TESTIMONY OF LARRY CLINTON,
PRESIDENT AND CEO OF THE INTERNET SECURITY ALLIANCE

UNITED STATES SENATE JUDICIARY COMMITTEE
NOVEMBER 17, 2009

Good morning. I am Larry Clinton, President of the Internet Security Alliance (ISA). I want to thank the Judiciary Committee for inviting me to testify today.

ISA was born in 2001, in collaboration with Carnegie Mellon University, as a trade association of major business users of internet security services. ISA is organized like the internet. We are international in our membership, with members on 4 continents, and we are cross-sectored in our representation. ISA represents members of the banking, insurance, defense, manufacturing, business integration, information technology, and telecommunications industries.

The ISA mission is to integrate advanced technology with both the pragmatic business imperatives of the owners and operators of the Internet - namely the private sector - and enlightened public policy to create a sustainable system of cyber security.

In November of 2008, the ISA published its policy recommendations for the 111th Congress and the Obama Administration: the Cyber Security Social Contract. Through this document we argued that, in the last century, when the hot new technology was phones and electricity, policy makers wisely realized that there was a public interest in universal phone and electric service and that universal service would not be achieved unless the government used its economic powers to intervene.

As a result, the government made a deal, a social contract, with the private sector providers of these services that essentially guaranteed the return on their private investment if that investment would service the public policy goal of universal service. That particular use of market incentives for private infrastructure investment worked, and it provided the basis for a century of American industrial and military prominence.

We have a similar situation today, in the fact that we need universal cyber security. Due to the interconnectedness of the system, one entity's insecurity

can cause tremendous harm to others downstream, including the government and the nation as a whole. Government will need to motivate private investment in infrastructure upgrades to serve this national interest.

ISA was delighted when President Obama came out with his Cyber Space Policy Review in May of 2008 especially because the first item quoted in that document was the ISA Cyber Security Social Contract.

In fact, the Executive Summary to the Administration's document both begins and ends by citing ISA documents, and the Cyber Space Policy Review goes on to cite more than a dozen other ISA white papers and submissions---far more citations than from any other source.

Naturally, ISA supports the Administration's Cyber Space Policy Review for a wide variety of reasons.

First, the President is correct in his appreciation of the need to view cyber security as not just a technical and security issue, but as an economic one as well. Notwithstanding the delay in appointing a cyber coordinator, we believe that it is absolutely correct to design that position with a line of authority to the National Economic Council, as well as the National Security Council.

In the 21st century - the digital century - economics and security are opposite sides of the same coin. You cannot affect one without impacting the other.

Second, in his White House speech on cyber security, the President was absolutely correct when he said he was opposed to regulatory, mandated standards on the private sector for cyber security. Federally-imposed mandates on the broad private sector will not work and will be seriously counterproductive to both our economic security and our national security.

Third, the Administration's Cyber Space Policy Review takes the right approach in advocating for the development of additional economic incentives, including procurement incentives, liability incentives, and even tax incentives, to promote cyber security. This approach is in line with the precedent set for successful infrastructure upgrades via the social contract that government struck with industry a century ago, as well as with the model for cyber security that ISA laid out last November, and it is the most

pragmatic path to achieving the critical national security goals that are government's priority.

There are many particulars in the Administration's document that the ISA also supports. In fact, on December 3, we will be releasing a new publication entitled, "Implementing the Obama Cyber Security Strategy via the Social Contract Model." This new document will detail specific steps to move from broad policy principles, where we find broad agreement, to implementation, and it will cover issues such as:

- Securing the global IT supply chain
- Developing a new information sharing model generating actionable information for the broad range of the private sector
- Aligning and managing the legal incongruities created by modern technologies and outdated legal structures
- Creating both a market and incentives to promote proven effective cyber security standards/practices and technologies
- Creating an enterprise education program to enable modern corporations to properly appreciate and manage financial cyber risk
- Addressing the critical cyber security issues facing higher education
- Developing automated security standards for unified communications platforms such as VOIP

However, given the short amount of time that I have with the Senate Judiciary Committee, I will focus my oral comments on three major truths that I believe to be central for Congress to understand if it is going to legislate on the issue of cyber security.

These are:

I. The Internet changes everything
II. Cyber security is as much an economic issue an "IT" issue
III. We will need to develop new understandings about government and industry's roles and responsibilities, and limitations if we are to address this serious 21st century problem on a sustainable basis.

I. THE INTERNET CHANGES EVERYTHING

Most of us in this room are part of the group that demographers are now calling the “digital immigrants,” meaning that we, unlike my teenage children who are ‘digital natives,” were not born into this digital world we that now surrounds us.

While senior policy makers, such as the members of this committee, can successfully adapt to their new digital world, it is important for them not to simply assume that the assumptions and governance models developed primarily during the cold war era apply well to digital technology.

The Internet is the quintessential example of this phenomenon. 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’s critical to our national defense, but it is not a military installation.
- It’s all these things, and much more.

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

It’s not even really an “It.” It’s actually lots of “Its” all knitted together. Some ‘Its’ are public, some are private, but all transmit information across corporate and national borders without once stopping to pay tolls or to 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 new system effectively.

The regulatory model that 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 regulatory agencies: the FCC, the SEC, the FTC. That system, for the most part, has worked arguably well.

However, 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, it would not be comprehensive enough. Even if some agency wrote a brilliant regulation, that regulation is likely to be out-dated before it got through the process, a process that can be further delayed through court challenges.

This also 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 are meeting the federal regulations, but everyone knows that the system is not really working.

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

Yet, we can't stand idly by, either. Together we must develop a mechanism to assure an effective and sustainable system of security that will accommodate the global breadth of the Internet and yet 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. We need to have corporations, who own and operate the vast majority of the Internet, to perceive that it is in their own self interest to continually improve not only their own security, but also the security of everyone else with which they interact. In order for us to create such a system, we need to appreciate the second core truth, namely:

II. Cyber Security is as much an Economic issue as an "IT" issue.

Until just recently, it was common for information security policy discussions in Washington to take place without any reference to economic issues. However, corporate suites are one arena in which these discussions rarely ignore economics.

As PricewaterhouseCoopers' 2009 Global Information Security Study documents, economic considerations are actually one of the most important considerations in determining corporate information security spending decisions, and these considerations rate higher than regulatory compliance, company reputation or internal policy compliance, and nearly as high as the number one issue, business continuity/disaster recovery.

Despite the obvious importance of understanding cyber security economics in the development of public policy, it is little discussed and often difficult to delineate.

For example, in order to attack their ultimate targets, it is common practice for cyber attackers to capture and use third-party computers. As a result, many attacked computers do not suffer the direct economic consequences of an attack since they are simply being used to facilitate a further attack. Moreover, the defense, of the ultimate targets of an attack is compromised through the interactions with these third-party systems. The owners of the third party computer systems utilized in a cyber attack may not have the economic incentives to adequately invest in their computers' defense since they do not suffer the direct economic costs of a cyber attack.

On the other hand, the defensive investments required of the ultimate targets of cyber attacks can be substantially undermined by the weakness of others with whom they are interconnected, thus reducing the return on investment (ROI) generated by their cyber security spending.

Ultimately, the economics of cyber security are not readily transparent and are poorly appreciated.

There are also substantial internal reasons for failing to recognize the true costs of cyber events. This is true for consumers, businesses and even the federal government.

For example, many consumers have a false sense of security due to their belief that most of the financial impact resulting from the loss of their personal data will be fully covered by corporate entities (such as the banks). In fact, much of these losses is transferred back to consumers in the form of higher interest rates and consumer fees.

Meanwhile, most of our corporate structures are built on outdated models wherein the owners of data do not understand themselves to be

responsible for the defense of that data. The marketing department has data, the finance department has data, the human resources department has data, but, in most instances, these departments think that the security of their data is not their responsibility, but the responsibility of the "IT guys" at the end of the hall. As a result, the financial risk management of cyber events across enterprise settings is not often properly analyzed, nor properly appreciated, and cyber defense is not adequately budgeted.

At the federal government level, there seems to be no appreciation of the enormous financial risk that the government itself shoulders from the prospect of a "cyber hurricane." In reality, the federal government is the de-facto "insurer of last resort," and would be faced with footing virtually the entire financial burden of a massive cyber event.

This lack of financial risk management on the part of the government is similar in kind to the blind eye that many corporate entities turn toward cyber events. In both cases, a conceptually prudent strategy would be to engage in risk transfer techniques (such as the use of insurance), but there is little evidence that this is occurring on a national level.

The interaction of these factors may be at the root of the fact that, despite the increasingly publicized dangers of cyber incursions, nearly half (47%) of all of the enterprises studied in the 2009 Global Information Security Study reported that they are actually **reducing their budgets for information security initiatives**.

These information security spending decreases are taking place even though many enterprises (42%) acknowledge that the "threats to their information security have increased" and more than half of these enterprises (52%) acknowledge that these cost reductions make adequate security more difficult to achieve**.**

Ultimately, the dispiriting realization, with respect to cyber security economics, is that all of the current economic incentives favor cyber attackers:

Cyber attacks are comparatively cheap and easy to execute.

The profits that can be generated from cyber attacks are enormous.

The cyber defensive perimeter is nearly limitless.

Losses are difficult to assess.

Defense is costly, and, often, does not generate perceived adequate return on investment.

The ISA Cyber Security Social Contract argues that, much like the utility service model, what will be required to address this issue is for the public sector to deploy market incentives to motivate private investment for the purposes of protecting the public interest. The government is charged with the responsibility to provide for the common defense. However, in the cyber world, the government cannot do this alone. They will require private sector cooperation and investment. While some of the investment will come from corporations serving their own private security needs, the extent of investment to serve the broader public needs, due to some of the unique aspects of cyber economics described previously will be greater than what is justified by private sector business plans.

This brings us to the third central truth that, namely:

> III. We will need to develop new understandings about government and industry's roles and responsibilities and limitations if we are to address this serious 21st century problem on a sustainable basis.

The government must face some inconvenient truths.

First, the diversified nature of the internet places much of the critical national security operations in private industry's hands. This does not that mean government has a lesser role; it means that government has a different, and, frankly, an even more challenging role.

Second, although US national security is clearly at stake, unilateral US action cannot solve the problem. The Internet is an inherently global technology. In fact, virtually every component of the system is designed, developed, manufactured, or assembled off US shores and is beyond the reach of US government oversight. We must develop a way to construct a secure system out of potentially insecure parts.

Simultaneously, there is an urgent need to move beyond the informal, DC-centered partnerships of the past. While these inside-the-beltway structures have an important place in the system, government must frankly

address industry at a business plan-level. Government needs to provide incentives for industry to invest in security items that may not be justified by their corporate business plans.

The good news is that we know a great deal about how to protect the Internet, and we can achieve tremendous progress rather quickly if we embrace new government and industry roles that are geared toward implementing voluntary compliance with practices, technologies and standards that have been independently-proven to be effective.

There is a wide range of evidence that the market has already generated the practices/standards and technologies that can address most of the cyber security problem. What we have yet to address are the economics of the problem.

The "Global Information Security Survey" conducted by PricewaterhouseCoopers found that organizations that followed best practices had zero downtime and zero 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 drew on over 500 forensic engagements over a four year period, including literally tens of thousands of data points. The study concluded that, in 87% of cases, investigators were able to conclude that the breach could have been avoided if reasonable security controls had been in place at the time of the incident."

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

So what is the best role for government to play in this new digital world?

To begin, Congress ought to heed President Obama's admonition, and not mandate cyber security standards for the private sector.

Apparently, there is still a belief among some of the digital immigrants around Capitol Hill that there must be some single, minimum, gold standard of cyber security that the government ought to mandate. There is not.

This is not to say that there are not standards that work. In fact, the joke in the cyber security world about standards is, the good thing about cyber security standards is that there are so many of them.

And, there is a reason for the multitude of standards and practices. Modern systems are not fully purchased off the shelf and then plugged into the wall like a TV. Enterprises are constantly modifying their systems internally, upgrading some portions of the systems and not others, and adapting these systems to fit various business models, competitive climates, and various contractual, cultural, and regulatory regimes. There is no one size fits all.

In truth, though, the government really ought not to care about what the standards are, or, even, who created them. What government ought to care about is what works.

The broad model we suggest that the government consider is that of the FDA, which does not create drugs, and instead evaluates drugs for efficacy. This is a role for the federal government to fulfill, although not directly. The federal government ought to fund the independent evaluation of cyber security standards, practices, and technologies so the private sector will know both what works and how well. Then, it should be completely up to private enterprises to select what they choose to adopt voluntarily.

The second role the government ought to undertake is to modernize the economic incentive structures so that they are geared to protecting both our immediate and long-term national economic and defense issues.

Again, in this regard, we support the initial steps that have been outlined in the Administration's Cyber Space Policy Review. ISA has developed a fairly detailed outline of how this system ought to work, which I have abstracted for our written testimony.

A third area for governmental involvement is with respect to education. Again, this is well-emphasized in the Administration's

document. However, I would make this area a point of caution. There is currently, by senior policy makers, a lot of talk about the need for cyber education among k-12 students. As the father of young children, I, myself, naturally support these efforts, especially if they focus on values and principles.

The caution is that these digital natives, who are in the k-12 quadrant, tend to be on average much more technology savvy than many of the digital immigrants who are their teachers.

We would suggest that the government pay greater attention to enterprise education as that will reach the people who are in the work force now, many of whom will be there for decades. This population is also among the main digital immigrants - especially the senior executives. Far more immediate and long-term return on investment might be gained through a sophisticated Enterprise Education program, along the lines mentioned in the Cyber Space Policy Review, than through in-depth k-12 cyber security education.

Finally, I would like to turn to how to create a functioning government industry partnership that is based on market incentives and will reach industry where the key decisions are made - at the business plan level.

In order to create a system to maximize the use of market incentives for cyber security, three essential elements need to be developed.

1. A system must be developed to determine, on an ongoing basis, what voluntary behaviors will merit incentives.
2. A network of incentives must be catalogued and then applied to the widely diverse private sector.
3. A system to monitor use of the voluntary regime must be developed in order to track the appropriateness and the effectiveness of the incentives.

ISA proposes a system that will address each of these areas:

1. Determining what actions deserve incentives

The best way for government to motivate the specific cyber security behaviors it would like industry to adopt to meet the national (i.e. beyond

normal business) interests, is to engage industry at the business plan level and to make it in the private corporation's best economic interests to enhance the infrastructure.

An effective method of stimulating security would be to create a competitive market for the development, and the adoption of sound security practices, standards, and technologies.

By creating a competitive market, the power of that market can be harnessed to motivate improved cyber security and, since many of the organizations targeted are international, improvements on a worldwide basis are quite possible.

The government, as well as the private sector, would create market incentives for higher tiers of standards and practices to be utilized within businesses by designating contractual requirements that matched the criticality of a product/program to a given security posture (e.g., a contract for critical infrastructure might require a Tier 4 certification while a contract for paper products might only require Tier 1).

Such a model would provide incentives for individual companies to invest, on purely voluntary basis, in enhanced cyber security in order to access even higher levels of incentives.

ISA proposes that government identify multiple entities, both public and private, to identify standards and practices that would be eligible for market incentives.

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

The government's first 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 standards and practices only based on the efficacy of their standards as determined by independent studies.

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

- Information security procedures adopted for regulated services by a Federal sector-specific regulatory agency.

- Standards established and maintained by the following recognized standards organizations such as:
  - International Standards Organization
  - American National Standards Institute
  - The Internet Security Alliance
  - 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.

- Technologies approved as designated or certified anti-terror technologies by the Department of Homeland Security under the SAFETY Act.

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

Various incentives would be awarded to enterprises based on the quality of the practices they have voluntarily chosen to implement.

The ISA model is superior for many reasons:

First, it allows for multiple "standards" to be rewarded and, thus, avoids the one size fits all problem of a single standard.

Second, standard-setting organizations would compete to continually improve their standards and their cost effectiveness in order to receive better grades and to qualify their users for improved incentives. The standard setting entities themselves are enhanced by the number of organizations that adopt their standards.

As a result, there is a continuing economic motivation to improve the "standards/practices/technologies." This has a social benefit since technologies, along with their vulnerabilities and threat vectors, also constantly change. While traditional regulatory mechanisms move far too slowly to keep pace with this continuing evolution, a system motivated by profit can move with far greater speed.

Third, international standards can qualify for US incentives, which will better meet the needs of international corporations and will side-step the problems of a US-only implementation or the setting of bad precedent.

Fourth, while the US cannot “govern” foreign operating organizations, it can provide incentives for good behavior to them or to US domestic entities in their non-domestic facilities. As a result, an incentive system will allow the US to improve not only domestic cyber security, but also international cyber security, which is in the US’ national interest.

2. Creating a system of incentives that can be matched to various, individualized corporate needs and levels of voluntary security compliance.

It is important to note at the outset, that the use of market incentives to promote cyber security does not necessarily mean large government spending increases. For example, in many instances, such as SBA loans or special instances such as the awarding of TARP money, the government is making the expenditure already and would simply be adding to the requirements for recipients. In addition, there are a variety of non-monetary incentives, including streamlined regulation and liability protections, that don’t entail any direct costs. Finally, there is a range of private sector incentives, such as insurance, that can be far better developed and can be used to improve cyber security just as other such mechanisms have been used to enhance health, driving, and other consumer behavior.

In the ISA model, various tiers of standard/practice compliance could then be mapped to the qualifying incentives for these various levels of compliance (e.g., level "x" yielding tax incentive "a," and level "y" yielding tax incentive "b").

However, just as it is true that one size of standard/practice may not apply equally well to various businesses or technology systems, it is also true that one set of incentives may have different applicability and attractiveness to different enterprises.

Obviously, a defense contractor might be most attracted by incentives tied to government procurement, whereas a financial institution might be more attracted to insurance benefits and smaller companies might be more interested in expanding the opportunity to access SBA loans. The list of examples can go on and on.

As a result, ISA suggests that a range of incentives ought to be made available to those companies that choose to enhance their own security.

The following is a list of incentives, many of which are of low or virtually no-cost to the public that can be used to alter 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 9/11 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, thereby 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.

2. Tie federal monies (grants/SBA loans/stimulus money/bailout money) to adoption of designated effective cyber security standards/best practices.

Using the model described previously 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).

One of the benefits of this approach is that there is no significant impact on the federal budget due to the fact that this money is already designated for distribution. There is also the potential for relatively immediate impact since this approach 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 will allow for compliance testing as a means of approving and of continuing the contracts. The reach of the positive effect of this approach will go beyond major players to include a broader universe of suppliers and contractors to CIKR.

3. Leverage Purchasing Power of Federal Government. Government could increase the value of security in the contracts it awards to the private sector, thereby 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 at inception 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 also have a significant effect on down-stream entities.

While this approach does have the potential for substantial benefits, government needs to enhance the value of the contracts because a number of the organizations within the supply chain do not have the same massive incentive to adopt government specifications that some larger players do. This approach has potential for real and immediate benefits, but it is important that government realize that such compliance cannot be expected to come "for free." National security has a cost, and that cost is the government's responsibility.

4. Streamline regulations/reduce complexity. Regulatory and legislative mandates and compliance frameworks that address information security, such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Health Insurance

Portability and Accountability Act, along with state regimes, could be analyzed to create a unified compliance mode for similar items and to eliminate any overlaps. Sector-specific requirements could be identified, of course, but effective security has many similar elements. Duplicative regulations would impose a cost on industry that, ultimately, increases its resistance to prioritizing compliance.

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

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

While tax incentives are often difficult politically, this approach may be targeted to small and medium-sized businesses. SMEs are a weak link in the cyber security supply chain and, without incentives, they may 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 that are developing and implementing cyber security technologies or practices. Alternatively, R&D could be run through one or more of the FFRDCs. This approach 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 while 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 these costs are 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 successful, one-in-a-million hostile attack. This type of outcome is not in the best interest of the public policy for 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. This objective stands in contrast to those who argue that there should be no liability at all.

8. Create A National Award for Excellence in Cyber Security. The Federal 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, and consumers will most likely value companies that have this type of recognition, particularly in a marketplace in which 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 to be measured against, all while simultaneously transferring a portion of risk that 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 that are adopting better security practices will receive lower insurance rates. This helps companies to internalize both the benefits of good security as well as the costs of poor security, which in turn leads to greater investment and improvements in cyber security. The security requirements utilized by cyber-insurers are also helpful in this regard.

With widespread take-up of insurance, these requirements will become de facto standards, while still being responsive to updates that are necessary in the face of new risks. Insurers have a strong interest in greater security, and their requirements are continually increasing. In addition to directly improving security, cyber-insurance is also enormously beneficial in the event of a large-scale security incident.

Insurance provides a smooth funding mechanism for recovery from major losses, helping businesses return to normal and to reduce their 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 and lower premiums for companies whose expected loss is lower. This avoids a potentially dangerous concentration of risk, while also preventing companies from gaining a free-ride. Insurance companies can also provide a market-based monitoring and assessment function that reduces the cost to the government while assuring compliance with ever-increasing standards and practices.

3. A system to monitor use of the voluntary regime must be developed in order to track the appropriateness and the effectiveness of the incentives.

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

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

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

The PricewaterhouseCoopers study, as reported in the October 2008 edition of CIO Magazine, claims that only "44% of respondents say they test their organizations for compliance with whatever laws and industry regulations apply." The study notes that this represents 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 that this is not an area in which the federal government performs well. As such, it is impractical for the federal government, funded only by tax dollars, to take on the massive role of determining, monitoring, and constantly adjusting cyber security requirements.

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

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

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