisory Committee (NSTAC); the Network Reliability and Interoperability Council (NRIC); the National Communications System (NCS) that operates within the Department of Homeland Security, along with its Alerting and Coordination Network; the National Cyber Security Division (NCSD), which includes CERT; and portions of the Homeland Security Information Network (HSIN), which is overseen by NCSD.

immense drain on resources to try to replicate the work already being done by a vast and diffuse network of private operators.

Instead, the Federal Government's role here boils down to one thing: *minding the store.* Working side by side with industry to shine a bright light on our nation's cyber vulnerabilities, helping to harness the resources needed to make sure that those vulnerabilities are addressed and encouraging the development of secure coding and strong computer architectures.

I appreciate and recognize the work that has been done by the Administration and the Congress to improve Federal cyber preparedness through initiatives such as the National Strategy to Secure Cyber Space, DHS' recently-announced National Infrastructure Protection Plan (NIPP), and the enactment of the Federal Information Security Management Act (FISMA). But I am sorry to say, Mr. Chairman, that despite these efforts, the Federal Government has fallen short in perhaps a more important way: The necessary leadership is not exercised on a day-to-day basis to place and keep cyber preparedness squarely on the national agenda.

Let me give you two examples:

First, it has been one full year since the Department of Homeland Security announced that it would elevate the responsibility for national cyber preparedness through the creation of the position of Assistant Secretary for Cyber Security and Telecommunications. And yet, one full year later, that position is still unfilled.

I recognize that it takes a while to fill sensitive jobs in Washington, Mr. Chairman, and I hesitate to put too much emphasis on a single vacancy when what is really needed is an integrated effort. But nonetheless, I believe that the fact that such an important role has remained unfilled for this period of time indicates a broader lack of urgency in many quarters of our nation with respect to cyber security.

I know that Secretary Chertoff and the Department of Homeland Security (DHS) are working round-the-clock to protect our nation. But with cyber security so integral to that protection, those of us who monitor, run, and own the networks that power our nation's critical infrastructure need to have access to a singularly-focused, authoritative point of contact. In short, we need to be able to talk to the person who is minding the store.

Secondly, Mr. Chairman, it is difficult for the Federal Government to preach strong cyber security practices across our economy when Federal networks themselves are so woefully unprotected. While steps have been taken in recent years to improve agency security practices, including through FISMA, most Federal agencies still get failing marks when it comes to securing their networks. And I mean this literally: we are all familiar with the cyber security report cards that Congress has given the Federal Government in recent years, in which most agencies have consistently gotten either unsatisfactory or downright failing grades. I wouldn't accept such marks from my children, and we shouldn't accept them from our government. Anyone who thinks the Federal Government is doing better than these scores would indicate need only open the newspaper, which each day seems to bring a new story about lax practices leading to the disclosure of private or sensitive information.

Mr. Chairman, when it comes to strengthening Federal leadership in cyber security, we need five specific items:

1. The appointment of an Assistant Secretary for Cyber Security and Telecommunications empowered with the authority to establish and execute the Federal Government's cyber security strategy, which includes protecting its own networks and helping to ensure that those of the broader economy are secured. Portions of a Federal strategy have been outlined in various documents and action plans in recent years but without a single individual tasked with their execution, implementation has been spotty at best.

2. A clear delineation and hardening of the roles and responsibilities of the many public-private entities working today to secure cyberspace. There is simply too much confusion and, I suspect, duplication among the myriad of public-private entities laboring with the best of intentions in this space.

3. To ensure that the Federal Government makes full use of existing industry resources to gather and analyze data on cyber security threats. There is no point in DHS attempting to reinvent the wheel, which is what I fear sometimes occurs in well-meaning attempts at information sharing. The expertise needed to collect and analyze threats already exists in spades in the private sector; what does <u>not</u> exist are clear Federal processes for how to best make use of the private sector's analytical capability. The Federal Government must do more to encourage information sharing among those who already possess that information - the private sector - and utilize that collective knowledge.

4. A national plan to restore connectivity on a prioritized basis in the event of a large-scale cyber attack against our critical infrastructure. Contingency planning, disaster preparedness and recovery are, after all, quintessential government responsibilities. And while industry provides the pieces that form our critical infrastructure, it is the Federal Government that must help us pull these pieces together.

And finally:

5. Sustained Federal funding and active Congressional oversight to ensure that the Department of Homeland Security is doing all it can to harden both our nation's critical infrastructures as well as the Federal Government's own networks.

* * *

There is no silver bullet here, Mr. Chairman. Securing our nation's critical infrastructure from cyber attack requires a heightened degree of public-private coordination, information sharing, and trust than has been asked of us in most enterprises. Indeed, it is a challenge as unique as Internet itself. But it is one that I believe we as a nation are more than ready to take on, Mr. Chairman.

ISS is pleased to be a partner with you in this important effort, and I thank you for the opportunity to appear before you today.