Thank you, Mr. Chairman.

I am Larry Clinton, President and CEO of the Internet Security Alliance. I also am a member of the DHS's Communications Sector Coordinating Council, the Critical Infrastructure Partnership Advisory Council and serve as an Officer on the IT Sector Coordinating Council. ISAlliance is a collaboration with the Carnegie Mellon University. We are a cross-sector trade association focused exclusively on information security. We have roughly 1,000 member companies. We provide our members with a range of services, including technical, business operational and public policy.

I want to congratulate the Chairman for holding this hearing of the Information Policy Subcommittee of the Government Reform Committee because government reform is clearly what is needed, as well as some private sector reform, to provide sustainable security from a serious and growing cyber threat.

The Internet Itself Demands Government (and Industry) Reform

Government reform is not necessitated by bad faith, corruption or incompetence of people charged with overseeing cyber security. Indeed, my experience is quite the opposite.

However, we need to change the way government, perhaps including Congress, thinks about and conceptualizes its role in assuring Internet security. In its June 2006 report, "Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan," the GAO got it right. It listed as the number one challenge we face the "innate characteristics of the Internet."

We need to realize that the Internet is unlike anything we have dealt with before. Consequently, it will require a security system unlike anything we have designed before.

How then is the Internet different?

- 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 is critical to our national defense, but it is not a military installation.
- It is all these things and much, much more.

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

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

We can not simply "cut and paste" previous governance systems from old technologies or business models and realistically expect that we will be able to manage this system effectively.

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, the FTC. And, that system has worked arguably well in most instances.

But that system will not work with Internet security. Even if Congress were to enact an enlightened statute, it would not have reach beyond our national borders and hence would not be comprehensive enough. Even if some agency wrote a brilliant regulation, it would likely be out-dated before it got 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 "dumb-down" the eventual regulations so that we wind up with a campaign-finance-style standard where everyone can attest that they met the federal regulations, but everyone knows the system is really not working.

That may work in politics, but, frankly, we can't afford that when it comes to Internet security.

Yet, we can't stand idly by either. 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.

Good News: There are Steps in the Right Direction

There is actually a fair amount of good news in the cyber security field.

To begin with, there has been a marked improvement is that the working relationship between industry and government on cyber security issues is improving.

Paramount in this area is the government's growing realization of the importance of cyber security.

You may recall some of us campaigned for years to establish a senior position in DHS, an Assistant Secretary for Cyber and Telecommunications, and once it was established it took some time to fill the post. We are extremely happy that the position has been filled by Greg Garcia. Greg, working with Assistant Secretary Stephan, has ushered in an era of true partnership consistent with the directives of PDD 67 and HLS Directive 7, as well as other planning documents calling for a true public-private partnership. This new approach has been felt at the ground level by the many private sector volunteers who are attempting to assist in this effort, and we are grateful for it.

Perhaps even more important, the role of cyber security in the defense of all our critical infrastructures has at long last been recognized. Early drafts of the NIPP treated cyber security as an afterthought of the telecommunications infrastructure. It has now been realized that virtually all our nation's key resources, not to mention the economy as a whole, are dependent on cyber security. As a result cyber security is now being integrated not just into the IT and Communications Sector Specific Plans but into all the sector plans. This is certainly a step in the right direction, but many more steps within the traditional sectors need to be continually encouraged.

In addition, DHS has shown important flexibility toward the private sector in recognizing that methods they are comfortable with in assessing physical sectors do not necessarily apply when we are discussing the cyber infrastructure.

A key example has to do with the currently on-going process of developing a risk assessment methodology associated with implementing the sector specific plans. In traditional infrastructures, such as power or chemical plants, such assessments usually begin with identification and cataloging of critical assets.

This sort of "bottom up" approach makes no sense in the cyber security field. The private sector had to engage in substantial education of our government partners to demonstrate to them that, in the cyber field, to do a useful risk assessment you need to take a top down approach, starting by identifying the key functions that must be maintained, not the physical assets (which maybe interchangeable). DHS's recognition of this perspective and our joint work as partners in that direction is truly encouraging.

Second, we already know a fair amount about how to prevent, mitigate and recover from cyber attacks.

The Committee has expressed a particular interest in major disruptions. It's important to understand that a major cyber event would probably be unlike a catastrophe like Katrina in several key respects.

To begin with, we could see Katrina coming, literally from hundreds of miles away. That is unlikely to be the case with a major cyber event. Terrorists or an enemy nation state could potentially place malware on critical infrastructure hardware or software that could lie dormant and undetected for an extended period of time waiting to be triggered unexpectedly by a seemingly unrelated event and timed to the worst possible moment of crisis. The results could be substantial electronic, property and human damage.

A useful analogy between Katrina and a major cyber event is that the tragedy of Katrina was not the event itself but the inadequacy of the systems designed to handle the event. Had the levies held, or the transportation and social services been properly maintained and managed the effects of Katrina could have been far less catastrophic.

My point is that the best way to manage the risk of a major cyber event is with an ongoing program of systematic maintenance and cyber monitoring coupled with following the ever evolving state of best practices that are continually being developed and modified.

Within the marketplace, there is a robust assortment of published regulations, standards, best practices and similar guidance that has already been produced that addresses the manner in which information security is to be developed and implemented in commerce. These publications target specific nations as well as international audiences; others address the requirements of specific trades or industries. Recent research shows that following these existing practices can indeed result in demonstrable improvements in cyber security.

The largest security research project ever done, the "Global Information Security Survey" conducted by PricewatterhouseCoopers for CIO Magazine, found that about one-fifth of its respondents, dubbed the "best practices" group, report that, although they suffered more cyber incidents than the average respondent (presumably because they are more attractive targets), they had less downtime and monetary damage. Indeed, one-third of the group reported that they had zero downtime and zero financial impact, despite being targeted more often by malicious actors.

These findings provide compelling evidence that there is a substantial, though not a majority, number of "good actors" in the corporate information security field. These organizations have, through various mechanisms, identified and implemented effective information security measures. The work of these good actors should be recognized and encouraged. We also need to find a way to get broader adoption of these practices hat have been shown to work.

A third piece of good news is that there is now a robust and growing industry, as well as trade groups such as ISAlliance, focused on internet security. This is a comparatively new phenomenon.

In fact, when ISAlliance was founded 6 years ago our first services were to provide threat, vulnerability and mitigation information to the private sector through the CERT/CC at Carnegie Mellon University. It is sometimes hard to remember but way back then many people actually thought that the internet was safe and secure. The information we provided about vulnerabilities and "exploits in the wild," and advance mitigation strategies were revelations to our members.

All that is now changed. With the creation of DHS the US CERT took over the services we had provided through contracts and non-disclosure agreements to our members. The US CERT information was free to anyone, but not nearly as detailed or useful. As a result the ISA members have found the government service not nearly as useful as we previously provided.

Also since 2001, numerous vendors of threat and vulnerability information have come on the market and this sort of information is now readily available as a commodity. However, as we have moved from vulnerabilities that might have taken months to exploit to the current era of zero day attacks, just getting information is no longer nearly enough.

Our efforts to improve corporate information security have matured with the evolving threat. We now realize that information security is not simply a technical issue, though it has a significant technical component. Treating cyber security just by providing information is like treating a staph infection with a band aid.

Our members now look to us to provide a comprehensive risk management approach that encompasses the full-system approach necessary to address the problem. An example is our Enterprise Integration Program which addresses discrete cyber security issues ranging from preventing and handling breaches of personal information to securing the IT supply chain in the era of globalization.

We address these issues by looking at their technical, business operational, human resource, legal and public policy aspects simultaneously and developing an integrated solution. We would commend this fully integrated model to our government partners to consider.

Moreover, as the world has become aware of the need for security products to address a technology built on inherently insecure protocols, the private sector is responding with ever more sophisticated products and services.

For example, we now know that threats to the net have morphed from broad and often relatively benign, if well publicized, attacks like Love Bug and Blaster, to designer malware constructed to target specific systems where it can reside undetected by traditional methods for an indeterminate period of time while causing serious damage.

As a result, traditional AV software and firewall solutions are becoming inadequate. However, a new generation of security products has been, and continues to be, developed to address the continually evolving threats.