DRAFT TESTIMONY
LARRY CLINTON, PRESIDENT INTERNET SECURITY ALLIANCE
HOUSE SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET
MAY 1, 2009

Mr. My name is Larry Clinton. I am President of the Internet Security Alliance (ISA). The ISA is a cross-sectoral, international trade association operating in collaboration with Carnegie Mellon University. Our mission is to integrate information security technology, business practices and public policy to create a sustainable system of cyber security. It is a privilege to be here.

The Problem

At her confirmation hearings two months ago, Secretary of State Hillary Clinton said that the single biggest threat to our country was the proliferation of weapons of mass destruction, and she identified four categories of these weapons: nuclear, biological, chemical and cyber.

The former Director of National Intelligence Advisor to President Bush, Mike McConnell, has argued that "the ability to threaten the US money supply through a cyber attack is [the] equivalent of today's nuclear weapon."

Just 10 days ago, Melissa E. Hathaway, Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils, previewed the report on cyber security she has provided to President Obama by saying: "The Internet is neither secure enough nor resilient enough for what we use it for today and will need into the future. This poses one of the most serious economic and national security challenges of the 21st century."

The cyber security threat is much more serious than the well publicized massive losses of personal data. There are now recorded instances of our government and industry's electronic infrastructure being compromised by criminals, nation states and even potential terrorists. The result of such attacks could be disastrous ranging from the possible shutting down of our electrical grid to having our own military weapons turned against us.

On a purely economic basis, if a single large American bank were successfully attacked, it would have an order of magnitude representing a greater financial impact on the global economy than September 11. But the threat is not just speculative. Today, cyber security injuries are already substantial: some estimates now place the economic loss from known cyber thefts at more than $300 million per day.

What We Are Talking About

There are a multitude of cyber security issues being simultaneously discussed in government and industry circles, so it may be useful to begin by placing some boundaries around our testimony.

While many of the solutions the Internet Security Alliance (or ISA) is advocating today have broad impact, our comments today relate primarily to what we call the critical infrastructure protection issues (e.g., protecting the infrastructure, corporate networks and corporate data assets against corporate espionage, Cyber terrorism and Cyber warfare) rather than the "consumer issues" (e.g. privacy/spam etc.).

In addition, there is a good deal of discussion about how the federal government ought to be organizing itself to address the cyber threat. While, as citizens we naturally have our own opinions on our government, as a private sector witness before the Committee representing the ISA, my testimony is focused on how the government ought to partner with the private sector to achieve a national security goal of cyber security, and not how the government chooses to deal with its own internal organizational issues. They are critical issues, but we feel it is vital to emphasize the importance that government place on the role of the private sector as a strong partner in achieving national security goals.

The Energy and Commerce Committee's Role

The President's economic initiatives are wholly dependent on the cyber infrastructure. Indeed virtually every element of modern life is now dependent on the digital infrastructure and the vast majority of the electronic infrastructure is in the hands of the private sector. As a result of these facts, our nation's economic and national security relies upon the security of the assets, properties and operations of the private sector. The interdependency is unlike anything our nation, or any nation, have previously faced in building effective protective strategies.

Traditionally, economic decisions have been made without considering cyber security. Similarly, cyber security decisions have been made without considering their economic impacts. We are now at the point where we must realize that economy and cyber security are opposite sides of the same coin. We cannot address one issue without the other.

Unfortunately with respect to cyber security, virtually all the economic incentives favor the attackers.

Attacks are cheap and relatively easy to conduct. Profits are enormous. The defensive perimeter is virtually endless and defensive measures are expensive

If we are going to develop a sustainable and evolving system of cyber security, we will need to address, and alter, the economics of cyber security.

Moreover, the fundamental reason our systems are currently insecure is that, while private sector organizations will usually invest to protect their own electronic and computer networks and systems, they do not invest adequately to achieve progress

against the broader national security objectives which are properly the government's responsibility. Addressing this imbalance must be part of our solutions in altering the economics of cyber security.

Private corporations are supported by public policy to invest in order to maximize shareholder value, but, in today's environment, maximizing shareholder value does not necessarily equate with government's priorities or government's responsibilities.

The National Infrastructure Protection Plan makes this exact point:

"While articulating the value proposition to the government is clear, it is often more 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 and homeland security interest in ensuring the collective protection of the nations Critical Infrastructure and Key Resources (CI/KR). Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad scale CI/KR through activities such as….creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted sound security practices."

The Energy and Commerce Committee, with its jurisdiction over so many of the critical infrastructures, including telecommunications, Internet energy, health care as well as commerce trade and consumer protections stand at a critical intersection between economy and security. It is the Energy and Commerce Committee, starting with the Telecommunications and Internet Subcommittee, that is positioned to take aggressive action to provide the market incentives needed to generate private investment in cyber security that goes beyond that demanded by individual business needs and extends this investment to advance against, and helps achieve, our broader national security needs.

<u>The Good News Part One</u>

The first piece of good news is that the Obama administration seems to be embracing the concept that we need to alter our approach to cyber security to include an overall appreciation of the economic aspects of the problem. The administration recognizes the need to enhance market incentives for private corporations to address the broader national security issues raised by our current cyber vulnerability.

When the Obama Administration was elected, the ISA Board proposed a bold new direction in cyber security. Our approach was modeled on the Social Contract that was the underpinning of the development of public utilities, such as power companies and telephone networks a century ago. Our proposal for a Social Contract has been previously submitted to the staff of this Subcommittee.

We advocated that government again engage industry at the business plan level and make it in private corporation's best economic interests to enhance their infrastructure creating a secure cyber network in the public interest.

A century ago, infrastructure development was critically needed and was accomplished in this nation by essentially guaranteeing the return on investments the private sector would need to make. Consumer interests were protected with price and service regulation. In the current environment, the government needs industry's help not to build out the infrastructure, but to secure it.

Just as before, the economic facts demonstrate that generally speaking there is simply not a sufficient return on investment for the private corporations to make the extensive cyber security investments needed to address the broader national interests. Therefore we have advocated a new social contract be struck for cyber security that will, for the first time, address our cyber security issues from as much an economic as a technical perspective.

Just over 2 months ago President Obama assigned Melissa Hathaway of the NSC to conduct a 60-day review of our nation's cyber security status. While the report has not been made fully public, Ms. Hathaway did give a preview a week ago in Silicon Valley.

Among the specifics from the report that she did share was acceptance of the principle that "Previous attempts to deal with cyber security in isolation have failed, in no small part, because they were perceived to be in conflict with the broader societal goals of progress and innovation, civil liberties and privacy rights… Cyber security only succeeds in the context of broader economic progress.'

In addition, Ms Hathaway specifically cited the need to work with the private sector "to improve market incentives" for better research development and security management.

This is an important distinction from previous policy. Under the National Strategy to Secure Cyber Space approved in 2002, it was assumed that market forces would simply emerge and that corporations would see the efficiencies of cyber security investments and makes such investments substantial enough to protect the entire infrastructure.

ISA differed with that belief in 2002, and we have persistently asserted that the missing link in that strategy is the lack of market incentives and the need for a public private partnership to create and sustain those incentives.

According to the largest industry survey of cyber security, conducted each year by PricewatershouseCoopers, a substantial minority---perhaps as much as 1/3 of corporations—will adopt industry best practices completely on their own volition because they see it as good business practice.

However, the majority of private sector entities still regard cyber security investment as a cost center and, while they will make investments consistent with their business plans, the investments are not sufficient to address the broader problem.

Among the alarming findings of recent studies are:

29% of senior executives did not know how many security events their firms had
50% of senior executives don't know how much money was lost from attacks
Only 59% of respondents attest to even having an overall security policy
Nearly half don't know the source of information security incidents
Only half of respondents provide employees with security awareness training
Only 43% audit or monitor compliance with security policies
Just over half of companies (55%) use encryption; 1/3 of don't even use firewalls
Only 22% of companies keep an inventory of all outside party's use of their data

It is now apparent that the approach in the earlier National Strategy has not worked sufficiently. The laissez faire approach of the National Strategy is inadequate. The security of the Internet can not be left to the invisible hand of the market.

There is considerable debate as to why this finding remains fairly constant. Some say it is a lack of appreciation of the problem. Some say it is the inherent distributed nature of cyber threats, where the host of vulnerability may not be the target of the attack and hence there is not a justifiable return on investment from that particular entity's perspective.

While such a debate may be interesting for some, the ISA regards it as of secondary importance to the issue at hand. The cyber threat to the nation is so real and so dramatic that continuing to debate macro level issues we probably can not resolve quickly is not time well spent, especially when there is so much good that can be done so quickly.

Good News Part II

Fortunately we know a good deal about how to protect our cyber systems; we are just not doing it.

Robert Bigman, the CIA's Chief of Information Assurance told attendees at the October 2008 Aerospace Industries Alliance meeting that, contrary to popular belief, most attacks was not all that sophisticated. Bigman said that with the use of "due diligence" between 80 and 90% of attacks could be prevented. "The real problem is implementation."

Independent research also shows that, when companies follow well established practices of security, they can dramatically reduce the effects of attempted cyber incursions

The "Global Information Security Survey" conducted by PricewaterhouseCoopers found that organizations that followed best practices had reduced downtime and financial impact, despite being targeted more often by malicious actors.

An almost identical finding was reported in the "2008 Data Breach Investigations Report" conducted by Verizon. This study of over 500 forensic engagements over a four year period (including tens of thousands of data points) concluded that 87% of known

system breaches could have been avoided if reasonable security controls had been in place.

Why the Traditional Regulatory Model Won't Work

A common theme from some policy makers who are relatively new to the severity of the cyber security problem is to say, "Well if industry won't do this on their own we will just have to regulate them." ISA believes such an approach is short- sighted and does not reflect a necessary understanding of the new breed of technology and issues created by the Internet.

To begin with, the Federal regulatory mandates are best designed to combat corporate malfeasance, but that is not the problem we face with cyber security.

The problem we have is lack of sufficient investment in cyber security. Regulations will add cost and may not improve security. By adding cost to US firms it may even be counterproductive.

Additional reasons why a centralized US regulatory model will not work are:

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.
A US law could put US industry at a competitive disadvantage in a global marketplace at a time we can least afford it.
Specific regulations would be too static as technology and threat vectors change.
An effort for flexible regulations may be too general to have real effect.
Regulations may be weaker than needed due to constant political pressure.
Minimum standards can become de facto ceilings (e.g., campaign finance).
It would be extremely difficult to enact legislation, wasting valuable time.

A Model for Addressing the Immediate Problem Immediately

For analytical purposes in proposing a model for moving ahead, we will divide cyber threats into two categories. First is the ultra-sophisticated attack such as that carried out nation-state to nation-state, perhaps targeted at high value government targets. Addressing these attacks require specialized longer term interventions which are addressed later in this testimony.

The following part of our analysis deals with the second, much larger, category of risks, which comprises the vast majority of attacks both upon government and private enterprise resources and assets. These are the risks associated with known threats and vulnerabilities for which existing best practices can be a strong defense.

The research, as well as expert testimony, informs us that existing technologies and best practices can and will resolve or mitigate large portions of our core cyber security problem, namely our vulnerability to known cyber attack methods and tools. However,

there are multiple different sets of technologies, standards and practices in the marketplace. While the patterns of attacks and threats are constantly changing, there is consistency in the types of resources to deploy as effective defenses. To build an effective and sustainable system of cyber security that advances our national objectives, three items must be considered:

A. How are we to establish which standards and practices and technologies are to be encouraged?
B. What do we encourage compliance with the approved standards, practices and technologies?
C. What is the best way to measure compliance in order to award benefits?

Standards of Care Ought to be Based on What Works

There is a tremendous similarity in the business and security practices the research indicates work against vulnerabilities and risks.

The PricewaterhouseCoopers world wide study of more than 10,000 corporations isolated 7 items which characterized their "best practices group" which almost entirely escaped the effects of attacks on their systems"

a) Spend on Security ---best practices companies tended to spend nearly 30% more on information security than the average organization.
b) Separate information security from "IT." Cyber security is not an IT issue, it is an enterprise wide risk management issue and successful firms treat it as such.
c) Penetration testing quarterly to patch up network and application security.
d) Conduct security audits to identify threats to employees and corporate IP.
e) Complete a comprehensive risk assessment to classify, prioritize threats and vulnerabilities.
f) Define an overall security architecture and plan based on the previous steps.
g) Conduct quarterly reviews with metrics to measure effectiveness.

The 2008 Verizon study evaluated 500 forensic investigations over a 4-year time period and found in 87% of the cases, compliance with 10 practices that worked could have prevented the attempted breach from being successful. Their lessons were:

a) Align process with practice. In 59% of breaches organizations had policies in place that may have prevented the breach, but failed to follow them.
b) Achieve the essential then worry about the excellent. 83% of breaches were achieved by attacks not considered highly difficult to handle, but many organizations were apparently so focused on stopping sophisticated attacks they failed to take care of the basics.

c) Secure business connections with partners. Nearly 40% of breaches were associated with business partners and might have been prevented with basic business partner facing security practices.
d) Create a data retention plan. 66% of breaches involved data the victim didn't know was on the system. A comprehensive plan ought to force organizations to understand where their sensitive data is and take appropriate steps to protect it.
e) Control data with transaction zones. Once data is properly categorized it can be places in an appropriate zone to allow for more sensitive data to receive more comprehensive security.
f) Monitor event logs. In 82 % of cases studied, information about events leading up to the attack was available and either went unnoticed or not acted upon.
g) Create an incident response plan. If and when a breach is suspected an effective response plan can ensure that the breach is stopped before data is fully compromised.
h) Increase awareness among employees. Increased awareness can increase timely reporting and prevent incidents as well as assist in mitigation and recovery.
i) Engage in mock testing, on a mandatory and routine basis.

Government's Role

Government's first role (apart from getting its own house in order) ought to be to encourage the broader adoption of the security practices that have already been demonstrated to be effective.

This encouragement should take two forms. First, entities, beyond the early adopters of these effective best practices, should be encouraged to emulate them and adopt these, or appropriately similar, practices. Second, the already-identified effective practices need to be continually adapted to keep pace with the changing technological and security needs that are inherent parts of the cyber-landscape.

Government can provide vast assistance to this effort by fashioning an incentive program for the good actors that will create a business advantage for them over less careful players by rewarding positive behavior (similar to how doctors and hospitals are receiving economic incentives to adopt electronic patient records). In so doing, the power of the market can be harnessed to motivate improved cyber security. Since many of the organizations targeted are in fact international, improvements on a worldwide basis are possible.

Part of such a program ought to be an evaluation component which will provide a real world replication study of these practices and revisions based on these follow up studies. Evaluating and measuring results is a powerful contribution to continually improving security practices.

Government ought to identify multiple entities (both public and private) which would be able to identify standards and practices that would be eligible for market incentives.

It is important that the government not set a single set of standards. Government can be subject to political pressure, and can be challenged to deal with the vast and ever-changing array of needs companies actively contributing to the US economy, many not US-based, may face. In addition there may likely be strong international resistance to standards solely determined by the US government. Perhaps more important, the notion of one size fits all does not recognize the reality of multiple business sizes, cultures, regulatory regimes degree of criticality within the infrastructure and business plans.

Our model contemplates that government encourage security adoption by defining targets of effectiveness to be achieved and providing incentives that are awarded based on achieving those objectives. It would be more appropriate to establish a tiered set of standards and practices that would allow companies to balance the criticality of the information they are protecting with their investment tolerance. We will protect an education system or a social network differently than we will protect our critical energy infrastructure or a military C2 network. Standards would naturally be different for each, so a tiered standard set that would recognize different levels of security and risk management is appropriate.

The various tiers could them be mapped to the qualifying incentives to these various levels of compliance (e.g. level "x" yielding tax incentive "a" and level "y" yielding tax incentive "b").

Government's interest is not in assuring compliance with any particular set of technologies, standards or practices, but rather achieving the efficacy of the intervention. Therefore, it makes little difference how the industry meets the effectiveness levels established as qualifying for the incentive, but simply that their investments are judged as effective and deserving of award of the available incentives.

The government's second role would be to select and fund independent research of the interventions created by the approved agencies. Entities would be able to remain on the list of qualifying standard and practice setters only based on the efficacy of their standards as determined by independent studies.

At the outset we propose companies have available federal incentives if they implement information security pursuant to and meet the:

- Information security procedures adopted by a Federal sector-specific regulatory agency.
- Standards established and maintained by the following recognized standards organizations:
    - International Standards Organization
    - American National Standards Institute
    - National Institute of Standards and Technology
- Standards established and maintained by an accredited security certification organization or a self-regulatory organization such as NASD, BITS, or the PCI structure.

- Private entities such as insurance and audit forms who can demonstrate either a financial interest in quality compliance or independent research.

Creating Incentives for to Promote Good Security Behavior

The application of good standards is a measure of due diligence not ironclad security.

Moreover, for both large and small companies, it is often difficult to find the money to implement desired security practices across the organization when there is no apparent business return on investment. Since securing the infrastructure writ large is the government's responsibility, an incentive system needs to be put in place to assure that private companies will meet this need in the absence of a purely business reason to do so.

The notion of providing market incentives for industry to accomplish pro-social needs as a proxy for the government exists broadly throughout our economy and history with the original social contract being only a paradigm case. We simply have not yet applied these principles to cyber security.

The following is a list of incentives, many of low or virtually no cost to the public, which can be used to alter the economic perspective with respect to investment in cyber security procedures and thus encourage private entities to improve their security posture in the broad national interest.

1. Create a Cyber Safety Act. The SAFETY Act, passed after 911 to spur the development of mostly physical security technology by providing marketing and insurance benefits, could be adapted to provide similar benefits for the design, development and implementation of cyber security technology, standards and practices.

   By designating or certifying organizations under the SAFETY Act for developing or using cyber security technology, practices and standards, these organizations can similarly use the marketing and insurance benefits, thus providing business benefits to extending their cyber security spending beyond what is initially justified by their business plans. The program has been successful in the physical arena. [any examples???]

2. Tie federal monies (grants/SBA loans/stimulus money/bailout money) to adoption of designated effective cyber security standards/best practices. Using model described above for selecting standards and practices make on-going eligibility for federal grants and loans contingent on compliance with identified security practices. This is a proven and successful method for advancing broad policy objectives (e.g., non-discrimination in employment).

Among the benefits of this approach is that there is no significant impact on the federal budget since this money is already designated for distribution. There is also the potential for relatively immediate impact since it utilizes current standards, practices and government programs. In addition this approach allows for adaptation to future needs since most applications must be periodically renewed. Finally, a renewal process in place for these types of government contracts allows for compliance testing as a means of approving and continuing the contract... The reach of the positive effect of this approach will go beyond major players to include broader universe of suppliers and contractors to CI/KR.

3. Leverage Purchasing Power of Federal Government. Government could increase the value of security in the contracts it awards to the private sector, thus encouraging broader inclusion of security in what is provided to government.

This approach could facilitate broad improvement of the cyber security posture among CIKR owners and operators by "building in" security from the beginning in products and services that are developed and delivered to the government. If the requirements were extended to suppliers and sub-contractors as well, this initiative could have a significant affect on down-stream entities as well.

While this approach does have substantial potential benefit, government would need to enhance the value of the contracts since not all the organizations in the supply chain have the same massive incentive to adopt government specifications that some large players do. This approach has potential for real and immediate benefit, but it is important that government realize that such compliance cannot be expected to come "for free". National security has a cost and it is the government's responsibility to pay it.

4. Streamline regulations/reduce complexity. Regulatory and legislative mandates and compliance frameworks addressing information security, such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act, and state regimes could be analyzed to create unified compliance mode for similar items & eliminate any overlaps. Sector specific requirements could be identified, of course, but effective security has many similar elements. Duplicative regulations impose a cost on industry that ultimately increases their resistance to prioritizing compliance.

If compliance with one set of regulations were to be considered as compliance with all, the reduction in compliance costs would allow for the freeing of resources to be returned to security as opposed to compliance efforts.

5. Tax incentives for development of and compliance with cyber security standards practices and use of technology. Using our model described above for selecting standards and practices, the receipt, and on-going eligibility for, tax credits can be made contingent on compliance with identified security practices.

While tax incentives are often difficult politically, this approach may be targeted to smaller and medium-sized businesses. SMEs are a weak link in the cyber security supply chain and may otherwise never perceive compliance with effective cyber security practices to be economically beneficial.

6. Grants/Direct Funding of Cyber Security R&D. The Federal Government could give grants to companies developing and implementing cyber security technologies or practices. Alternatively, R&D could be run through one or more of the FFRDCs. This would reduce the private-sector cost of developing and deploying cyber security technologies.

7. Limit liability for good actors. The Federal Government could create limited liability protections for certified products and processes, such as those approved under the modified SAFETY Act proposal, or those certified against recognized industry best practices. . Alternatively, liability might be assigned on a sliding scale (comparative liability), such as limiting punitive damages but allowing actual damages and providing affirmative defenses with reduced standards (preponderance of evidence vs. clear and convincing etc.).

Liability costs are among the most sensitive issues confronting senior corporate executives and a long-standing target for reform. Tying adherence to best practices and standards to a limitation in liability might be extremely effective in building a business case for extended cyber security investment. There is no such thing as perfect security, but one of the biggest concerns within industry is that, despite making the best possible investments in security, a court would still impose liability for a one-in-a-million hostile attack that succeeds. That outcome is not in the best interest of the public policy of improving security.

In making this proposal, our objective is to provide incentives to those who make authentic investments in improved security, consistent with the standards and best practices that are incorporated into an overall Government program. That objective stands in contrast to those who may argue that there should be no liability at all.

8. Create A National Award for Excellence in Cyber Security. The Government could create an award for companies that adopt cyber security best practices (e.g., the Malcolm Baldridge Award by the Department of Commerce).

This is a low cost effort with substantial benefits. Organizations may strive to receive the award as a means of differentiating themselves in marketing; consumers will value companies that have this type of recognition, particularly in a marketplace in which their security concerns continue to increase.

9. Promote Cyber Insurance. Cyber insurance, if more broadly utilized, could provide a set of uniform and constantly improving standards for corporations to

adopt and be measured against, while simultaneously transferring a portion of risk the Federal government might face in the case of a major cyber event. Insurers require some level of security as a precondition of coverage, and companies adopting better security practices receive lower insurance rates. This helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cyber-security. The security requirements used by cyber-insurers are also helpful.

With widespread take-up of insurance, these requirements become de facto standards, while still being responsive to updating as necessary to respond to new risks. Insurers have a strong interest in greater security, and their requirements are continually increasing. As well as directly improving security, cyber-insurance is enormously beneficial in the event of a large-scale security incident.

Insurance provides a smooth funding mechanism for recovery from major losses, helping to businesses to return to normal and reducing the need for government assistance. Finally, insurance allows cyber-security risks to be distributed fairly, with higher premiums for companies whose expected loss from such risks is greater. This avoids potentially dangerous concentration of risk while also preventing free-riding Insurance companies can also provide a market based monitoring and assessment function thus reducing the cost to the government while assuring compliance with ever increasing standards and practices.

The Government could assist in bringing about these changes by (1) creating a Cyber-Safety Act as I discussed earlier, (2) fund or support necessary R&D efforts by the insurance industry, (3) provide temporary "reinsurer of last resort" support in cases of massive cyber events (so called "cyber-hurricanes"), (4) require cyber-insurance for those contractors that touch governmental data or systems and (5) encourage the purchase of cyber-insurance thorough use of the "government podium".

How Best to Monitor Compliance

It is sometimes blithely asserted that if the private sector doesn't do a better job of cyber security the government will simply have to regulate them.

Often these assertions are followed by suggestions that Sarbanes/Oxley/GLB or HIPPA standards could simply be expanded.

Leaving aside the broad policy problems with these simple solutions which are articulated above, research suggests that such expansion of government regulation is unlikely to succeed even if enacted.

The previously referenced PricewatershouseCoopers study reported in the October 2008 edition of CIO Magazine that only "44% of respondents say they test their organizations for compliance with whatever laws and industry

regulations apply." The study notes that this is an increase in compliance, but it is extremely noteworthy that several years after these laws and their regulations (such as HIPAA and Sarbanes-Oxley) have been in effect, less than half of the surveyed companies are even testing for compliance.

CIO magazine goes on to note "many organizations aren't doing much beyond checking off the items spelled out in regulations---and basic safeguards are being ignored" (which is consistent with the findings of the 2008 Data Breach Investigations Report cited earlier).

The federal government's lack of success in getting federal agencies to meet their own FISMA requirements also suggests this is not an area the federal government does well. It is impractical for the federal government to take on the massive role of determining, monitoring and constantly adjusting cyber security requirements funded only by tax dollars.

Far more practical would be for the federal government to use its resources to establish a functional private sector system which the federal government could participate in and where necessary regulate. Insurance companies are the best available vehicle for such a program.

The insurance industry is in a uniquely motivated to understand and communicate to its insured's what are the standards of due care appropriate for the management of network security because they have "skin in the game". That is to say, in the event of a loss it is the insurance company that will pay excess of any self-insured retention, and any damages to third parties as well as reimburse the policyholder for any loss of business and additional expense associated with the event.

A robust cyber insurance industry, operating under traditional regulatory regimes, could serve the public interest by providing a mechanism for continually upgrading security practices and standards, monitoring compliance and reducing governments risk exposure in the event of a cyber hurricane.

Longer Term Issues and Solutions

While the model outlined above would make substantial progress in addressing the vast majority of current cyber risks, there remain a range of sophisticated issues which will not be adequately addressed by implementing best practices.

As part of the process for Melissa Hathaway's 60-day review Board members of the Internet Security Alliance provided policy papers addressing some of the more difficult issues for the nation. These papers are provided as appendices, but are summarized below:

A Model for Cyber Protection by Disrupting Attacker Command & Control Channels
Jeff Brown Raytheon

There is no way to prevent a determined intruder from breaking into a system that uses e-mail and web surfing and no business can survive without these tools of the information age. Raytheon CISO Jeff Brown proposes that in addition to focusing on preventing attackers from getting into your system we should also focus on detecting and disrupting the attackers command and control communications back out of our networks, thereby leaving them unable to exfiltrate vital data. While some of the process Raytheon uses in effecting this strategy are probably practical only for firms with the size and resources of a Raytheon some of the collaborative processes Raytheon uses are practical for organizations of all sizes. There are substantial incentives for participation at all levels with implications for government industry relations, private sector models of threat and vulnerability detection and information sharing.

Information Security for the Next Century
Dr Pradeep Khosla Dean Carnegie Mellon University Engineering and Computer Science

Operating from many of the same premises as Jeff Brown, Carnegie Mellon University's Dr. Pradeep Khosla also suggests the need for approaching information security through an entirely different model. Dr. Khosla suggests an information centric approach which shifts the focus of protection from the devices (computers/USBs etc.) and instead seeks to secure the data itself with security policies are applied to the data itself with the policies embedded in the data thus making it self-protecting. Dr. Khosla argues that with the rise of virtualization information security will inevitably become information centric.

Securing the Globalized IT Supply Chain a Strategy and Framework
Scott Borg Director US Cyber Consequences Unit

There is a serious danger that the supply chain for electronic components, including microchips, could be infiltrated at some stage by hostile agents. These hostile agents could alter the circuitry of the electronic components or substitute counterfeit components with altered circuitry. The altered circuitry could contain "malicious firmware" that would function in much the same way as malicious software. If the electronic components were connected to any network that enemy attackers could access, the malicious firmware could give them control of the information systems. A logic bomb in a weapons system could shut down the larger information system or, worse, turn the equipment controlled by the information system against those operating it.

Once malicious firmware has been inserted into electronic components, it can be almost impossible to detect. Because it is in the hardware, the malware will remain in place even when all the software has been upgraded or replaced. Building on a series of conferences ISA conducted with Carnegie Mellon US Cyber Consequences Director Scott Borg describes a strategy and framework though which this complicated technical and economic problem can be managed long term.

Adapting 20th Century Regulations to the 21st Century Technologies
Jeffry Ritter, CEO, Waters Edge Consulting

Governments, corporations and the courts have struggled to interpret the applicability of privacy statutes enacted in the 1980s and 1990s to the rapidly evolving technologies and communication services that have been built upon the platform of the Internet. Many of the critical words used in the 20th century laws have proved difficult to apply to 21st century technologies—key terms such as "intercept", "record", "monitor", "electronic communication", "contents", "transmission" were not drafted with a focused capability to adapt to evolving Internet services.

At a time in which US companies are desperately looking to find new operational efficiencies and improve their competitive capability in a global, wired market, the existing legal issues created by these 20th century laws are inhibiting sound, productive investments in UC solutions. Simply stated, companies are genuinely concerned that they are unable to employ modern, conventional Internet security services across UC solutions without exposing themselves to legal sanctions and possible prosecution. WatersEdge CEO Jeffrey Ritter outlines the study he has taken at the request of the ISAlliance Board to develop business models to adapt to this confusion which may yield policy implications as well.

Technology to Enable Effective Information Sharing
Joe Buonomo, President Direct Computer Resources

Even though, Government is uniquely positioned to coordinate intelligence collection and analysis and provide sanitized threat and vulnerability information to the private sector there has been a certain reluctance not to do so because of the classified nature of the information.

Joe Buonomo, of Direct Computer Resources, Inc. (DCR), believes that there is currently industry-proven, off-the-shelf technology that has become widely available in recent years which can ameliorate this reluctance and incline Government to make this information more readily available to the private sector.

Although this technology in itself won't instantly resolve complex issues in government any more than it does for industry, DCR contends that it will provide a means through which any government agency can safely provide selected critical information to another or to industry sectors on a need-to-know basis and without exposing classified data. Allowing the free flow of critical information on a timely and secure basis should provide government agencies and the private sector with enough time necessary to react to a potential threat and nip it in the bud.

Thank you Mr. Chairman I will be happy to answer any questions the Committee may have.