September 13, 2006

Subcommittee on Telecommunications and the Internet

"CyberSecurity: Protecting America's Critical Infrastructure, Economy, and Consumers"

Written Testimony of Larry Clinton,
Chief Operating Officer, Internet Security Alliance

Good Morning, I am Larry Clinton, Chief Operating Officer of the Internet Security Alliance. I also sit on the Board of the National Cyber Security Partnership, and both the IT and Telecommunications Sector Coordinating Councils. In addition, I chair the NCSP Committee on Incentives for Improved Corporate Security. I want to thank Chairman Upton for having this hearing and inviting me to participate on behalf of the Internet Security Alliance.

The ISAlliance represents about 500 companies operating on 4 continents who are primarily major corporate *users* of Internet services. Our diverse membership includes companies from a wide variety of economic sectors including financial services, IT and Telecommunications, entertainment, manufacturing, food services, defense, business consulting and security services. Companies such as American International Group, Mellon Financial Corporation, Northrop Grumman, Visa, Verizon, Verisign, NAM, Sony, Tata Consulting, Raytheon, Nortel and Ceridian, among many others. Companies join ISAlliance because we believe we must work across corporate and national boarders, and engage both security providers and users in order to improve cyber security in a comprehensive fashion. Our goal is to improve cyber security across the nation and the globe through education, training and the creation of market based incentives for action.

My remarks today will focus on three main messages I would like to leave with the Committee today.

First, the threat to this nation's and the world's economic infrastructure from the risk of cyber-attack is real. It is not science fiction. It is not theoretical. It is happening today and in all likelihood will get worse.

Second, regrettably not enough is being done, either by government or industry, to secure cyber space. We continue down this path at great peril. If we are to address the threats we face in the Internet security space, we must broaden our thinking considerably. We cannot manage what is, essentially, the first 21st century technology solely using regulatory models designed two centuries ago. A new, more creative, model built on market incentives and creative solutions must be developed and added to the mix.

Third, fortunately, there are concrete steps that can be taken to both by industry and government to create this new model. Some of these steps have already begun, but we need to pick up the pace of activity considerably.

CYBER THREATS ARE SIGNIFICANT AND GROWING

It was not that long ago that popular myth held that cyber attacks were largely propagated by some Matthew Broderick type High School student playing "war games" with the pentagon computer system to prove how smart he was. If that ever was the case it is no longer. Now the most likely perpetrator is more likely to be agents of foreign countries, organized criminal syndicates or highly educated and trained cyber-terrorists.

Here are some core facts:

- The dot-com bust gave the illusion that Internet growth slowed down, but in fact it has grown at remarkable rates. At the height of the dot-com boom in 2000, for example, roughly 250 million people used the Internet. Today, according to Internet World Stats, more than 1 billion users worldwide rely on the Internet, a 300 percent increase since 2000.

  The explosion of Internet-enabled devices and applications – text messaging, music downloads, VoIP, Blackberries and device-to-device communications – has created exponential growth in Internet traffic far surpassing the increase in users. While users have increased 300 percent since 2000, the volume of traffic on .com and .net has increased 1,900 percent in that same period.

- This very growth of Internet users, broadband capacity and number of Internet-enabled devices has created an opportunity for hackers, organized criminals and even more serious terrorists to attack our networks. Some do so for technical trophies, some for political objectives, but today, most bad behavior on the Internet is done for financial gain.

  In fact, the very devices and increased bandwidth that make the Internet more robust and user friendly are being deployed to compromise the Internet. Now that computers are always-on, they are easily accessible to hackers and other abusers to hijack. And the increased bandwidth and computing power available literally gives hackers more ammunition to utilize against the infrastructure.

- In October 2002, the Internet community got a wake-up call when the 13 DNS root servers, which serve as the heart of the Internet addressing system, came under heavy denial of service (DoS) attack. In these attacks, the hackers send countless bogus inquiries to domain-name servers, which are computers that direct Internet traffic. By sending phony website requests to these servers, they overload and disable them, making websites unavailable.

  The most alarming of attacks occurred in early January 2006, when a hacker systematically disabled over 1,500 websites using hijacked PCs. In these attacks, the hacker didn't directly attack the domain-name servers. Instead, they sent their traffic to a legitimate server with a DNS query and a forged source address.

- Twenty-five percent of America's economic value ---up to 3 trillion dollars a day--- moves over network connections each day. The main protocol used to protect this data is over 30 years old and has multiple well-know security flaws. There are now more electronic financial transactions each day than there are paper checks written.

  If the Internet were to go down for a just few hours, we would lose hundreds of millions of dollars of economic activity. If it went down for several days, U.S. economic activity would be severely curtailed; payrolls would not be met, securities transactions not cleared; invoices not paid.

- In 2004 the Congressional Research Service estimated that the economic impact of cyber attacks on business grew to $226 billion. In truth, we don't know the precise amount of the economic losses because there is a tremendous disincentive to disclose this information. But we do know it's huge and growing.

- In August 2006 the SANS Institute claimed that bank's financial losses caused by cyber attacks were up 450% from the first half of 2005.

- August 2006 was the worst month in history for data breach notifications according to SANS. Consumers Union tells us that although about 98% of bank robbers get caught, only 1 in a thousand identity thefts are prosecuted. One of the main reasons is again the internet infrastructure itself makes tracing these thieves very difficult.

- There has been a massive increase in cyber crime from organized groups in Eastern Europe and Asia.

This is the on-going chronic cyber security problem we face day in and day out.

However, the threat is not just from criminals. International terrorists are becoming increasingly sophisticated in their use of the global net creating a threat potentially more dangerous than physical explosives. Of course, for some time now, terrorists have used the net for fund raising, communication and recruitment activities. However, there is growing testimony from the intelligence community that they are pursuing methods to inflict a deadly combination of electronic breakdown and serious physical injury either using cyber means alone or in combination with physical explosives.

Former CIA Director George Tenent has said the Internet represents the "Achilles heel" of our financial stability and physical security. Former CIA Director Gates has warned that cyber-terrorism could be the most devastating weapon of mass destruction yet.

In April of 2002, then Homeland Security Director Tom Ridge probably said it best: "Terrorists can sit at one computer connected to one network and can create worldwide havoc. [They] don't necessarily need a bomb or explosives to cripple a sector of the economy, or shut down a power grid."

A recent Google search on the term "cyber-terrorism" found over 900,000 entries.

Accordingly to the Insurance Information Institute, 2005 was the most costly on record for the insurance industry, with insured losses from Hurricane Katrina alone at $40.6 billion and total catastrophe losses for the year from 24 disasters totaling $61.2 billion. We have but to watch the news to see vividly the misery and destruction caused to New Orleans and the surrounding areas.

Now, imagine a hurricane with intelligence. One that learns and grows more destructive with each year. Imagine a hurricane that methodically, intentionally with malice born of a lifetime of anger plans and executes a destructive force to precisely hit the very fabric of our economy and daily life. That is a cyber-terrorism attack.

However, those of us who operate major information systems know that we must worry not just about that cyber-hurricane of the future but of the smaller attacks we are under every day---thousands of times a day.

Thus, it is our job in industry to work with you in government to address not just the large scale, massive, attack scenarios but also to address the chronic cyber security problems we face.

To do this, we must broaden our approach.

WE NEED TO BROADEN OUR THINKING ABOUT INTERNET SECURITY GOVERNANCE

When I say we need to broaden our thinking about the Internet, I mean that we need to do at least three things.

First, we need to realize that the Internet is unlike anything we have dealt with before.

- It transmits phone calls but it is not a phone line.
- It makes copies but it is not a Xerox machine.
- It houses books but it is not a library.
- It broadcasts images but it is not a TV station.
- It's critical to our national defense, but it is not a military installation.
- It's all these things and much much more.

The Internet is international, interactive, constantly changing and constantly under attack.

Consequently, it will require a security system unlike anything we have designed before.

It's not even really an "It." Its actually lots of "Its" all knitted together. Some public, some private --all transmitting information across corporate and national boarders without stopping to pay tolls or check regional sensitivities.

The regulatory model we have traditionally used to govern business has not changed much since we created it to deal with the breakthrough technology of 2 centuries ago---the railroad.

To manage the railroad, Congress decided to create an expert agency, the ICC to pass specific regulations. The ICC begat the rest of the alphabet soup, the FCC, the SEC and the FTC. And that system has worked arguably well in most instances.

But that system, whatever its advantages, will not work with Internet security. Even if Congress were to enact an enlightened statute, it would not reach beyond our national boarders and hence would not be comprehensive enough. Even if some agency wrote a brilliant regulation, it is likely to be out-dated before it went through the process, a process that can be further delayed with court challenges.

And that assumes, unrealistically, that the political process inherent in a government regulation system doesn't compromise, simplify and "dumb-down" the eventual regulations so that we end up with a standard which offends no one, where everyone can attest that they met the new federal regulations, but everyone knows the system is not really working.

That is not to say that regulation doesn't have its place, especially with traditionally regulated industries. It is to say that regulation, standing alone, will not be sufficient.

We must, together, develop a mechanism to assure an effective and sustainable system of security that will accommodate the global breadth of the Internet and still result in a dynamic and constantly improving system of mutual security.

We, the Internet Security alliance, contend that the best mechanism to assure an adequate and sustainable defense system is to inject the market with a combination of motivations.

We need to have corporations, who own and operate the vast majority of the Internet, to perceive that it is their own self interest to continually improve not only their own security, but that of everyone else with whom they interact.

Sadly, this is not the case now.

A range of studies have demonstrated that corporations, for various reasons, tend to regard security and resilience, including cyber security, as a cost center to be minimized.

Moreover, the enlightened companies will do what they perceive is appropriate to assure the cyber defense within their corporate borders, however, the Internet is a shared infrastructure.

We need to develop a system that assures comprehensive security---and nothing motivates the private sector like market incentives.

Psychologists tell us that punishment as the sole means of behavioral modification doesn't effectively work past the age of two. Rather, the best course of action is the use of the carrot, sometimes alone and sometimes in combination, with an already in place and existing stick.

THE ROLE OF INSURANCE

Numerous private and governmental documents have encouraged the use of cyber-insurance and the creation of a robust cyber-insurance market. There is little wonder about this. Insurance can:

(1) motivate best practices by modifying the availability and affordability of insurance based on the degree of implementation of such best practices,

(2) spread the financial costs of a cyber-attack, especially a massive cyber-attack, among society creating an efficient funding mechanism in the event of "digital Pearl Harbor", and

(3) be a primary distribution channel for risk management information on preventing and mitigating cyber-risks given the history view of the insurance industry as the "risk management experts".

Given that a robust insurance market is necessary to achieve these essential public goods, the question is how best to achieve such a market. While the primary burden is on the insurance sector itself to make this happen, left purely on its own, the industry will move "too little, too late". One main reason for this is that the lack of historical loss information makes the creation of standard actuarial tables impossible leaving carriers to "guesstimate" correct rates, something most carriers do not want to do. Thus, the market is currently estimated to be less than $200 million in premium with only a handful of carriers willing to issue policies.

Fortunately, there are concrete steps, some easy and some hard, that can be taken by the insurance industry and government to achieve the goal of a sustainable and robust insurance system for the inevitable cyber-hurricane.

THERE ARE CONCRETE STEPS THAT WE CAN TAKE TO DEVELOP A SUSTAINABLE MODEL OF INTERNET SECURITY

A. What We Are Doing

The mantra of the Internet Security Alliance is that since the Internet is largely owned and operated by the private sector, it is up to the private sector to provide Internet security.

Consistent with that policy, the Internet Security Alliance has executed and supported a wide range of activities within the private sector to improve security.

INFORMATION SHARING

ISAlliance was founded in April 2004---5 months before the tragedy of 9/11 placed an increased emphasis on security because, even then, we realized the need for advanced information sharing. We established one of the first and most sophisticated information sharing operations in conjunction with our partners at Carnegie Mellon University's CERT/cc. This became the model used by DHS, which eventually took over that function from us with the creation of US-CERT.

BEST PRACTICE DEVELOPMENT

One of the under-reported stories of Internet security is that we actually know how to solve much of these problems. Best Practices in various areas of Internet security have been developed in the private sector and research has empirically demonstrated that these Best Practices work: though corporations, who follow them invariably still get attacked, they can better withstand and manage the attacks suffering little if any down time or financial loss.

ISAlliance has been a leader in the development of best practices, and has published a continuing series of works that communicate those best practices to the full range of large, small, and medium size enterprises.

Unfortunately, so far, only a minority of corporations follow these best practices.

WORKING WITH THE INSURANCE INDUSTRY

AIG insurance has, in conjunction with ISAlliance, attempted to stimulate wider adoption of these best practices by offering credits on cyber insurance for corporations who comply with them. Working closely with the ISAlliance technical team and Carnegie Mellon University, AIG developed the first cyber-insurance certification tool to be used in conjunction with ISAlliance's Best Practice Guides. This tool permits companies to show that they are meeting the standards of the Best Practice Guides and are entitled to insurance credits where permitted by law.

SMALL COMPANIES

In 2004 the private sector, in conjunction with DHS, held the first national Cyber Summit. The very first recommendation to come out of that summit was that something had to be done to bring more small companies into the perimeter of a secure cyber space.

The ISAlliance was asked to create a program specifically to address the needs of smaller companies. In the past two years we have developed a separate set of best practices for them, developed a self assessment tool to assess these needs, offered private incentives such as lower insurance rates for compliant companies and created an innovative mechanism for small companies to participate in our information sharing and educational programs. Since the cyber summit, the ISAlliance has increased its reach into the small company community by several hundred new companies.

REACHING OUT TO THE INVESTMENT COMMUNITY

Next month we, along with several coalition partners such as the Council on Competitiveness and BITS, will be holding a major event at NASDAQ. The purpose of that event is to reach out to the investment community who we believe have been undervaluing corporate investment in security and business resilience. Based on recent research we hope to convince the investment community that companies who do invest in business resiliency projects are indeed better investments. That is, companies that invest in cyber security are not dumping money in to economic black-hole. Rather, an investment in cyber security not only makes a company more resilient but also produces a positive return on investment. Clearly, if we can make this case strongly it would have a major impact on increasing the market incentive for improved security.

REVIEWING CORPORATE STRUCTURES

In addition, based on a series of recent studies, we believe that in many corporations there is insufficient integration among CSO's, CIO's and Risk Managers leading to less commitment from the COO, CEO and Boards of Directors for security and resiliency investments. As a result, we are engaged in a program to get this message out and achieve results in improved corporate governance.

ADDRESSING PARTNERSHIP AND OUT-SOURCING SECURITY ISSUES THROUGH MODEL CONTRACTS

Companies who participate in organizations like the Internet Security Alliance are often also among those "best practices" companies who are actually doing a very good job of assuring the security of their own cyber systems. However, with a shared infrastructure like the Internet you are only as secure as the company with whom you are interacting. Hence, we needed to develop a market system to expand the state-of-the-art procedures we follow to all our partners including those who are based off-shore. The mechanism we chose was commercial agreements recognizing that the agreement was an inherent part of setting up shared infrastructure. We developed a set of model contract terms and conditions which provide contract trading partners with a market mechanism that assures that both sides are following the necessary procedures to assure each other's compliance, while at the same time cutting legal costs.

Our work in this model contract project was endorsed by the Information Systems Security Association, an international professional association of over 10,000 information security professionals.

COORDINATING WITH RECOGNIZED STANDARD SETTING BODIES

As a next step within the Model Contracts Project, ISAlliance is collaborating with the American National Standard Institute (ANSI). We have agreed to work cooperatively to take the adopted standards for information security programs and develop contract language that embraces these standards. We are also hoping to broaden this effort to embrace international standards, and are working with internationally based partner corporations to incorporate legal requirements in other countries.

INTEGRATION OF MULTI-FACETED SECURITY ISSUES

It is a misnomer that cyber security is a technical problem. While it obviously has many technical aspects maintaining cyber security has technical, legal, business operational and public policy dimensions. Unfortunately, many organizations are ill-equipped to address these issues in an integrated fashion leading to uncoordinated and inefficient security programs. In cooperation with our partners at Carnegie Mellon University

CyLab, ISAlliance is developing integration programs including legal/technical and business analysis coordinated with web-based education and training to improve our member's performance in their own management of cyber security as part of the business agenda.

ADDRESSING THE INSIDER THREAT

Many of the breakdowns in cyberspace (including the recent highly publicized personal security breeches on the part of agencies of the federal government) have been the function of personnel misconduct rather than technology failures. DHS Chief for Cyber Security research, Scott Borg, has reported that the single biggest vulnerability in industry is the lack of adherence of senior corporate personnel to cyber security policies and best practices. ISAlliance in conjunction with CMU and the US Secret Service has developed a separate set of best practices for addressing insider threats. This is coupled with web-based training which is also made available to Congressional and government personnel at no charge.

COOPERATION WITH INDUSTRY AND GOVERNMENT COALITIONS

The ISAlliance contributes both time and resources to support a range of voluntary industry and government coalitions such as the Information Technilogy Sector Specific Council, the Telecommunications Sector Specific Council, The National Cyber Security Partnership, and US-CERT.

B. What government Can Do

BACKGROUND

As I have already outlined, the private sector must take a leadership role in assuring the security of cyber space. Many organizations, including ISAlliance, its members, and the many coalition partners we have referred to above are doing a great deal.

But, the current level of effort is not enough.

Although research indicates that by following already identified best practices companies can make substantial progress toward mitigating the effect of cyber attacks. However, current research also suggests only about ¼ of corporations adhere to them.

The biggest obstacle is cost, weighed against perceived value.

The National Strategy to Secure Cyberspace, published almost exactly 4 years ago, correctly concluded that reliance upon government regulation in this domain was not the proper course of action. Given the ever changing nature of the Internet, it would be largely ineffective and most likely counter productive for American industry.

Yet, we have also maintained, since our comments filed in the development of that document, that there was a missing link in the strategy. While regulation would likely be ineffective, largely for the reasons detailed above, a pure voluntary program would also likely fail.

Although many have hopefully suggested that there would be a positive return on investment to cyber security spending, it has not so far been demonstrated effectively in most corporate board rooms.

Since the publication of the National Strategy, the ISAlliance has campaigned for the development of an incentive program to assure an effective and sustainable program of cyber infrastructure protection.

The road has been a long one, involving substantial dialogue and productive analysis of the alternatives available. Here are several notable activities to which the ISAlliance has contributed.

CISWG

In 2004, the then Chairman of the House Information Policy Subcommittee on Government Reform appointed a group of 45 industry executives to present a program that would take a deregulatory approach to cyber security. I was honored to serve as co-chair (along with ISAlliance COO Larry Clinton) of the Incentives Committee. We issued a series of fairly detailed reports covering issues such as best practices, educational outreach, and incentives.

WYE II

In 2005, the National Cyber Security Partnership engaged with DHS and 13 federal agencies in a series of off-site meetings built on DHS's own conference on cyber security held in December of 2004 at Wye River. The Wye II program also recommended an incentive program built on and extending the work done by CISWG.

NIPP and the SECTOR COORDINATING COUNCILS
In 2006, as part of the process in developing the National Infrastructure Protection Plan (NIPP), DHS requested that each sector form a Coordinating Council to help provide input on and eventually implementation of the Sector Specific plans that are expected to grow out of the NIPP.

As with the CISWG reports and the WYE II reports, both the IT and Communications Sector Coordinating Councils provided almost identical comments to DHS suggesting that the NIPP include the need to develop a value proposition and market incentives to improve and sustain cyber security.

NIPP ESTABLISHES THE NATIONAL SECURITY LINK FOR ESTABLISHING A VALUE PROPOSITION FOR INDUSTRY INCLUDING INCENTIVES

The NIPP was published on June 30, 2006. It embraces the notion that as a matter of national security and homeland security a value proposition for industry must be developed including the creation of economic incentives.

"The public private partnership called for in the NIPP provides for the foundation for effective CI/KR protection…The success of the partnership depends on articulating mutual benefits to government and private sector partners. While articulating the value proposition to the government typically is clear, it is often difficult to articulate the direct benefits of participation for the private sector…In assessing the value proposition for the private sector there is a clear national security and homeland security interest in ensuring the collective protection of the Nation's CI/KR. Government can engage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CI/KR protection through activates such as:…

Creating an environment that supports incentives for companies to voluntarily adopt widely accepted sound security practices" (NIPP page 9)

ISAlliance wants to thank and congratulate DHS Assistant Secretary for Infrastructure Protection Bob Stephan and Acting Cyber Security Director Andy Purdy and their staff for making this paradigm shifting assessment and including it in the National Infrastructure Protection Plan.

NOW IT'S TIME FOR CONGRESS

It is now time to move from the general notion of recognizing the national security need to develop a value proposition for industry for improved security to the much harder question, "how exactly do we do it?"

The ISAlliance does not come to the Committee today with legislative language to be introduced. That is premature today, but it may not be in a few months. What we do come to you today is specific legislature ideas which, once agreed to, will then be translated into suggested legislative language.

Congress should continue the process you have started today and hold hearings on the various ideas we have identified for creating an incentive-based security model so that we can address the issue with the attention that the national security perspective suggests.

What I can provide for the members today is a fairly specific list of suggestions that have been developed through the CISWG, WYE II and NIPP comment processes I have discussed. In brief we can identify numerous paths, most with Congressional precedent for Congressional action to provide incentives that are in the national interest. These are all appropriate for adaptation and application in the cyber security space.

Among the alternatives we believe are appropriate for Congressional review are:

1. Congress can tie incentives such as civil liability safe harbors or procurement credits to companies who can demonstrate compliance with market generated best practices for cyber security. As I previously noted, research has demonstrated that a substantial minority of corporations currently follow industry generated cyber best practices which yield empirical success. The problem is motivating more companies to adopt these procedures. In the last Congress Chairman Putnam of the Information Policy Subcommittee of Government Reform created the Corporate Information Security Working Group. The Incentives Committee of that group proposed a system though which this can be accomplished.

2. Congress can stimulate the stunted cyber insurance market. Cyber insurance can help achieve social goals by managing government risk in a cyber hurricane while providing a mechanism to maximize corporate security behavior that is dynamic enough to address the fast changing and international characteristics of cyberspace. This can be done by:

    a. Having government serve as an insurer of last resort to stimulate the market (Precedent: Terrorism Risk Insurance Act of 2002).
    b. Establish a revolving fund reinsurance system funded by taxes on insurance products (Precedent: Federal Aviation Act 1958).
    c. Requiring government contractors to purchase cyber insurance. (Precedent: Federal Acquisition Regulations)
    d. Promote cyber security information sharing allowing for the creation of better actuarial tables resulting in lower premium costs, increased competition and broader coverage. (Precedent The Year 2000 Information Readiness Disclosure Act of 1998)

3. The Congress can create an industry/government/university consortium to stimulate the needed research, development and adoption of security protocols. This will enable government, academia and industry to work together to replace today's security poor Internet protocols with security rich protocols. Congress followed a similar model (Sema-Tech) in the late 1980s to address the computer chip gap.

4. The Congress can use tax incentives to motivate corporations to adopt security practices beyond those already justified by their own corporate needs but conducive to the national and Homeland Security needs cited in the National Infrastructure Protection Plan (NIPP July 2006). (Precedent: IRS Code 26 U.S.C; IRS Code 26 U.S.C.832 (e); Energy Policy Act 2005).

5. The Government can create awards programs to highlight the contributions of corporations and senior executives who have gone beyond their own corporate interests and expended resources. In the 1980s when industry believed that "Quality" was a luxury they could not afford the federal government initiated the "Baldrige Awards" for quality which eventually became a sought after market differentiator for corporations.

6. The government can support private sector initiatives to use market forces to enhance cyber security. As noted, the ISAlliance, in conjunction with the ISSA and ANSI is developing a series of publications of model contract language that enable traditional and emerging standards of security within commercial agreements utilizing the market power of business alliances as a means to expand security. The ISAlliance in conjunction with BITS and the Council on Competitiveness is sponsoring a series of studies and forums educating the investment community as to the business benefits of security/resiliency and the corporate organizational reforms needed to expand this concept. All this is simultaneously in the public's national security interest. DHS, the Department of Commerce and other federal agencies should identify, promote and support these programs aggressively as a cost effective mechanism; doing so serves to expand their culture of security message.

I would like to thank the committee again for allowing ISAlliance to testify today and I would be happy to answer any questions the Committee may have.