Mr. CLAY. Thank you.

STATEMENT OF LARRY CLINTON

Mr. CLINTON. I want to congratulate you, Mr. Chairman, on holding this hearing of the Government Reform Committee, because Government reform is clearly what is necessary.

The June 2, 2006 GAO Report got it exactly right. The problem is the inherent characteristics of the Internet. The Internet is unlike anything we have ever dealt with before. It is international, it is interactive, it is constantly on the attack. Consequently, it will require a security system unlike anything we have ever designed before.

We can't simply cut and paste previous government systems and put them into Internet security. Even if Congress enacted a brilliant statute, it would only go to our national borders. Even if a regulator came up with a brilliant solution, it would be outdated before you could put it into effect.

Fortunately, we need other things to attack the Internet. The committee has expressed some interest in the instance of Katrina, saying that we should model ourselves on that. There are major differences between cyber-attack and Katrina. Katrina, we could see it coming. Literally. From hundreds of miles away. The adequate analogy to Katrina is that the problem with Katrina wasn't the event itself. The problem with Katrina was that the systems weren't in place to properly handle the event.

Now, fortunately, we actually know a good deal about how to mitigate and manage a number of issues dealing with cyber security. The largest study ever conducted in this field found that the best practices group, people who follow the industry recognize best practices were able to have fewer incidents, less downtime, less financial loss.

What we need to do is find a way to get more people to follow the best practices that industry is already following. Industry is also not waiting for government to get its act together. Industry is aggressively moving forward with new products and services because, as it has already been pointed out, the problem has morphed.

We are no longer looking at these well publicized instances like Blaster and Love Bug that were designed to get publicity. Instead, what we are dealing with now are carefully targeted designer malware that can sit on a system for an extended period of time, cause tremendous damage and we don't even know it is there.

Fortunately, we are developing new systems to attack this. But there is a role for the government. And role for the government was pointed out in that 2006 GAO Report, where they pointed out that in the private sector, competitors were working together to deal with these incidents when they see that there is a direct business relationship benefit to that. And the NIPP, the National Infrastructure Protection Plan, also pointed out—and this is the one thing that I choose to read for you, Mr. Chairman:

> That the public private partnership called for in the NIPP provides for the foundation for effective critical infrastructure protection. The success of the partnership depends on articulating the mutual benefits to government and the private sector partners. While articulating the value to the proposition for the government is typically clear, it is often difficult to articulate the

direct benefits to the private sector. In assessing the value proposition for the private sector, there is a clear national security interest and homeland security interest in ensuring that the collective protection of the critical infrastructure goes beyond that of the business unit. Government can engage industry to go beyond efforts already justified by their corporate business needs and assists in a broad-scale critical infrastructure protection by creating an environment that supports incentives for companies to voluntarily adopt widely held best practices.

And I conclude my presentation by listing for you 10 steps that I would suggest that the committee consider for roles that the Government can embrace, which are not your traditional regulatory role, but are things like leading by example, using your market power instead of your regulatory power; supporting research and development that is not going to be undertaken by industry; using the market incentives that you have traditionally used in other areas; address the lack of cyber insurance; raise your aim in terms of awareness to focus on senior executives rather than individuals; adopt a coherent strategy for dealing with the private sector, something discussed before; clarify the roles and procedures for crisis management; and rethink your approach to information sharing.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Clinton follows:]

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.

Industry has committed significant resources to increasing levels of security assurance in hardware and software and the development of security enhancing new products and features.

Some of these advances are directly focused on security issues currently creating concern for government and the private sector. Technology that will be released shortly will increase the protection for data at rest through innovative use of encryption. This hardened encryption should help mitigate the risk from security failures such as lost lap tops by making it extremely difficult to retrieve encrypted data off a stolen device. In addition, companies plan to release new technology to protect against threats from malicious software, thus providing information technology departments with better mechanisms for logging onto networks which will help contain malicious software and remediate the impacted systems.

There is Still Much More to Do

Let me be very clear. Notwithstanding the fact that many in the private sector have begun to address this problem seriously, we are not nearly as far along as we need to be.

And, notwithstanding the positive steps being made in some aspects of the industry-government relationship, that relationship is far from being adequately productive.

The point I am making is that, while we know a good deal about how to improve cyber security and are continuing to work as the threat evolves, much more needs to be done.

Getting the amount of buy-in from the government and industrial users, owners and operators necessary to create a sustainable system of immediate, not to mention long-term, cyber security is still a long way off.

Fortunately, we are beginning to see a consensus emerge as to how to formulate an effective government-industry partnership, but we have yet to see much in the way of concrete actions to make that system a reality.

The most effective way to establish an effective and sustainable system of cyber security is to create an economic value proposition for all entities to continually adopt and improve state-of-the art cyber security practices.

The June 2006 GAO Report on the Challenges in Developing a Joint Public Private Partnership again provides us with a road map. That report states: "Private companies currently deal with cyber attacks and physical disruptions on a regular basis.... Infrastructure representatives also noted that in the event of a network disruption, companies that are competitors work together to resolve the disruption. They said that although the companies are competitors that they have a business interest in cooperating because it is common to rely on each other's networks."

It is also a very positive sign that the US government has recognized the fact that there is a compelling national interest in creating this value proposition for the private sector as the most effective and efficient way to improve our collective security. Specifically, the National Infrastructure Protection Plan (NIPP) notes:

> 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).

Government can provide a vast assist to this effort by fashioning an incentive program for the good actors that will create a business advantage for them over less careful players. In so doing, we hope to harness the power of the market to motivate cyber security on a worldwide basis.

The NIPP and the GAO Report show the way, but we are not yet seeing government start down this road.

The problem is that in order for government to engage industry in the sort of partnership suggested, they must rethink their role in the partnership. This cannot be a parent-child, superior-subordinate relationship. It needs to be more of a partnership wherein both sides achieve their goals.

What is Government's Role—A Top Ten List

As we discussed at the outset, the traditional government role of regulator, while appropriate in narrow instances such as consumer protection, does not fit well for broad infrastructure protection due to the intrinsic characteristics of the internet.

But if government's role is not to regulate, what is its role? Does government, specifically, does the US federal government have a role?

Yes, it does, and many in fact. While fully laying out a modernized set of roles for the US government goes well beyond my expertise and the limits of this testimony, I can offer at least a top ten list of things the US federal government ought to be doing to improve cyber security.

1. Government can lead by example. Treat cyber security within government agencies with a higher priority in recognition of its critical importance, including providing government agencies with the financial and personnel resources necessary and rewarding down to the employee review level adherence to cyber security goals and objectives which create a culture of security within federal agencies.

2. Government can use its market power, instead of its regulatory power, to provide a market incentive for improved cyber security. For example, security ought to be a true decision point in the awarding of federal contracts, along with cost, rather than a comparatively minor item.

3. Government can work with us on developing a series of market incentives to encourage greater adoption of security best practices. The National Strategy to Secure Cyber Space had it right when it noted that the market would need to be the motivator for necessary improvements in cyber defense. But markets do not spring up spontaneously. They need to be developed and nurtured. Government can, and traditionally does, have a role in developing these market incentives to address social goals such as infrastructure security. There is a range of mechanisms at the government's disposal to do this including taxes, procurement, awards programs, as well as more creative programs such as the cap and trade systems enacted to address environmental issues. ISA has developed a series of proposals which it would be delighted to discuss.

4. To mitigate against the effects of a major event, the government needs to address the lack of cyber insurance. The costs of a major cyber event have been estimated to potentially run to the tens of billions of dollars. Should such an event occur, the vast majority of the damages may have little or no insurance coverage at all, meaning thousands of businesses and potentially millions of people would be economically stranded with only the federal government as the payer of last resort. Most traditional insurance policies do not cover cyber losses. In fact one recent study showed more than half of industry CIOs either did not know if they were covered for cyber loss, or thought they were covered when in fact they were not. There are some very logical reasons why the cyber insurance market has been truncated, but not unprecedented ones. Government ought to realize that there is a compelling national interest to manage some of their own cyber risks by transferring a portion of it to the private sector. By enhancing the cyber insurance market government will also assist consumers by lowering prices, providing security and establishing an incentive lever for improved behavior much as health and car insurance are used to motivate improved health and driving behaviors.

5. Government can raise its aim in terms of its awareness efforts. The national security interest is served much more directly by addressing the senior corporate leaders about the need to better secure the information infrastructure, rather than mom and pop awareness efforts.

6. Government can develop a coherent strategy for dealing with private sector. Much like Congress, federal agencies have not coordinated their approach to dealing with the private sector. Even at DHS there appears to be one set of private sector contacts operating through the private sector office, and another through the infrastructure protection/cyber divisions. Many of us on the private sector side are contributing untold hours to meeting and coordinating with government, only to find at times that an entirely different group has been designated as the private sector contact for a particular effort or exercise. The private sector is delighted to work with our government partners, but the system needs to be made more efficient and productive.

7. Government can begin to look at cyber security as a broad international issue, not a narrow US federal government issue. The bifurcated international approach on cyber security is inadequate. It focuses too much on a narrow group of countries and primarily on a government-to-government basis. Given the fact that cyber attacks inherently cross multiple borders, this government-centric approach has limited utility. A more productive approach would be to give greater priority to US-based multinational corporations and to those of allies whose systems transcend national borders to provide a pathway to global system security.

8. Government must clarify the roles and procedures for crisis management and enact any necessary legislation to address pending issues. Now, years past Katrina, there is still unresolved issues such as a lack of assurance that critical infrastructure providers such as those who operate the internet will have access to needed resources and that clear lines of communication have been established between government and industry in the case of a major disruption.

9. Government can support R&D into government-level issues that will not likely be addressed by the private sector. For example, many experts have noted that the TCP/IP protocols upon which the internet is based are inherently insecure. A heavy lift R&D effort by the government to write and implement truly secure protocols, a project that may take some time, is an appropriate role for the government. Use of creative models such as the Sema-Tech model used to attack the 1980s issues with computer chips might be useful models.

10. Government can rethink its approach to information sharing. The traditional model is to withhold information and disclose if necessary. The lack of sharing of information, and government requirements for treating corporate information once disclosed, is one of the major reasons that the necessary trust environment has not been established and the information sharing regime is widely held to be inadequate by all sides.

Mr. CLAY. Thank you so much, Mr. Clinton. The committee will now recess for the duration of these votes on the floor. They tell me it will be about half an hour. I am sorry. The committee stands in recess.

[Recess.]

Mr. CLAY. The committee will come to order. Ms. Allen.

STATEMENT OF CATHERINE T. ALLEN

Ms. ALLEN. Thank you, Chairman Clay and members of the subcommittee and committee for the opportunity to submit testimony before you today on private and public sector efforts to secure our Nation's Internet infrastructure.

The Santa Fe Group does a lot of work for the industry and still for BITS. I am actually going to go directly to the recommendations because of the time.

And what I am suggesting is that the financial services industry has done a great deal to strengthen business continuity, planning and coordinate prior to and during times of crisis. We have business continuity plans which are constantly updated. We refine and test them, and this is a regulatory requirement, and part of our risk management process.

Most financial institutions, in fact, all that are deemed mission critical are required by our regulators to have recovery operations in place and back-up in a very narrow timeframe. And this requires telecommunications, it requires power and it requires dependency upon IT. If any of those are not working, we cannot meet our regulatory requirements.

I would be the first to tell you that we have a long way to go as an industry, but there is much of what we do that we believe could be copied or modeled for other critical infrastructure industries.

We have a very successful FS-ISAC, Financial Services ISAC, and FSSCC, a coordinating council for critical infrastructure protection. We work very closely with our regulators through the FBIIC and with the Department of Treasury in coordinating on everything from Katrina to the power outage after 9/11.

Most recently, we ran a pandemic exercise which included a component that looked at if the Internet was down and we had many people working from home, what would that mean.

And I would say that the two most important things that we have done related to Internet recovery are the work that we did on business critical telecommunications services, where we developed best practices, not only for the financial sector but for the telecom sector, upon which we are extremely dependent, to make sure that they had the diversity and redundancy that we needed.

We also finished a business critical access to power. We did this with the power industry, again to look at best practices for alternative power if there was disruption in any of the IT industry.

Last, we worked in managing third-party service providers. Much of the Internet is dependent upon third parties, many of whom are located in India and China and other places. So, looking at how we manage those. Those are all models for other industries.

The recommendations that I have are, recognize that other industries may need to share the same level of responsibility and li-